



Zoklet BI Guide

Disclaimer

By reading beyond this disclaimer the reader understands that Zoklet.net and all affiliated parties, including the writers of this document, are in no way responsible for any loss, injury, retribution or any legal action of any kind that may occur from conducting anything mentioned, suggested or implied in this article. This disclaimer extends to any circumstances/situations not readily foreseeable at this time.

The reader understands that the fabrication, and ownership, of several items in this document is illegal in most countries and that if they are discovered in possession of these items legal action may be taken against them -the reader.

The reader also agrees that should legal proceeding occur, zoklet and all affiliated parties, including the writers of this document, cannot in anyway be brought into account for anything. Should this be ignored the reader fully agrees to compensate zoklet and all affiliated parties, including the writers of this document, in a manner to be specified by the latter -the writers- at the end of the legal proceedings.

This document is not intended to fall into the hands of children, or be used by them. Should this occur parents are to be held responsible for not blocking this content from their Childs online searches, and for not observing said child whilst online.

This is a disambiguation document, which only deals with theoretical situations.

In layman's terms:

If anything bad happens it's not our fault and if you try to blame us you have no choice but to compensate us in a way we choose

Introduction

This guide is compiled from several sources, as well as experience from the contributors. It is an easy to understand and use guide on all things "[Bad Ideas](#)".

On the 19th of January 2009 the temple of the screaming electron (totse or &t) closed down its servers. After having been online for upwards of twenty years the website had compiled many guides, and how-to manuals on a variety of topics all of which would have been lost if not for the website zoklet, the owner of which agreed to host the [totse archives](#).

So, in celebration of totses new form, this small but practical, guide has been compiled. Whilst lacking in content now this guide will eventually grow to encompass a wider variety of topics.

Also, stop by the [Bad Ideas](#) forum and give your input? The whole online community can benefit from your knowledge and experience.

Index

Explosives

- Introduction
- Sulphuric acid
- Potassium nitrate
- Nitric acid
- Picric acid
- Lead azide
- Mercury fulminate
- Ammonium tiriodide
- R.D.X
- Potassium chlorate
- D.D.N.P
- Nitro-glycerine
- Dynamite (basic)
- Ammonium nitrate
- Nitrogen trichloride
- Tovex
- H3
- Acetone peroxide
- Addendum

Night-ops

- Introduction
- Concealment
- Movement
- Physical security and intrusion detection systems
- Police call radio guide
- Lying methodology
- The art of escaping
- Multiple personalities and id's
- Tear gas

Poisons

- Introduction
- Chlorine gas
- Carbon tetrachloride
- Nicotine
- Ethylene glycol
- D.V.D.P
- Potassium/sodium cyanide
- Aspirin
- Paracetamol
- Petrol
- Potassium chloride
- Parquet
- Vinegar poison
- Castor bean
- Puffer fish venom
- Hemlock
- Oleander
- Digitalis
- Yew tree needles and laurel leaves
- Rhubarb

Miscellaneous:

- Light Bulb Bombs
- Loss Prevention.
- Dealing with LP.
- Barcoding with Barcode Magic 3.1 Guide.
- The Grocery Store Shoplifting Guide.
- Make Your Own Finger Prints.
- How to Use TamperData to Get Intangible, Easily Resalable Stuff for a Cent.
- Tor
- Everything you need to know about Carding.

Explosives



Explosives

This section covers a wide range of explosive material and how to obtain them and make them

Some safety rules need to be followed when making or handling any explosive material, such as:

- ❖ When making a new explosive, make it in small quantities if you do not know how the explosive will react.
- ❖ Always make and handle explosives with care, do not jostle them about, do not leave them exposed to any elements or high temperatures
- ❖ Do not store explosive materials for more than a few days, or none at all if it can be helped.
- ❖ Dress in general protective clothing as some of the substances that you will be handling are harmful.
- ❖ Finally, don't fabricate any of these materials near anything of value.

Generally try to be as safe as possible, any random safety measurers that you fabricate can also help you not to blow your hand off its joint. Many anarchists and children have overlooked safety as a direct result of guides similar to this one not specifying any. So be a cautious as possible when dealing with this section.

Sulphuric acid

Sulphuric acid is far too difficult to make outside of a laboratory or industrial plant. However, it is readily available in an uncharged car battery. A person wishing to make sulphuric acid would simply remove the top of a car battery and pour the acid into a glass container. There would probably be pieces of lead from the battery in the acid which would have to be removed, either by boiling or filtration. The concentration of the sulphuric acid can also be increased by boiling it; very pure sulphuric acid pours slightly faster than clean motor oil.



Potassium nitrate

Also known as salt peter

Potassium nitrate could be obtained from store-bought black powder, simply by dissolving black powder in boiling water and filtering out the sulphur and charcoal. To obtain 68 g of potassium nitrate, it would be necessary to dissolve about 90 g of black powder in about one litre of boiling water. Filter the dissolved solution through filter paper in a funnel into a jar until the liquid that pours through is clear. The charcoal and sulphur in black powder are insoluble in water, and so when the solution of water is allowed to evaporate, potassium nitrate will be left in the jar. It can also be obtained from pharmacies off-the-shelf



Nitric acid

There are several ways to make this most essential of all acids for explosives. One method by which it could be made will be presented.

MATERIALS

[potassium nitrate](#)

Distilled water

Concentrated [sulphuric acid](#)

EQUIPMENT

Adjustable heat source

Retort

Collecting flask with stopper

Glass stirring rod

Ice bath



Procedure

1. Pour 32 millilitres of concentrated sulphuric acid into the retort.
2. Carefully weigh out 58 grams of sodium nitrate, or 68 grams of potassium nitrate, and add this to the acid slowly. If all of it does not dissolve carefully stir the solution with a glass rod until it does.
3. Place the open end of the retort into the collecting flask, and place the collecting flask in the ice bath.

Begin heating the retort, using low heat. Continue heating until liquid begins to come out of the end of the retort. The liquid that is formed is the nitric acid. Heat until the precipitate in the bottom of the retort is almost dry, or until no more nitric acid is forming.

CAUTION: If the acid is heated too much, the nitric acid will decompose as soon as it is formed. This can result in the production of highly flammable and toxic gasses that may explode. It is a good idea to set up the above apparatus, and then get away from it.

Picric Acid

Picric acid can be used as a booster explosive in detonators or as an intermediate to preparing lead picrate or DDNP.

MATERIALS

Aspirin, 20 tablets (5 grain/tablet)

[alcohol](#) - 95 percent pure

Concentrated [sulphuric acid](#)

[Potassium nitrate](#)

Water

EQUIPMENT

Canning jar (1 pint)

Hot water bath

Paper towels (for filter)

Glass tube or rod

Glass containers

Dish (ceramic or glass)

Heat source

Cup

Teaspoon



Procedure

1. Crush 20 tablets of Aspirin in a glass container and work into a paste with a teaspoon of water.
2. Add approximately 1/3-1/2 cup (100 millilitres) of alcohol with stirring and filter through a paper towel into another glass container.
3. Discard the solid left on the paper and pour the liquid from the container into the dish. Evaporate the alcohol and water on a hot water bath, leaving a white powder.
4. Add this white powder to 1/3 cup (80 millilitres) of concentrated sulphuric acid in a canning jar.
5. Heat the jar in a simmering hot water bath for 15 minutes and remove. Stir; solution will gradually turn black.
6. Add 3 level teaspoons (15 grams) of potassium nitrate in three portions with vigorous stirring. After heating put the jar in cold water and add the saltpetre.
7. Allow the yellow-orange solution to cool to room temperature with intermittent stirring. Solution is darker than yellow-orange.
8. Pour the solution into 1.25 cups (300 millilitres) of water (cold if possible) and allow this to cool. Upon pouring, the solution is now yellow-orange.
9. Filter the mixture through a paper towel and wash the light yellow material (picric acid) with 1/8 cup (25 millilitres) of water through paper towel. This takes considerable time to filter if genuine filter paper is used.
10. Dry at 160-200 degrees F for two hours. The yield is 4.0-4.5 grams.

Note:

If aspirin is pure enough (usually cheap priced aspirin are) then steps 1, 2 and 3 can be omitted and you can proceed to add crushed aspirin to sulphuric acid.

Lead azide

Lead Azide is a material that is often used as a booster charge for other explosive, but it does well enough on its own as a fairly sensitive explosive. It does not detonate too easily by percussion or impact, but it is easily detonated by heat from an ignition wire, or a blasting cap. It is simple to produce, assuming that the necessary chemicals can be procured.

MATERIALS

Sodium azide
Lead acetate
Water

EQUIPMENT

Filter
Beakers 3
Heat source
Glass rod



Procedure

1. Dissolving sodium azide and lead acetate in water in separate beakers, the two materials are put into an aqueous state.
2. Mix the two beakers together, and apply a gentle heat. Add an excess of the lead acetate solution, until no reaction occurs, and the precipitate on the bottom of the beaker stops forming.
3. Filter off the solution, and wash the precipitate in hot water. The precipitate is lead azide, and it must be stored in a wet environment for safety. If lead acetate cannot be found, simply acquire acetic acid, and put lead metal in it. Black powder bullets work well for this purpose.

Mercury Fulminate

Mercury fulminate is perhaps one of the oldest known initiating compounds. It can be detonated by either heat or shock, which would make it of infinite value to an anarchist. Even the action of dropping a crystal of the fulminate causes it to explode. A person making this material could use the following procedure:



MATERIALS

[Mercury](#) (5 g)
Concentrated [nitric Acid](#) (35 ml)
[Ethyl alcohol](#) (high alcohol beverages) (30 ml)
Distilled water

EQUIPMENT

Glass stirring rod
100 ml beaker (2)
Adjustable heat source
Blue litmus paper
Funnel and filter paper

Procedure

1. In one beaker, mix 5 g of mercury with 35 ml of concentrated nitric acid using the glass rod.
2. Slowly heat the mixture until the mercury is dissolved, which is when the solution turns green and boils.
3. Place 30 ml of ethyl alcohol into the second beaker, and slowly and carefully add all of the contents of the first beaker to it. Red and/or brown fumes should appear. These fumes are toxic and flammable.
4. After thirty to forty minutes, the fumes should turn white, indicating that the reaction is near completion. After ten more minutes, add 30 ml of the distilled water to the solution.
5. Carefully filter out the crystals of mercury fulminate from the liquid solution. Dispose of the solution in a safe place, as it is corrosive and toxic.
6. Wash the crystals several times in distilled water to remove as much excess acid as possible. Test the crystals with the litmus paper until they are neutral. This will be when the litmus paper stays blue when it touches the wet crystals
7. Allow the crystals to dry, and store them in a safe place, far away from any explosive or flammable material.

Note:

This procedure can also be done by volume, if the available mercury cannot be weighed. Simply use 10 volumes of nitric acid and 10 volumes of ethanol to every one volume of mercury.

Ammonium triiodide crystals

Ammonium triiodide crystals are foul-smelling purple coloured crystals that decompose under the slightest amount of heat, friction, or shock, if they are made with the purest ammonia (ammonium hydroxide) and iodine. Such crystals are said to detonate when a fly lands on them, or when an ant walks across them. Household ammonia, however, has enough impurities, such as soaps and abrasive agents, so that the crystals become less sensitive and will detonate when thrown, crushed, or heated.

Upon detonation, a loud report is heard, and a cloud of purple iodine gas appears about the detonation site. Whatever the unfortunate surface that the crystal was detonated upon will usually become ruined, as some of the iodine in the crystal is thrown about in a solid form, and iodine is corrosive. It leaves permanent brownish-purple stains on whatever it contacts. Iodine gas can damage lungs, and it settles to the ground and stains things there as well.

Touching iodine leaves brown stains on the skin that last for about a week, unless they are immediately and vigorously washed off.

Ammonium triiodide crystals can be produced in the following manner:

MATERIALS

[Iodine](#) crystals
Clear ammonia

EQUIPMENT

Funnel and filter paper
Paper towels
Two throw-away glass jars

Procedure

1. Place about two teaspoons of iodine into one of the glass jars. The jars must both be “throw-away” because they will never be clean again.
2. Add enough ammonia to completely submerge the iodine.
3. Place the funnel into the other jar, and put the filter paper in the funnel. The technique for putting filter paper in a funnel is taught in every basic chemistry lab class: fold the circular paper in half, so that a semi-circle is formed. Then, fold it in half again to form a triangle with one curved side. Pull one thickness of paper out to form a cone, and place the cone into the funnel.
4. After allowing the iodine to soak in the ammonia for a while, pour the solution into the paper in the funnel through the filter paper.
5. While the solution is being filtered, put more ammonia into the first jar to wash any remaining crystals into the funnel as soon as it drains.
6. Collect all the purplish crystals without touching the brown filter paper, and place them on the paper towels to dry for about an hour. Make sure that they are not too close to any lights or other sources of heat, as they could well detonate. While they are still wet, divide the wet material into about eight chunks.
7. After they dry, gently place the crystals onto a one square inch piece of duct tape. Cover it with a similar piece, and gently press the duct tape together around the crystal, making sure not to press the crystal itself. Finally, cut away most of the excess duct tape with a pair of scissors, and store the crystals in a cool dry safe place.

The crystals have a shelf life of about a week, and they should be stored in individual containers that can be thrown away, since they have a tendency to slowly decompose, a process which gives off iodine vapours, that will stain whatever they settle on. One possible way to increase their shelf life is to store them in airtight containers.

To use them, simply throw them against any surface or place them where they will be stepped on or crushed.

R.D.X

R.D.X., also called cyclonite, or composition C-1 (when mixed with plasticizers) is one of the most valuable of all military explosives. This is because it has more than 150% of the power of T.N.T., and is much easier to detonate. It should not be used alone, since it can be set off by a not-too severe shock. It is less sensitive than mercury fulminate, or nitro-glycerine, but it is still too sensitive to be used alone. R.D.X. can be made by the surprisingly simple method outlined hereafter. It is much easier to make in the home than all other high explosives, with the possible exception of ammonium nitrate.

MATERIALS

[Hexamine or methenamine](#)

Fuel tablets (50 g)

Concentrated [nitric acid](#) (550 ml)

Distilled water

Table salt

Ice

[Ammonium nitrate](#)

EQUIPMENT

500 ml beaker

Glass stirring rod

Funnel and filter paper

Ice bath container (plastic bucket)

Blue litmus paper

Centigrade thermometer



Procedure

1. Place the beaker in the ice bath, and carefully pour 550 ml of concentrated nitric acid into the beaker.
2. When the acid has cooled to below 20 degrees centigrade, add small amounts of the crushed fuel tablets to the beaker. The temperature will rise, and it must be kept below 30 degrees centigrade, or dire consequences could result. Stir the mixture.
3. Drop the temperature below zero degrees centigrade, either by adding more ice and salt to the old ice bath, or by creating a new ice bath. Or, ammonium nitrate could be added to the old ice bath, since it becomes cold when it is put in water. Continue stirring the mixture, keeping the temperature below zero degrees centigrade for at least twenty minutes
4. Pour the mixture into a litter of crushed ice. Shake and stir the mixture, and allow it to melt. Once it has melted, filter out the crystals, and dispose of the corrosive liquid.

5. Place the crystals into one half a litre of boiling distilled water. Filter the crystals, and test them with the blue litmus paper. Repeat steps 4 and 5 until the litmus paper remains blue. This will make the crystals more stable and safe.
6. Store the crystals wet until ready for use. Allow them to dry completely using them. R.D.X. is not stable enough to use alone as an explosive.
7. Composition C-1 can be made by mixing 88.3% R.D.X. (by weight) with 11.1% mineral oil, and 0.6% lecithin. Knead the materials in a plastic bag. This is a good way to desensitize the explosive.
8. H.M.X. is a mixture of T.N.T. and R.D.X.; the ratio is 50/50, by weight. It is not as sensitive, and is almost as powerful as straight R.D.X.
9. By adding ammonium nitrate to the crystals of R.D.X. after step 5, it should be possible to desensitize the R.D.X. and increase its power, since ammonium nitrate is very insensitive and powerful. Sodium or potassium nitrate could also be added; a small quantity is sufficient to stabilize the R.D.X.

Note:

R.D.X. detonates at a rate of 8550 meters/second when it is compressed to a density of 1.55 g/cubic cm.

Potassium chlorate

Potassium chlorate itself cannot be made in the home, but it can be obtained from labs. If potassium chlorate is mixed with a small amount of Vaseline, or other petroleum jelly, and a shockwave is passed through it, the material will detonate with slightly more power than black powder. It must, however, be confined to detonate it in this manner. The procedure for making such an explosive is outlined below:



MATERIALS

Potassium chlorate (9 parts, by volume)
Petroleum jelly (Vaseline) (1 part, by volume)

EQUIPMENT

Zip-lock plastic bag
Wooden bowl and wooden spoon or clay grinding bowl



Procedure

1. Grind the potassium chlorate in the grinding bowl carefully and slowly, until the potassium chlorate is a very fine powder. The finer that it is powdered, the faster (better) it will detonate.
2. Place the powder into the plastic bag. Put the petroleum jelly into the plastic bag, getting as little on the sides of the bag as possible, i.e. put the Vaseline on the potassium chlorate powder.
3. Close the bag, and knead the materials together until none of the potassium chlorate is dry powder that does not stick to the main glob. If necessary, add a bit more petroleum jelly to the bag.
4. The material must be used within 24 hours, or the mixture will react to greatly reduce the effectiveness of the explosive. This reaction, however, is harmless, and releases no heat or dangerous products.

D.D.N.P

MATERIALS

Distilled water
 Lye (caustic soda)
[Picric acid](#)
[Sulphur](#)
[Sulphuric acid](#)
[Potassium nitrate](#)



EQUIPMENT

Teflon rod
 4 Glass jars with ml increments
 Gas burner/ heat source
 Filter papers (coffee filter, paper towels)
 Eyedropper
 Stopper

Procedure

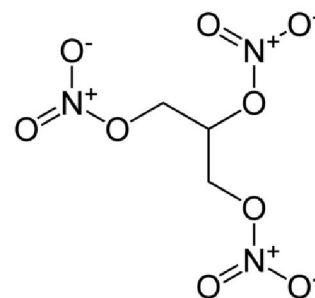
1. In a pint glass jar place 90 ml warm water and 1.5 grams of lye (sodium hydroxide). Mix these with a "Teflon" stirrer until all the lye had dissolved. Dissolve 9 grams of picric acid crystals in the lye-water solution by stirring. Label this jar solution #1.
2. In a 500 ml beaker 3 ml of water is placed. Dissolve 7.5 grams of sulphur and 7.5 grams of lye (sodium hydroxide) by stirring the solution. Boil this solution over a heat source. When the solution turns dark red remove and allow the liquid to cool. Label this solution #2. Add this cooled solution #2 in three portions, to solution #1. Stir with a Teflon rod while the liquid is being added. Again allow the solution mixture cool.
3. Filter this mixture through filter papers Small red particles will gather on the paper. Discard the liquid. Dissolve these red particles in 180 ml of boiling water. Remove and filter this hot liquid through a filter paper. Discard the particles left on the paper and label the liquid left #3.
4. To Solution #3 with an eyedropper slowly add sulphuric acid to the filtered solution until it turns orange brown. Add an additional 7.5 grams of acid to the liquid. In a separate pint jar, dissolve 5.4 grams of potassium or sodium nitrite in 240 ml of water. Label this solution #4.
5. In one portion solution #4 is added with stirring to solution #3. Allow the solution to stand for 10 minutes. The mixture will turn light brown.

CAUTION: At this point the brown colour is the DDNP that has formed. Keep away from flame, avoid friction and keep from shock. Filter the light brown solution through a filter paper. Wash the particles left on the paper with 60 ml of water. Allow to completely dry for 24 hours. Drying time can be reduced to 2 hours if crystals are placed in a shallow Pyrex dish and this placed in a hot (not boiling) water bath.

CAUTION: D.D.N.P. is sensitive to shock, friction and flame. Expose to any of these will very likely detonate the compound prematurely. This powder should be stored in small quantities in Stoppard glass containers. There is more safety in storage, leave 25% water in the powder and dry immediately prior to use.

Nitro-glycerine

Nitro-glycerine is one of the most sensitive explosives. Although it is possible to make it safely, it is difficult. Many a young anarchist has been killed or seriously injured while trying to make it. When Nobel's factories make it, many people were killed by the all-to-frequent factory explosions. Usually, as soon as it is made, it is converted into a safer substance, such as dynamite. Anyone who attempts to make nitro-glycerine would use the following procedure:



MATERIALS

Distilled water

Table salt

Sodium bicarbonate

Concentrated [nitric acid](#) (13 ml)

Concentrated [sulphuric acid](#) (39 ml)

[Glycerine](#)

EQUIPMENT

Eye-dropper

100 ml beaker

200-300 ml beakers (2)

Ice bath container (a plastic bucket serves well)

Blue litmus paper

Centigrade thermometer



Procedure

1. Place 150 ml of distilled water into one of the 200-300 ml beakers.
2. In the other 200-300 ml beaker place 150 ml of distilled water and about a spoonful of sodium bicarbonate then stir them until the sodium bicarbonate dissolves. Do not put so much sodium bicarbonate in the water so that some remains un-dissolved.
3. Create an ice bath by half filling the ice bath container with ice, and adding table salt. This will cause the ice to melt, lowering the overall temperature.
4. Place the 100 ml beaker into the ice bath, and pour the 13 ml of concentrated nitric acid into the 100 ml beaker. Be sure that the beaker will not spill into the ice bath, and that the ice bath will not overflow into the beaker when more materials are added to it. Be sure to have a large enough ice bath container to add more ice. Bring the temperature of the acid down to about 20 degrees centigrade or less.
5. When the nitric acid is as cold as stated above, slowly and carefully add the 39 ml of concentrated sulphuric acid to the nitric acid. Mix the two acids together, and cool the mixed acids to 10 degrees centigrade. It is a good idea to start another ice bath to do this.
6. With the eyedropper, slowly put the glycerine into the mixed acids, one drop at a time. Hold the thermometer along the top of the mixture where the mixed acids and glycerine meet. Do not allow the temperature to rise above 30 degrees centigrade; should this come to pass run away, very fast. The glycerine will start to nitrate

immediately, and the temperature will immediately begin to rise. Add glycerine until there is a thin layer of glycerine on top of the mixed acids.

7. It is always safest to make any explosive in small quantities.
8. Stir the mixed acids and glycerine for the first ten minutes of nitration, adding ice and salt to the ice bath to keep the temperature of the solution in the 100 ml beaker well below 30 degrees centigrade. Usually, the nitro-glycerine will form on the top of the mixed acid solution, and the concentrated sulphuric acid will absorb the water produced by the reaction.
9. When the reaction is complete, and when the nitro-glycerine is well below 30 degrees centigrade, slowly and carefully pour the solution of nitro-glycerine and mixed acid into the distilled water in the beaker in step 1. The nitro-glycerine should settle to the bottom of the beaker, and the water-acid solution on top can be poured off and disposed of. Try to drain as much of the acid-water solution as possible, without disturbing the nitro-glycerine.
10. Carefully remove the nitro-glycerine with a clean eye-dropper, and place it into the beaker in step 2. The sodium bicarbonate solution will eliminate much of the acid, which will make the nitro-glycerine more stable, and less likely to explode for no apparent reason, which it can do. Test the nitro-glycerine with the litmus paper until the litmus stays blue. Repeat this step if necessary, and use new sodium bicarbonate solutions as in step 2.
11. When the nitro-glycerine is as acid-free as possible, store it in a clean container in a safe place. The best place to store nitro-glycerine is far away from anything living, or from anything of value.

Note:

Nitro-glycerine can explode for no apparent reason, even if it is stored in a secure cool place.

Note

The process of removing the glycerine from the soap is fairly complicated (and of course, there are a lot of variations on the theme). In the simplest terms: you make soap out of fats and lye. The fats already contain glycerine as part of their chemical makeup (both animal and vegetable fats contain from 7% - 13% glycerine). When the fats and lye interact, soap is formed, and the glycerine is left out as a "by-product". But, while it's chemically separate, it's still blended into the soap mix.

While a cold process soap maker would simply pour into the moulds at this stage, a commercial soap maker will add salt. The salt causes the soap to curdle and float to the top. After skimming off the soap, they are left with glycerine (and lots of "impurities" like partially dissolved soap, extra salt, etc.). They then separate the glycerine out by distilling it. Finally, they de-colorize the glycerine by filtering it through charcoal, or by using some other bleaching method.

Dynamite (basic)

The name dynamite comes from the Greek word "dynamis", meaning power. Dynamite was invented by Nobel shortly after he made nitro-glycerine. It was made because nitro-glycerine was so dangerously sensitive to shock. An individual with some sanity would, after making nitro-glycerine, immediately convert it to dynamite. This can be done by adding various materials to the nitro-glycerine, such as sawdust. The sawdust holds a large weight of nitro-glycerine per volume. Other materials, such as ammonium nitrate could be added, and they would tend to desensitize the explosive, and increase the power. But even these nitro-glycerine compounds are not entirely safe

MATERIALS

Fine sawdust

[Nitro-glycerine](#)



Procedure

1. Keeping the nitro-glycerine in the container that it was fabricated in, slowly add the fine sawdust to the nitro-glycerine.
2. Do this until all the nitro-glycerine is absorbed by the sawdust.
3. Carefully collect the saturated sawdust and place it in a container for the explosive

Ammonium nitrate

Ammonium nitrate is a high explosive material that is often used as a commercial "safety explosive" It is very stable, and is difficult to ignite with a match. It will only light if the glowing, red-hot part of a match (ember) is touching it. It is also difficult to detonate; it requires a large shockwave to cause it to become a high explosive.

Commercially, it is sometimes mixed with a small amount of nitro-glycerine to increase its sensitivity. Ammonium nitrate is used in the "Cold-Packs" or "Instant Cold", available in most drug stores. The "Cold Packs" consist of a bag of water, surrounded by a second plastic bag containing the ammonium nitrate. To get the ammonium nitrate, simply cut off the top of the outside bag, remove the plastic bag of water, and save the ammonium nitrate in a well sealed, airtight container, since it is rather hygroscopic, i.e. it tends to absorb water from the air. It is also the main ingredient in many fertilizers.



MATERIALS

[Nitric acid](#)

Household ammonia

EQUIPMENT

Adjustable heat source

An ice bath

Large flask



Procedure

1. Pour nitric acid into the large flask in an ice bath. Then, by simply pouring household ammonia into the flask, and running away, ammonium nitrate would be formed.
2. After the materials have stopped reacting, one would simply have to leave the solution in a warm place until all of the water and any non-neutralized ammonia or acid have evaporated.
3. There would be a fine powder formed, which would be ammonium nitrate. It must be kept in an airtight container.
4. The crystals formed in the above process would have to be heated VERY gently to drive off the remaining water.

Note

After heating the ammonium nitrate allow it to cool naturally. Any attempts to speed up this process will cause it to combust

The major disadvantage with ammonium nitrate, from an anarchist's point of view, would be detonating it. A rather powerful priming charge must be used, and usually with a booster charge. The primer explodes, detonating the booster, sending a tremendous shockwave through the ammonium nitrate, detonating it.

ANFOS

ANFO is an acronym for Ammonium Nitrate - Fuel Oil Solution. An ANFO solves the only other major problem with ammonium nitrate: its tendency to pick up water vapour from the air. This results in the explosive failing to detonate when such an attempt is made. This is rectified by mixing 94% (by weight) ammonium nitrate with 6% fuel oil, or kerosene. The kerosene keeps the ammonium nitrate from absorbing moisture from the air. An ANFO also requires a large shockwave to set it off.

Nitrogen Trichloride

Nitrogen trichloride, also known as chloride of azode, is an oily yellow liquid. It explodes violently when it is heated above 60 degrees Celsius, or when it comes in contact with an open flame or spark. It is fairly simple to produce.

MATERIALS

[Ammonium nitrate](#)

Distilled water

[Chlorine gas](#) (hydrochloric acid and potassium permanganate)

Alternatively: anhydrous ammonia gas/ household ammonia

EQUIPMENT

100 ml beaker (2) and stopper

Tea spoons

Masking tape

Adjustable heat source

Test tube stand

Eye dropper

Glass pipe

Procedure

1. In a beaker, dissolve about 5 teaspoons of ammonium nitrate in water. Do not put so much ammonium nitrate into the solution that some of it remains un-dissolved in the bottom of the beaker.
2. Collect a quantity of chlorine gas in a second beaker by mixing hydrochloric acid with potassium permanganate in a large flask with a stopper and glass pipe.
3. Place the beaker containing the chlorine gas upside down on top of the beaker containing the ammonium nitrate solution, and tape the beakers together. Gently heat the bottom beaker. When this is done, oily yellow droplets will begin to form on the surface of the solution, and sink down to the bottom. At this time, remove the heat source immediately.
4. Alternately, the chlorine can be bubbled through the ammonium nitrate solution, rather than collecting the gas in a beaker, but this requires timing and a stand to hold the beaker and test tube.
5. The chlorine gas can also be mixed with anhydrous ammonia gas, by gently heating a flask filled with clear household ammonia. Place the glass tubes from the chlorine-generating flask and the tube from the ammonia-generating flask in another flask that contains water.
6. Collect the yellow droplets with an eyedropper, and use them immediately, since nitrogen trichloride decomposes in 24 hours.

Tovex

This explosive is useful in that it is mostly stable and releases a large amount of energy for its mass, thus making it optimal for use in grenades

MATERIALS

[Ammonium Nitrate](#) crystals

Powdered Aluminium (a blend of flaked and atomized)

[Salt peter](#)

Gelatine or Starch (kitchen grade)

Potassium Dichromate (thickening agent). You may substitute this with chrome, iron, selenium, sulphates, nitrates or chlorides, i.e.

kitchen grade borax.

Urea, retardant, prevents swelling and gas generation in storage. Optional if material is not stored for long.

KH₂PO₄ /sodium peroxide (in 29/1 mol. ratio), also optional if storage is intended.

Distilled Water

EQUIPMENT

Sieve

Scale

Glass containers (10)

Glass stirring rod



Procedure

1. Filter an adequate quantity of each solid material through a sieve. If necessary crush the ammonium nitrate first.
2. Weigh the required quantity of each material.
Ammonium Nitrate crystals 55%
Powdered Aluminium 20%
Salt peter 10%
Gelatine or Starch 2.5%
Potassium Dichromate 1%
Urea 0.5%,
KH₂PO₄ L/sodium peroxide (in 29/1 mol. Ratio)
3. Place the screened and weighed materials in separate containers and close tightly.
4. Place Ammonium Nitrate into mixing bowl.
5. Add boiling water and stir until all Ammonium Nitrate is dissolved. (Ammonium Nitrate solubility is 580 gm per 100 ml's water at 80° c.
6. Blend the gelling powder and the potassium or sodium nitrate in a separate container.
7. Add the mix from step 7 to the hot Ammonium Nitrate solution.
8. Stir for 3 minutes.
9. Add aluminium powder.
10. Mix contents of bowl thoroughly.
11. Dissolve thickener/cross linking agent (potassium dichromate), in a little hot water and add to the bowl's contents.
12. Add mixed stabilizer and enhancer to the mix (Ingredients 6 & 7, Optional for storage.)
13. Blend thoroughly for 5-10 minutes or until mix is free of lumps.
14. Pour filler into the grenade body.
15. Insert a spacer into the molten filler for the detonator.
16. Place grenade with filler and spacer into a warm air dryer until filler coagulates into a uniform, tough gelatinous mass.
17. Remove spacer and install detonator at time of use.

Note:

Remember that, once dry, the explosive cannot be shaped into the container. So prepare the body of the grenade before completing the explosive.

All percentages are by weight

H3

H3 is a low explosive that works in a similar manner as match heads. It is a reliable and fairly powerful explosive as well, a good substitute for black powder. In addition, it does not require any special equipment to prepare. Next to match heads it is among the easiest to make explosives, provided you can get your hands on a good source of potassium chlorate. H3 burns rather quickly, like black powder or match head powder. It is a good choice of filler for firecrackers, small bombs, salutes, and a multitude of other things. It is sensitive to flame, mildly sensitive to friction, and incompatible with glycerine and phosphorus compounds.

MATERIALS

[Potassium chlorate](#). This is best used powdered. You can get it from most any chemical supplier and is supposedly available in the United Kingdom as weed killer.

Charcoal. Willow charcoal is best. This can be bought at supply stores. It should be powdered.

Starch –Cornstarch or flour-

Water

EQUIPMENT

A bowl

Strainer

Glass rod

A mortar and pestle

Procedure

1. If they are not already, grind the charcoal and potassium chlorate into fine powder, separately.
2. Mix 75 parts potassium chlorate, 23 parts charcoal, and 2 parts starch together thoroughly in a bowl.
3. Add hot water slowly and stir until a thick paste-like substance is rendered. Keep mixing until it cools.
4. Take the mass and work it through the screen. This is accomplished by tapping the edge of the sieve so that the powder falls through, similar to any baking method. However, unlike when baking, do not try to grind the H3 as this may ignite it if it's dry, but grinding can be used while the mixture is still damp. The aim here is to end up with many very small pieces of the solidifying mixture.
5. You may have to screen the mixture more than once as it hardens. Spread it out and let it dry. Once it is completely dry it is ready to use.

Acetone Peroxide

Acetone peroxide (AP) is an interesting high explosive that may be made at home fairly easily. It's a good explosive, fairly powerful, but also fairly sensitive to heat and shock. Making AP is a common entry point to the world of high explosives. AP is a common material for detonators.

Hydrogen Peroxide comes in an opaque brown bottle. You can get it at any pharmacy. You'll need a 30% concentration, and usually what is sold over the counter is usually less than that (around 3%). If you can't get 30%, you can add 10 times more peroxide than the recipe suggests. The reaction will take longer due to the dilute peroxide, however.

Acetone peroxide can be set off by crushing it or striking it hard enough, or by it coming into contact with high temperatures or flame. It has a maximum shelf life of about three weeks. It should be used shortly after making it



MATERIALS

High concentration Acetone
Hydrogen Peroxide (disinfectant)
Hydrochloric acid. Other mineral acids will work as well.

EQUIPMENT

Glass beakers
Glass rod
Thermometer
Eyedropper
Equipment for an ice bath. Bucket, ice, water, and salt
Filter paper or fine fabric



Procedure

1. Make an ice bath in the bucket. Dump some ice in it and fill it with water. Add salt to melt the ice and lower the temperature. Place the beaker in the ice bath and put the thermometer in the beaker.
2. Put 50 ml of acetone into the beaker. Then mix in 30 ml of hydrogen peroxide. Let the mixture cool to around 5 ° C.
3. Using the eyedropper, slowly add and mix in 5 ml of hydrochloric acid. Watch the thermometer as you do so, as the reaction will release heat. The ideal temperature for the reaction is between 5 ° and 10 ° C. This is important because the type of AP formed depends on the temperature of the solution. At the ideal temperatures the reaction forms tricycloacetone peroxide, which is the desired result. At higher temperatures the reaction forms dicycloacetone peroxide, which is far less stable and is more dangerous.
4. Stir for about 5 minutes.
5. Keep the beaker in a cool place, either in the ice bath or in the refrigerator (covered, of course) for a few hours. If you used dilute hydrogen peroxide, you should wait twenty four hours. If you used the recommended 30% hydrogen peroxide, about four hours should do it.
6. You will notice a white precipitate has formed in the beaker. Filter it out, and wash it in a beaker of clean water. This is the AP. Dry it someplace that isn't humid and is dark (Like a fridge.). Do not dry the AP by leaving it in the sun; this may cause it to detonate.

Chemical fire bottle

The chemical fire bottle is really an advanced Molotov cocktail. Rather than using the burning cloth to ignite the flammable liquid, which has at best a fair chance of igniting the liquid, the chemical fire bottle utilizes the very hot and violent reaction between sulphuric acid and potassium chlorate. When the container breaks, the sulphuric acid in the mixture of petrol sprays onto the paper soaked in potassium chlorate and sugar. The paper, when struck by the acid, instantly bursts into a white flame, igniting the petrol. The chance of failure to ignite the petrol is less than 2%, and can be reduced to 0%, if there is enough potassium chlorate and sugar to spare.

MATERIALS

[Potassium chlorate](#) (2 teaspoons)
Sugar (2 teaspoons)
Concentrated [sulphuric acid](#) (120 ml)
[Petrol](#) (240 ml)

EQUIPMENT

Glass bottle (360 ml.)
Cap for bottle with plastic inside
Paper towels
Glass or plastic cup and spoon
Cooking pan with raised edges

Procedure

1. Test the cap of the bottle with a few drops of sulphuric acid to make sure that the acid will not eat away the bottle cap during storage. If the acid eats through it in 24 hours, a new top must be found and tested, until a cap that the acid does not eat through is found. A glass top is excellent.
2. Carefully pour 240 ml. of petrol into the glass bottle.
3. Carefully pour 120 ml. of concentrated sulphuric acid into the glass bottle. Wipe up any spills of acid on the sides of the bottle, and screw the cap on the bottle. Wash the bottles outside with plenty of water. Set it aside to dry.
4. Put about two teaspoons of potassium chlorate and about two teaspoons of sugar into the glass or plastic cup. Add about 1/2 cup of boiling water, or enough to dissolve all of the potassium chlorate and sugar.
5. Place a sheet of paper towel in the cooking pan with raised edges. Fold the paper towel in half, and pour the solution of dissolved potassium chlorate and sugar on it until it is thoroughly wet. Allow the towel to dry.
6. When it is dry, put some glue on the outside of the glass bottle containing the petrol and sulphuric acid mixture. Wrap the paper towel around the bottle, making sure that it sticks to it in all places. Store the bottle in a place where it will not be broken or tipped over.
7. When finished, the solution in the bottle should appear as two distinct liquids, a dark brownish-red solution on the bottom, and a clear solution on top. The two solutions will not mix. To use the chemical fire bottle, simply throw it at any hard surface.

Note:

Never open the bottle since some sulphuric acid might be on the cap; this could trickle down the side of the bottle and ignite the potassium chlorate causing a fire or explosion

To test the device, tear a small piece of the paper towel off the bottle, and put a few drops of sulphuric acid on it. The paper towel should immediately burst into a white flame.

Addendum

Anyone can get many chemicals from hardware stores, supermarkets, and drug stores to get the materials to make explosives or other dangerous compounds. All one needs is an SUV and some money to acquire many of the chemicals named here.

Chemical	Used In	Available at
Alcohol, Ethyl *	Alcoholic beverages	Liquor stores solvents (95% min. For both) hardware stores
Ammonia +	Clear household ammonia	Supermarkets/7-eleven
Ammonium	Instant-cold packs,	Drug stores; nitrate fertilizers and medical Supply stores
Nitrous Oxide	Pressurizing whip cream	Party supply stores
Magnesium	Fire starters	Surplus/camping stores
Lecithin	Vitamins	Pharmacies/drug stores
Mineral Oil	Cooking, laxative	Supermarket/drug stores
Mercury @	Mercury thermometers	Supermarkets/hardware stores
Sulphuric Acid	Uncharged car batteries	Automotive stores
Glycerine	N/a	Pharmacies/drug stores
Sulphur	Gardening	Gardening/hardware store
Charcoal	Charcoal grills	Supermarkets/gardening stores
Sodium Nitrate	Fertilizer	Gardening store
Cellulose (Cotton)	First aid	Drug/medical supply stores
Strontium Nitrate	Road flares	Surplus/auto stores
Fuel Oil	Kerosene stoves	Surplus/camping stores
Bottled Gas	Propane stoves	Surplus/camping stores
Potassium Permanganate	Water purification	Purification plants
Hexamine Or Methenamine	Hexamine stoves (camping)	Surplus/camping store
Nitric Acid ^	Cleaning printing plates	Printing shops photography stores
Iodine &	First aid	Drug stores
Sodium Perchlorate	Solidox pellets for cutting torches	Hardware stores

Notes:

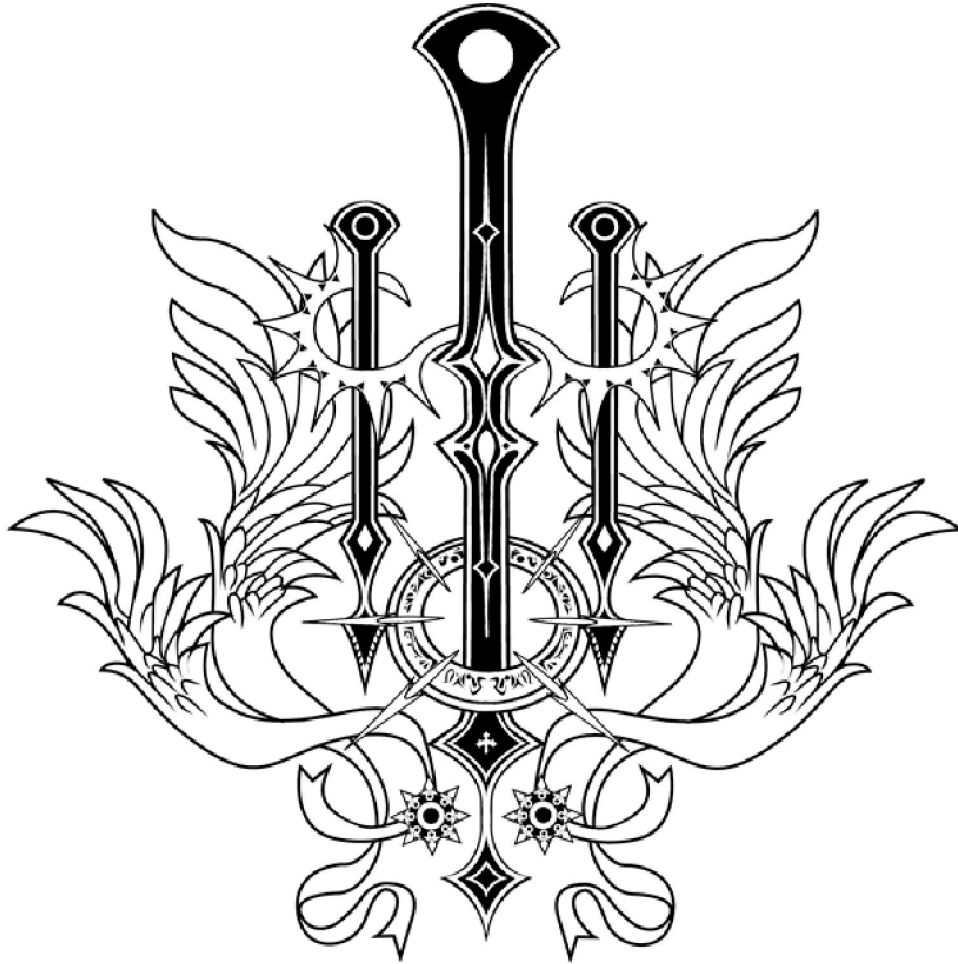
* Ethyl alcohol is mixed with methyl alcohol when it is used as a solvent. Methyl alcohol is very poisonous. Solvent alcohol must be at least 95% ethyl alcohol if it is used to make mercury fulminate. Methyl alcohol may prevent mercury fulminate from forming.

+ Ammonia, when bought in stores comes in a variety of forms. The pine and cloudy ammonias should not be bought; only the clear ammonia should be used to make ammonium triiodide crystals.

@ Mercury thermometers are becoming a rarity, unfortunately. They may be hard to find in most stores. Mercury is also used in mercury switches, which are available at electronics stores. Mercury is a hazardous substance, and should be kept in the thermometer or mercury switch until used. It gives off mercury vapours which will cause brain damage if inhaled. For this reason, it is a good idea not to spill mercury, and to always use it outdoors. Also, do not get it in an open cut; rubber gloves will help prevent this.

^ Nitric acid is very difficult to find nowadays. It is usual stolen by bomb makers, or made by the process described later in this section. The desired concentration for explosive synthesis is about 70%.

& the iodine sold in drug stores is usually not the pure crystalline form that is desired for producing ammonium triiodide crystals. To obtain the pure form, it must usually be acquired by a doctor's prescription, but this can be expensive. Once again, theft is the means that terrorists result to.



Night OPS

Night Ops

This section covers what is known on zoklet and -when it was still around- totse as night ops.

Night ops covers a broad spectrum of general illegalities, as the core aspect of night ops is to break into a place for whatever reason, be it exploration, theft or even just to terrorise people, its can be compared to parkour, only its decidedly more illegal. This section can be applied to many situations covered in the rest of this document.

It is a generally fun topic.

The best way to learn is through experience, but the problem with experience, as all should know, is that the test comes first, and the lesson after. So this section is written to better prepare the less experienced so that they may survive their first basic experiments. And, although this section does deal with some advanced, and unlikely, situations it does cover all important aspects.

Unfortunately this section does require some logic, not all information can be fed to you. For example, equipment is different for all night ops. You need to use your own discretion in these instances. Also knowing when to discard your equipment and what to discard is another example of the use of logic.

In all activities; it's best to be prepared. Plan ahead for all contingencies and double check everything that you have planed for.

Concealment

People are seen for a number of reasons, remembering these vital rules will help you to stay covered at all times;

Shape

Lose your shape, break up the bodies outline and blend in with the surroundings

Shine

Mask any shiny or reflective objects on your person, including the face as sharp features reflect light.

Shadow

Move behind lights when possible. If not move in the shadows, the human shadow is easily distinguished.

Silhouette

The human shape is familiar and stands out. Keep low from sky lines.

Surface

Blend in with the surroundings.

Spacing

When in a group spread out randomly. Nature is not orderly.

Movement

Things are seen especially when they move. Avoid unnecessary movement

Inpo

Inpo, the art of hiding, is an integral part of the ninjitsu system. It simply means that one must take advantage of every possible object, natural as well as man made, to conceal oneself. Inpo gave rise to the legends that the ancient ninja could vanish at will.

Foremost among the precepts of inpo is the admonition to avoid unnecessary movement. Following are the five preferred inpo methods:

EARTH METHOD

The best example of this technique is supplied by Uzura gakure no-jitsu, which suggests hiding like a quail in small gaps between two larger objects.

The primary consideration here is that one must be able to completely fill the space between the objects. In this way, one may escape detection, since an observer will scan past these as he walks. Of note also is the technique of hiding under overhanging brush or grass. Stay low to observe and look around the cover.

AIR METHOD

This refers to hiding like a racoon. It means that one should climb a tree or other high place and press oneself against the object so that one seems to be a part of it.

The infamous jewel thieves, Alan Kuhn and Jack Murphy- who stole the Star of India from a New York museum- made frequent use of this tactic. They believed, and rightly so, that people seldom look up.



WATER METHOD

This means to imitate the actions of the fox by concealing oneself in water. Not only does this aid in erasing one's trail, but also allows only poor footing for the pursuing enemy. This method is also extremely useful when one can spring on an enemy out of the water for the purpose of drowning him.

FIRE METHOD

This is perhaps the most difficult of the inpo arts. It refers to the erasing of sound and shadow. Always move behind a light source to avoid casting a shadow or silhouette which might betray you. Learn to move silently. Only practice in the nine steps can develop this skill.

WOOD METHOD

Pu Neng Mu is the term used to mean "invisibility in plain sight". When no cover is available one must hide behind nothing.

This is accomplished by distorting the silhouette. It is possible to form the body into many shapes by means of yogic exercises. In the old days of ninjitsu, one excellent tactic involved replacing a scare crow and standing in the centre of a ploughed field. By kneeling and wrapping the arms around the knees, one assumes a position like a stone or bush.

Numerous other methods exist for concealing one's presence from the enemy, such as disguises, mingling with crowds, false identities, and so on. These alternatives lie in the realm of strategy, rather than tactical considerations. Conceal items within common items when ever possible. I.e. poison filled syringe in a pen.

Positions of concealment

There are six basic positions which may be used to conceal your presence:

ABOVE- A position above the enemy is the first of these, as mentioned people rarely look up. One may use this propensity to his advantage. Roof tops are a good place of concealment as by laying flat observations can be made. However, avoid silhouetting.

BELOW- One can also hide below people when hiding or observing. Look for crawl spaces, air ducts or cellars. Remember to replace any furniture, barriers etc. that may have been in your way. Beware of being trapped; never move into a space with only one exit.

BESIDE- Beside cover is a third method which may be used. Regardless of the object, keep as low as possible at all times. Use shadows when ever possible- conceal yourself within it and assume the same shape.

BEHIND- Hiding behind cover is another technique. In selecting this approach it important to remember that you must assume the same shape as the object. Shrubs, hedges, crates, stacked material, and so on, may be used for this purpose.

INSIDE- Hiding inside is another method of concealment. The trick is to choose places where a person is not expected to fit. One must possess great flexibility and the ability to remain utterly still. Remember to beware of becoming trapped.

IN FRONT- In front of cover is the boldest and most difficult of all these concealment methods. To accomplish this, one must select the object of concealment, position himself directly before it, and assume its shape. Lower the torso and look directly ahead without fixing the eyes on any one point. Relax the body.

In all of these concealment methods, the primary consideration is no movement. It is of utmost importance in hiding in plain view. These techniques most favoured by the ancient ninja, who would position themselves along a path travelled by the enemy, stepping forward to attack him as he passed.

Note:

Do not look directly at people as this will cause them to sense your presence.

Movement

The Nine Steps

Man sees in three ways, by movement, silhouette, and colour. Man also hears, and some hear more acutely than others. Also, since some people can sense a foreign presence, one must have a calm mind to escape their notice. To elude all these sensory pickups is to be invisible for all practical purposes. To eradicate colour, one employs black art. Black is the absence of colour. This means that a black surface absorbs all of the light rays' incident upon it, reflecting none. It is the reflected rays that give an object its apparent colour. Further a black surface casts no shadow upon itself to define its depth. To erase shadow and sound, one must employ the nine steps detailed next:

1. Black/Stealthily Step

Lower the hips and raise both arms; the feet are turned inwards and one shoulder width apart. The hips are back and the head lowered. The eyes are directed without being fixed at a spot about ten feet ahead. Keeping the upper body still move the right foot in to the left then out and forward in a semi-circle manner, keeping all the weight on the left foot and feeling the ground ahead with the foot for a suitable step. Always keep the arms up and elbows in to protect the body and feel for obstacles. Always direct the Chi (inner/sixth sense) forward.

2. Cross Step

Stand sideways to the direction you wish to go. The lead arm is held middle to low section in front of you ready to steady the body if it should become unbalanced and the rear arm is held up by the head in a ready position. Move all of the body weight onto the front foot then bring the rear foot around in front of the body and place it half a step in front, in the direction you want to go. Then take the front foot, from behind the previous rear foot, and stretch it out as far as possible feeling for a suitable position to place it. The eyes scan the ground about three feet in front. This technique is easily mastered and is extremely efficient for quick, silent movement. When passing a window, or the like, one should listen for sounds before, during and after one has passed the obstacle. Always try and move on the balls of the feet, as this gives faster, smother movements.

3. Night Walking Ability

This is employed when it is necessary to move quietly and quickly forward. Lower the body for better balance, and extend the arms, palm down at waist level. Step forward with the left foot, balancing on the right leg. Place the toes lightly on the ground and shift body weight forward. As you move, press the left heel down gently. Glide forwards, advancing the right foot in a similar manner.

4. Serpent Step

This technique is employed when one needs move close to the ground. Keep the body as flat as possible. The hands are kept palms down, near the face, with elbows close to the body, legs spread, and toes outward. The head is lifted to observe the enemy. To move forward, extend the arms and draw the left leg forward. The weight is borne on the forearms and ankle to knee on the leg, so that the body does not drag on the ground. Change the pushing leg frequently to avoid fatigue. Stop and listen after each movement, silence and slow movement are essential.

Dragon Step

This is a variation of the serpent step. Keep the body free of the ground by resting on the forearms and lower legs. Move forwards by alternately moving the right knee/left elbow and then the left knee/ right elbow. This position is quite vulnerable so use it at distance.

5. Rushing Step

Use this technique when changing cover. From a press up position, bring the right leg up to the chest, the same as a 100m runner. Spring forward and run to the next position keeping low with the arms hanging in front. At the new position silently drop to the knees then to the front of the body and roll into cover.

6. Entering Pivot

This is most effective when turning a corner, i.e. a wall. Press against the wall with the back, resting the weight forward. Place the leading hand by the knee and the rear hand around the body and press it against the wall by the

face. Slowly lean forward and look around the corner. Do this at a fairly low level. Having determined that the move can be accomplished move the head back out of sight. Stretch the leading leg around the corner as far as possible and slide the body around the corner. When the hips have cleared the wall the rear leg is pulled through. Press your back against the wall and check that the movement was not observed.

7. Wall Climbing Ability

To perfect this technique to scale bare or smooth walls requires three years floor work, three years climbing walls with jutting bricks and three years bear wall climbing. Press the body against the wall, getting a feel for the surface material. Look directly upward, selecting a hand hold route you will employ. Grip the ledge, and place the toes on a second ledge. Simultaneously push with the legs and pull with the arms, gaining sufficient momentum to carry your hand to the edge of the wall. Regain balance and go again, moving only one point at a time. Walls may also be advanced with the chest facing, and using drainpipes and trellises, bearing in mind that they are considerably weaker at the top than at the bottom. Always test the object before attempting to scale them. When confronted by a fence topped by barbed wire, three methods may be used to cross the perimeter. First you may climb the barrier, finding ample support for feet and hands near the support poles. When crossing the barbed wire, grasp it at either the support or between the barbs and slowly let yourself over taking care not to get caught on the wire. Drop clear of the fence on the other side executing a forward roll to break the impact, reduce noise and roll to a pre-selected point of concealment. Take care not to touch electrified fences, look for small insulator boxes at intervals and dead animals nearby, but it is unlikely that any electric fences are powerful enough to kill anything.

8. Side Step

This technique is employed when the need to pass an open door or threshold arises. Assume the position as in the 'entering pivot step' (#6) Observe the situations, noting any personnel and their positions. As quickly, and silently as possible, push off with the rear leg stepping clear of the opening and landing on the left leg in one swift motion. On the other side, check once again that the movement was not observed.

9. Lost Track Pivot

Stand with knees slightly bent toes pointing forward, and the body lowered slightly. Pivot on the ball of the right foot while turning toward your right forward corner and step out to your left. You will now be facing 90 degrees from your original position. The instant the left foot touches down, shift the weight to that side and execute another 90 degree pivot, this time to your right rear corner. You now face 180 degrees from your original position.

More Ways to Move

When ascending stairs keep close to the wall and move using the cross step. Alternatively you could use the dragon step to move up the stairs. This spreads out the body weight and pressure and reduces noise while keeping the body's position covered. When confronted by a mirror, treat it as an opening or window passing out side the field of reflection. Observe the position of your shadow as this may give you away.

Moving At Night

Not all of the movement methods are suitable at night. The appropriate method for night movement must be adopted.

* At night you hear more than you see * Stop and listen. Keep close to the ground. * Freeze if you hear a noise.

When moving at night always keep in mind the following things:

- Keep quite
- Don't have loose equipment
- Move carefully Use the appropriate method of moving
- Clear the route do not step on any dry vegetation
- Use available cover
- Flares turn night into day

Listening At Night

Use your ears and turn them towards any sound. Closing the eyes will help to increase the amount of noise that you hear. If there are men about, keep an ear close to the ground or any other dense material such as walls, roads, rail tracks, etc. Sound travels a lot better through denser materials than it does through air.

Night Vision

Humans can see in the dark, however, the eyes take approximately 30 minutes to become used to the dark. At night remember:

- We can see less than in daylight
- We see shapes not detail
- We see skylines and silhouettes
- We may see movement.
- Exposure to bright light will temporarily ruin the eyes night vision. If caught in the light of flares, headlights or other strong sources of light take cover at once (in open ground), freeze (in a wood). If you see a flare, or bright light source, instantly close one eye. This will help to protect the night vision in that eye.

Movement Rules

Follow these general rules to move without being seen or heard by anyone:

- Camouflage yourself and your equipment.
- Wear soft, well-fitting clothes. Starched clothing swishes, baggy clothing is likely to snag.
- Use ankle ties to blouse the trousers. Do not tie them too tightly as this restricts circulation.
- Do not carry unnecessary equipment.
- Look for your next point of concealment before leaving your position.
- Change direction when moving through tall grass; a straight path cause's unnatural motion which attracts attention.
- If you alarm birds or animals, remain in your position and observe. Their flight may attract attention.
- Take advantage of distractions provided by natural noises.
- Cross roads and tracks where maximum cover exists, look for a low spot or curve, cross quickly and silently.
- Follow the furrows when crawling over ploughed land, crossing the furrows at low spots.
- Avoid steep slopes and areas with loose gravel or stone.
- Avoid cleared areas and prevent silhouetting.
- Avoid heavily trafficked areas.
- Avoid areas that are not trafficked at all, they could be mined or booby-trapped.
- Always move downwind from kennels or guard dog positions.
- Observe the enemy as much as possible, watching for indications that you have been discovered.
- When in doubt, don't move.
- Learn the patterns used to see, that you may move outside the field of view.
- Learn to move without disturbing your surroundings.

In these you must research and train diligently.

Physical Security and Intrusion Detection Systems

Introduction

- Physical Security relies on the following ideas to protect a facility:
- Deterrence, Prevention, Detection and Response
- Deterrents are used to 'scare' the intruder out of trying to gain access.
- Prevention tries to stop the intruder from gaining access.
- Detection 'sees' the intruder while attempting to gain access.
- Response tries to stop and/or prevent as much damage or access to a facility as possible after detection.

There are 3 security levels used in this article and in industry to designate a facility's need. They are: Low, Medium, and High. The amount and types of security devices used by a facility are directly proportional to the level of security the facility 'thinks' it needs. This article will be primarily concerned with the protection of the perimeter.

The Perimeter:

A facility's first line of defence against intrusion is its' perimeter. The perimeter may have any or all of the following:

- A single fence
- An interior fence coupled with an exterior fence
- Regular barbed wire
- Rolled barbed wire
- Various fence mounted noise or vibration sensors
- Security lighting and CCTV
- Buried seismic sensors and different photoelectric and microwave systems fences.

Fences are commonly used to protect the perimeter. The most common fence in use today is the cyclone fence, better known as the chain link fence. Fences are used as a deterrent and to prevent passage through the perimeter. Common ways of defeating fences are by cutting, climbing, and lifting. Cutting is not usually recommended for surreptitious entry, since it is easily noticeable. In this article, we will be taking the 'Stealth' approach.



Climbing

Climbing is most commonly done, but if the fence is in plain view, it may not be advisable since you can be seen easily. The higher the fence, the longer it takes to climb. The longer it takes to climb, the longer security has to detect and respond to your actions. Lifting is better since you are closer to the ground, and not as easily spotted, but the fence must be very flexible, or the sand very soft so you can get under the fence quickly and easily. Whenever you see a somewhat 'un-climbable' fence -or one that you simply do not want to climb- you should check the perimeter for large trees with uncut branches hanging over the fence or other objects which will enable you to bypass the fence without ever touching it.

You could use a ladder but you don't want to leave anything behind, especially with your fingerprints on it. Electric fences are not used for security purposes as much as they were in the past. Today its main use is to keep cattle or other animals away from the perimeter, either from the inside or outside. There are devices which send a low voltage current through a fence and can detect a drop in the voltage when someone grabs onto the fence, but again this is not common.

For high security installations, there may be 2 fences, an outer fence and an inner fence which are 4, 5-9 meters apart. It isn't often that you encounter this type of setup; it is mainly used by government agencies and the military. You can be very sure that there are various intrusion detection devices mounted on the fence, buried underground between them, and/or line-of-sight microwave or photoelectric devices used. These will be mentioned later. If you insist on penetrating the perimeter, then you should try to measure how far it is between fences.

Now find a 61 centimetre by X centimetre board where X is the distance between the 2 fences. Very slowly place the board on top of both fences. If there are no fence vibration sensors you can just climb the fence and step onto the board to walk across the top. If there are fence sensors, you will need a ladder which cannot touch the fence to get you on top of the board. You can then walk on the board, over the ground in between, and jump down, being careful not to disturb the fences. This will work if there are no sensors after the 2 fences. Identifying sensors will be mentioned later. Obviously the method of using a long board to put on top of the two fences will not work if the fences are spaced too far apart. Also, you and the board can be seen very easily.

Barbed Wire:

There are two common types of barbed wire in use today. The more common and less secure is the type that is strung horizontally across the fence with three or more rows. The 'barbs' are spaced about 15 centimetres apart, enough for you to put your hand in between while climbing over. Also, it is thin enough to be cut very easily. If you think you will need to leave in a hurry or plan on problem free surreptitious entry and the only way out will be to climb over the fence again you can cut the wire from one post to another, assuming the wire is tied or soldered to each post, and replace it with a plastic wire which looks like the wire you just cut. Tie it to each post, and come back anytime after that. You can then climb over it without being cut.



The other type of wire, which is more secure or harmful, depending on how you look at it, is a rolled, circular wire commonly called Razor Ribbon. One manufacturer of this is the American Fence Co. which calls it 'the mean stuff'. And it is. The barbs are as sharp as razors. Of course this can be cut, but you will need very long bolt cutters and once you cut it, jump as far back as you can to avoid the wire from springing into your face. As mentioned earlier, cutting is irreparable, and obvious. If the wire is loosely looped, there may be sufficient room in between to get through without getting stitches and losing lots of blood. If the wire is more tightly looped you may be able to cover the wire with some tough material such as a leather sheet so you can climb over without getting hurt. This method is not easy to accomplish however. You may want to see if you can get under the fence or jump over rather than climb it.

Fence Mounted Noise or Vibration Sensors:

Let's assume you have found a way to get past the fence. Of course you have not tried this yet, since you should always plan before you act. You are now past the deterrent and prevention stages. Before you put the plan into action you had better check for the things mentioned earlier. If a fence is the first step in security defence, then fence mounted sensors are the second step. The types of detection equipment that can be mounted on the fence are:

Fence shock sensors: These mount on fence posts at intervals of 3 to 6 meters, or on every post. They are small boxes clamped about 2/3 up from ground level. There is a cable, either twisted pair or coax running horizontally across the fence connecting these boxes. The cable can be concealed in conduits or inside the fence itself, thus, making it hard to visually detect. Each fence sensor consists of a seismic shock sensor that detects climbing over, lifting up or cutting through the fence. So if the fence is climbable, it would not be wise to do so since you may be detected. Of course it doesn't matter if you're detected if there is no security force to respond and deter you.

Another type is called the E-Flex cable. It's simply a coax cable running horizontally across the fence. This cable can also be used on concrete block, brick or other solid barriers. It may be on the outside, or mounted inside the fence, thus making detection of the device harder. Of course detection of this and other similar devices which cannot be seen doesn't make it impossible. A way to detect this is by simply repeatedly hitting the wall with a blunt object or by throwing rocks at it. If nothing out of the ordinary happens, then you can be reasonably sure it is not in place. This is basically a vibration sensor.

Low frequency microphones:

This is essentially a coax cable that responds to noise transmitted within the fence itself. Vibration sensors: These are based on mercury switches, a ring or ball on a pin or a ball on a rail. Movement of the fence disturbs the switches and signals alarms. A hint that this is in use is that it can only be used on a securely constructed and tightly mounted fence, with no play or movement in it. Otherwise, the occupant will be getting false alarms ad nauseum.

Now you know all about these types, how do you get around it? Well, don't touch the fence. But if there is no alternative, and you must climb it, then climb the fence where it makes a 90 degree turn (the corner) or at the gate. Climb it very slowly and carefully, and you should be able to get over without being detected by these sensors. Make sure you climb on the largest pipe and don't fall.

Security Lighting and CCTV:

Often times, fences may be backed up by Closed Circuit TV (CCTV) systems to make visual monitoring of the perimeter easier and quicker. By installing an adequate lighting system and conventional CCTV cameras, or by using special low light sensitive cameras, the perimeter can be monitored from a central point. Security personnel can then be dispatched when an intruder is detected on the monitors. Some systems are stationary, and others can be moved to view different areas of the perimeter from within the central station. It would be in your best interest to determine if the camera is stationary or not. If so, you may be able to plan a path which will be out of the view range of the camera. If it is movable,



you will have to take your chances. Light control sensor: This utilizes a Passive Infrared (PIR) sensor to detect the body heat emitted from someone entering the detection area, and can activate a light or other alarm. The sensor has an option called: 'night only mode' in which a light will flash when a person enters the area, but only during night hours. It can tell if it's dark by either a photoelectric sensor, or by a clock. Of course if its daylight savings time (America only), the clock may not be totally accurate, which can be used to your advantage. If it is photoelectric, you can simply place a flashlight pointing directly into the sensor during daylight hours. When it gets dark, the photoelectric sensor will still 'think' its day since there is sufficient light, thus not activating the unit to detect alarm conditions. This should enable you to move within the area at will.

Buried Seismic Sensors and Electronic Field Sensors:

Seismic detectors are designed to identify an intruder by picking up the sound of footsteps or other noises related to passing through the protected area. These sensors have a range of about 6 meters and are buried underground; linked by a cable, which carries their signals to a processor. There, the signals are amplified and equalized to eliminate frequencies that are unrelated to intruder motion. The signals are converted to pulses that are compared with a standard signal threshold. Each pulse that crosses this threshold is tested on count and frequency. If it meets all the criteria for a footstep, an alarm is triggered. These sensors can be installed under asphalt or concrete by cutting a trench through the hard surface. It is also immune to weather and can follow any type of terrain. The only restriction is that the area of detection must be free of any type of obstruction such as a tree or a bush. You cannot see them, but you don't have to. Simply get 3-4 medium sized stones. Throw them into the place where you think the protected area is. Repeat this several times. This works on the lesser advanced systems that have trouble distinguishing this type of seismic activity from a human walking/running. If nothing happens, you can be reasonably sure this is not in use.

Electronic Field Sensors detect an intruder by measuring a change in an electric field. The field sensors use a set of two cables, one with holes cut into the cable shielding to allow the electromagnetic field to 'leak' into the surrounding area. The other cable is a receiver to detect the field and any changes in it. Objects passing through the field distort it, triggering an alarm. This sensor can either be buried or free-standing and can follow any type of terrain. But it's very sensitive to animals, birds, or wind blown debris, thus, if it is very windy out, and you know this is being used; you can get some paper and throw it so the wind takes it and sets off the alarm repeatedly. If it is done enough, they may temporarily turn it off, or ignore it due to excessive false alarms. It is not hard to tell if these devices are in use.

Now that you can detect it, how do you defeat it? As far as the electronic field sensor is concerned, you should wait for a windy night and cause excessive false alarms and hope they will turn it off.

As far as the seismic sensors, you can take it one step at a time, very softly, maybe one step every 30-60 seconds. These sensors have a threshold of, for example, two or more consecutive footsteps in a 30 second time interval will trigger the alarm. Simply take in one step at a time, slowly, and wait, then take another step, wait, until you reach your destination. These detectors work on the assumption that the intruder has no knowledge of the device, and will walk/run across the protected area, thus causing considerable seismic vibrations. The problem with this method is that it will take you some time to pass through the protected area. This means there is more of a chance that you will be seen. If there are a lot of people going in and out of the facility, you may not want to use this method. Another way would be to run across the protected area, right next to the door, (assuming that is where the response team will come out) and drop a large cat or a dog there. When they come out, they will hopefully blame the alarm on the animal. The sensor shouldn't really pick up a smaller animal, but odds are the security force are contract guards who wouldn't know the capabilities of the device and the blame would fall on the animal and not you, assuming there were no cameras watching.

Microwave Systems:

In an outdoor microwave system, a beam of microwave energy is sent from a transmitter to a receiver in a conical pattern. Unlike indoor microwave detectors, which detect an intruders' movement in the microwave field, the outdoor system reacts to an intruders' presence by detecting the decrease in energy in the beam. The beams can protect an area up to 1500 feet long and 40 feet wide. All transmission is line-of-sight and the area between transmitter and receiver should be kept clear of trees and other objects that can block the beam. Microwave systems can operate in bad weather, and won't signal an alarm due to birds or flying debris. These systems work on the Doppler Effect, in which they detect motion that changes the energy, and sets off an alarm. These devices will usually be placed inside a fence to avoid false alarms. These devices are very easy to visually detect. They are posts from 1-2 meters high, about 15 centimetres by 15 centimetres and there are 2 of them, one receiver and one transmitter. In some cases there will be more, which enables them to protect a larger area. To defeat this, you can enter the field, very slowly, taking one step at a time but each step should be as if you are in slow motion. It doesn't matter how hard you hit the ground, since it doesn't detect seismic activity, only how fast you approach the field. If you take it very slowly you may be able to get past.

Detectors of this type get more and more sensitive as you approach the posts. Ergo, choose a path which will lead you furthest away from the posts.

Photoelectric Systems:

These systems rely on an invisible barrier created by beams of infrared light sent from a light source to a receiver. When the beam is interrupted, the alarm sounds. The beam can have an effective range of up to 153 meters. Multiple beams can be used to increase the effectiveness of the system, making it harder for you to climb over or crawl under the beams. Photoelectric systems can be prone to false alarms as a result of birds or wind-blown debris passing through the beam. The problem can be corrected by the installation of a circuit that requires the beam to be broken for a specified amount of time before an alarm is sounded. Weather conditions like heavy fog, can also interrupt the beam and cause an alarm. This can also be corrected by a circuit that reacts to gradual signal loss. These systems should not face directly into the rising or setting sun since this also cuts off the signal beam. As you can see this system has many problems, of which you can take advantage of to bypass it. As with any system and method; surveillance of the facility should be accomplished in various weather conditions to help verify the existence of a particular detection device and to see how they react to false alarms. Many times you will be able to take advantage of various conditions to accomplish your mission. If there is only one set of devices (transmitter and receiver), try to estimate the distance of the sensors from the ground. You can then either crawl under or jump over the beam. This also works on the assumption that the intruder will not recognize that the device is in use.



Miscellaneous

Guards: There are two types, in-house or company paid guards and contract guards. Contract guards are less secure since they do not work for the facility and if they make a mistake they simply get transferred to another facility, no real problem. In-house guards know the facility better and have more to lose; thus they are probably more security conscious. Be aware of any paths around the perimeter in which guards can/will walk/ride to visually inspect the exterior of the facility.

Central monitoring: Monitoring of the devices mentioned in this article is usually accomplished at a 'Central Station' within the facility. Usually, guards should be monitoring these. If you have planned well enough, you may find that the guard leaves his/her post to do various things at the same time every night. This would be an ideal time to do anything that may be seen by cameras. Unfortunately, there will probably be more than one guard, making this nearly impossible.

Gates: Probably the easiest way to pass through the perimeter is to go through the gate. Whether by car or foot, this may not be too easy if it is guarded or if there is a card reading device used for entry.

Exterior card readers: For now, if the card used is magnetic (not Weygand) it is quite possible to attack it. If you have an ATM card, Visa, or other magnetic card, slide the card through, jiggle & wiggle it, etc. and quite possibly the gate will open. Reasons for this are that since it is outside the reader is subjected to extreme weather conditions day in and day out, thus the detecting heads may not be in the best of shape, or since it is outside it may be a cheap reader. In either case it may not work as well as it should and can make 'mistakes' to allow you access.

Combinations: The devices listed in this article do not have to be used alone. They can and are used in conjunction with each other for greater security.

Diversions

In some cases, a diversion could better insure your passage through the perimeter. Keep this in mind.

Extreme weather conditions:

All devices have an effective operating range of temperatures. On the low end of the scale, most devices will not operate if it is -34 degrees Celsius or lower. Though, quite a few will not operate effectively under the following temperatures: -25° C, -20° C, -12° C, and 0° C. On the other side of the scale, they will not operate in excess of: 48°C, 54° C and 65° C. It is unlikely that the outside temperature will be above 48 degrees, but in many places, it may be below freezing. Take this into consideration if a facility has these devices, and you cannot bypass them any other way.

It was not possible to mention everything used in perimeter protection in this article, although the most common methods were dealt with.

Alarms and Security Keypads:

This text will describe how to bypass an alarm or to bypass a security keypad. If the alarm is one of the older versions where a loud bell or horn rings to draw attention to the location you are at then you can simply fill the horn or bell with polyurethane foam to silence them. You can purchase this at any hardware store as insulation. It is easy to handle and dries faster. Once the foam is in place the bell or horn will not be able to produce sound and so the security system may still be active, but nothing comes of it. Some high-security installations use keypads just like touch-tone pads (a registered trade mark of bell systems) to open locks or disarm alarms. Most use three or four digits. To figure out the code, wipe the key-pad free from all fingerprints by using a rag soaked in rubbing alcohol. After the keypad has been used just apply finger print dust and all four digits will be marked. Now all you have to do is figure out the order. The best way to figure out the order is to look for some sort of pattern. Following the following examples you should be able to ascertain what the combination is: 7 8 9 4 5 6 1 2 3 * 0 # usually there will be four different numbers like 7,5,3,0. If those happened to be the four numbers then the obvious pattern would be 7,5,3,0 because they form a line diagonal. The same holds true for the patters like 9,5,1,0. There is almost always a pattern to the way that the owner of the system has used to make it easier to remember.

Two things you have to look out for. The first is that you can only have so many wrong inputs before the system triggers. Also, sometimes even though you may disarm the system, after a certain number of wrong answers a security guard will come by to make sure everything is OK. The second thing is that after you dust for prints you may only find 3 numbers. However, the combination may be 4 numbers with one repeating. If this is the case, try to look for a digit that has a slightly smudged or shadowed finger print on it. With 4 numbers, each being used once there are 24 different combinations. Follow the example using the numbers 1,2,3,4

1 2 3 4 2 1 3 4 3 1 2 4 4 1 2 3 1 2 4 3 2 1 4 3 3 1 4 2 4 1 3 2 1 3 2 4 2 3 1 4 3 2 1 4 4 2 1 3 1 3 4 2 2 3 4 1 3 2 4 1 4 2
3 1 1 4 2 3 2 4 1 3 3 4 1 2 4 3 1 2 1 4 3 2 2 4 3 1 3 4 2 1 4 3 2 1

However, if there are only 3 numbers in a four pin combination the amount of different combinations jumps from 24 to 33. For an explanation follow the example using numbers 0,1,2

0 0 1 2 1 1 0 2 2 2 1 0 0 0 2 1 1 1 2 0 2 2 0 1 0 1 0 2 1 0 1 2 2 1 2 0 0 1 2 0 1 0 2 1 2 1 0 2 0 2 0 1 1 2 1 0 2 0 2 1 0 2
1 0 1 2 0 1 2 0 1 2 1 0 0 2 0 1 1 2 1 2 2 0 1 0 2 0 0 1 2 1 1 2 0 2 1 2 0 0 0 2 1 1 1 0 2 2 2 0 0 1 2 1 1 0 0 2 2 1 2 1 0 0
2 0 1 1 0 1 2 2

Many units have a panic button, this can be activated by pressing the * and # keys on the keypad at the same time.

Note: Never try to remove these panels from the wall, as they have built-in tamper switches.

Police call radio guide

* PHONETIC ALPHABETS *

- A-ALPHA
- B-BRAVO
- C-CHARLIE
- D-DELTA
- E-ECHO
- F-FOXTROT
- G-GOLF
- H-HOTEL
- I-INDIA
- J-JULIETTE
- K-KILO
- L-LIMA
- M-MIKE
- N-NOVEMBER
- O-OSCAR
- Q-QUEBEC
- P-PAPA
- R-ROMEO
- S-SIERRA
- T-TANGO
- U-UNIFORM
- V-VICTOR
- W-WHISKEY
- X-X RAY
- Y-YANKEE
- Z-ZULU

- A-ADAM
- B-BOY
- C-CHARLES
- D-DAVID
- E-EDWARD
- F-FRANK
- G-GEORGE
- H-HENRY
- I-IDA
- J-JOHN
- K-KING
- L-LINCOLN
- M-MARY
- N-NORA
- O-OCEAN
- P-PAUL
- Q-QUEEN
- R-ROBERT
- S-SAM
- T-TOM
- U-UNION
- V-VICTOR
- W-WILLIAM
- X-X RAY
- Y-YOUNG

- Z-ZEBRA

*** DECODE SECTION ***

- 10-1 RECEIVING POORLY
- 10-2 RECEIVING WELL
- 10-3 STOP TRANSMITTING
- 10-4 OK or ACKNOWLEDGEMENT
- 10-5 RELAY
- 10-6 BUSY
- 10-7 OUT OF SERVICE
- 10-7B OUT OF SERVICE AT HOME
- 10-8 IN SERVICE
- 10-9 REPEAT
- 10-10 OUT OF SERVICE SUBJECT TO CALL
- 10-11 TRANSMITTING TO RAPIDLY
- 10-12 OFFICIALS OR VISITORS PRESENT
- 10-13 WEATHER OR ROAD CONDITIONS
- 10-14 ESCORT OR CONVOY
- 10-15 EN ROUTE WITH PRISONER
- 10-16 PICK UP PRISONER
- 10-17 PICK UP PAPERS
- 10-18 COMPLETE PRESENT ASSIGNMENT A.S.A.P
- 10-19 RETURN OR RETURNING TO STATION
- 10-20 WHAT IS YOUR LOCATION?
- 10-21 CALL YOUR STATION OR DISPATCHER BY TELEPHONE
- 10-21A ADVISE MY HOME I WILL RETURN AT _____.
- 10-21B CALL YOUR HOME BY TELEPHONE
- 10-21T REPLY BY TELEPHONE
- 10-22 CANCEL LAST MESSAGE OR ASSIGNMENT
- 10-23 STANDBY
- 10-25 DO YOU HAVE CONTACT WITH _____?
- 10-27 CHECK "MCAPS" COMPUTER FOR WARRANTS
- 10-28 REGISTRATION REQUEST
- 10-28C CHANGE IN OWNERSHIP-CONTACT DMV
- 10-29 CHECK FOR STOLEN OR WANTED
- 10-30 NO RECORD OR WANTS YOUR SUBJECT
- 10-31 SUBJECT HAS RECORD BUT NO WANTS
- 10-32 SUBJECT WANTED.ARE YOU CLEAR TO COPY?
- 10-33 STANDBY.EMERGENCY TRAFFIC ONLY
- 10-34 RESUME NORMAL RADIO TRAFFIC
- 10-35 CONFIDENTIAL INFORMATION
- 10-36 CORRECT TIME
- 10-37 NAME OF OPERATOR ON DUTY
- 10-39 MESSAGE DELIVERED
- 10-40 IS _____ AVAILABLE FOR TELEPHONE CALL?
- 10-40A IS _____ AVAILABLE FOR RADIO CALL?
- 10-42 PICK UP OFFICER
- 10-45 SERVICE YOUR EQUIPMENT
- 10-46 STANDBY, I AM PROCEEDING TO A BETTER LOCATION
- 10-48 I AM NOW READY TO TAKE INFORMATION
- 10-49 PROCEED TO _____
- 10-86 TRAFFIC CHECK-DO YOU HAVE TRAFFIC FOR THIS UNIT?
- 10-87 MEET _____ AT _____

- 10-88 WHAT PHONE NUMBER SHALL WE CALL TO MAKE STATION TO STATION CALL?
- 10-96 REQUEST TEST OF SELECTIVE CALL EQUIPMENT
- 10-97 ARRIVED AT SCENE
- 10-98 FINISHED LAST ASSIGNMENT

- 11350 POSSESSION OF DANGEROUS DRUGS OR HEROIN
- 11357 POSSESSION OF MARIJUANA
- 187 MURDER
- 207 KIDNAPPING
- 207A ATTEMPT KIDNAPPING
- 211 ROBBERY
- 211S ROBBERY-SILENT ALARM
- 217 ATTEMPT MURDER
- 220 ATTEMPT RAPE
- 240 MISDEMEANOR ASSAULT
- 242 BATTERY
- 245 ASSAULT WITH DEADLY WEAPON
- 261 RAPE
- 288 LEWD AND LASCIVIOUS CONDUCT
- 314 INDECENT EXPOSURE
- 390 DRUNK
- 390C DRUNK IN AUTO
- 390D DRUNK DOWN
- 415 DISTURBING THE PEACE
- 415A DISTURBING THE PEACE - AUTO/S INVOLVED
- 415E DISTURBING THE PEACE - MUSIC OR PARTY
- 415F DISTURBING THE PEACE - FAMILY
- 415G DISTURBING THE PEACE - GANG
- 415M DISTURBING THE PEACE - MECHANICAL OR MISCELLANEOUS
- 417 MAN WITH A GUN
- 447 ARSON
- 459 BURGLAR ALARM
- 459A BURGLAR ALARM AUDIBLE
- 459S BURGLAR ALARM SILENT
- 480 HIT & RUN FELONY
- 481 HIT & RUN MISDEMEANOR
- 483 HIT & RUN PARKED VEHICLE
- 484 THEFT/LARCENY
- 487 GRAND THEFT
- 488 PETTY THEFT
- 502 DRUNK DRIVER
- 503 STOLEN CAR/MOTORBIKE/MOTORSCOOTER/BOAT
- 504 CAR TAMPERING OR STRIPPING
- 505A RECKLESS DRIVER/DRIVING
- 510 SPEEDING OR RACING VEHICLE
- 586 ILLEGAL PARKING
- 594 MALICIOUS MISCHIEF
- 901 TRAFFIC ACCIDENT, UNKNOWN IF INJURY
- 901K AMBULANCE DISPATCHED
- 901N AMBULANCE NEEDED
- 901Y IS AMBULANCE NEEDED?
- 901T INJURY TRAFFIC ACCIDENT
- 902 ACCIDENT, NON TRAFFIC
- 902H EN ROUTE HOSPITAL

- 902M MEDICAL AID
- 902T NON INJURY TRAFFIC ACCIDENT
- 903 PLANE CRASH
- 903L LOW FLYING PLANE
- 904 FIRE
- 904A FIRE ALARM
- 904B BOAT FIRE
- 904C CAR FIRE
- 904G GRASS FIRE
- 904I ILLEGAL FIRE OR INCENDIARY
- 904M TRASH FIRE
- 904S STRUCTURAL FIRE
- 904T ANIMAL INFORMATION
- 905B ANIMAL BITE
- 905D ANIMAL DEAD
- 905H ANIMAL IN HEAT
- 905I ANIMAL INJURED
- 905R RABIES SUSPECT
- 905L LOOSE STOCK
- 905N ANIMAL NOISE
- 905S STRAY DOG OR CAT RESCUE
- 906N RESCUE UNIT NEEDED
- 906K RESCUE UNIT DISPATCHED
- 907N PARAMEDIC TEAM NEEDED
- 907K PARAMEDIC TEAM DISPATCHED
- 907Y IS PARAMEDIC TEAM NEEDED?
- 909 TRAFFIC INFORMATION
- 909C TRAFFIC CONGESTION/CONTROL
- 909F TRAFFIC FLARES NEEDED
- 909T TRAFFIC HAZARD
- 910 CAN HANDLE CALL
- 911B CONTACT THE OFFICER
- 912 ARE WE CLEAR TO/FOR _____?
- 913 YOU ARE CLEAR TO/FOR _____?
- 914A ATTEMPT SUICIDE
- 914C CORONOR NEEDED
- 914D DOCTOR NEEDED
- 914H HEART ATTACK
- 914S SUICIDE
- 917A ABANDONED VEHICLE
- 918 MENTAL CASE (SAME AS 5150)
- 918V VIOLENT MENTAL CASE
- 919 KEEP THE PEACE
- 920A MISSING ADULT (18 OR OLDER)
- 920C MISSING CHILD (13 AND YOUNGER)
- 920J MISSING JUVENILE (14 TO 17)
- 920F FOUND CHILD
- 921 PROWLER
- 922 ILLEGAL PEDDLING
- 924 STATION DETAIL
- 924D STATION DETAIL/DESK
- 924F FOOD FOR PRISONERS
- 924R RETURN TO STATION TO FILE
- 925 SUSPICIOUS PERSON

- 925C SUSPICIOUS PERSON IN CAR
- 925V SUSPICIOUS VEHICLE
- 926 TOW TRUCK NEEDED
- 926A TOW TRUCK DISPATCHED
- 927 UNKNOWN TROUBLE
- 927D INVESTIGATE DEAD BODY
- 928 FOUND PROPERTY
- 928B FOUND BICYCLE
- 929 INVESTIGATE PERSON DOWN
- 930 SEE THE MAN
- 931 SEE THE WOMAN
- 932 OPEN DOOR
- 933 OPEN WINDOW
- 949 GASOLINE SPILL
- 950 BURNING PERMIT
- 951 NEED FIRE INVESTIGATOR
- 952 REPORT ON CONDITIONS
- 953 CHECK SMOKE
- 954 OFF THE AIR AT SCENE
- 955 FIRE UNDER CONTROL
- 956 ASSIGNMENT UNFINISHED BUT AVAILABLE FOR DISPATCH TO ANOTHER ASSIGNMENT
- 957 FIRE OUT ON ARRIVAL
- 960 CAR STOP, REQUEST FOLLOWUP
- 960X CAR STOP, EXPEDITE FOLLOWUP, DANGEROUS SUSPECTS
- 961 CAR STOP, NO FOLLOWUP NEEDED
- 962 SUBJECT ARMED AND DANGEROUS. ARE YOU CLEAR TO COPY?
- 965 TAB FOR INTELLIGENCE UNIT. FULL FI
- 966 SNIPER ACTIVITY
- 967 OUTLAW MOTORCYCLE MOVEMENT
- 968 REQUEST RECORD CHECK OF A PERSON
- 970 ILLEGAL SURFING
- 971 BOAT OVER
- 972 BOAT SPEEDING
- 973 SWIMMER ON BOAT
- 974 BOAT ADRIFT
- 975 WRECKAGE ADRIFT
- 976 OIL SLICK
- 977 CHECK MOORING LINE
- 978 VESSEL AGROUND
- 979 VESSEL SINKING
- 980 RADIOACTIVE MATERIALS PRESENT OR INVOLVED
- 981 NEED RADIOLOGICAL MONITORING TEAM
- 982 BOMB THREAT AT _____
- 983 EXPLOSION AT _____
- 995 RIOT OR MAJOR DISTURBANCE
- 997 OFFICER NEEDS ASSISTANCE FROM OWN AGENCY UNITS ONLY. URGENT
- 998 OFFICER INVOLVED IN GUN BATTLE
- 999 OFFICER NEEDS HELP, ANY UNITS RESPOND. EMERGENCY.

*** HANDLE CODES ***

NO CODE HANDLE CALL IN ROTATION

CODE 1: ROUTINE. TAKE THIS CALL NEXT

CODE 2: URGENT. EXPEDITE, BUT OBEY ALL TRAFFIC LAWS. NO RED LIGHTS/SIREN.

CODE 3: EMERGENCY, PROCEED IMMEDIATELY USING RED LIGHT AND SIREN.

CODE 4: NO FURTHER ASSISTANCE NEEDED

CODE 4A: NO FURTHER ASSISTANCE NEEDED, SUSPECT AT LARGE IN AREA.

CODE 5: STAKE OUT. OTHER UNITS STAY AWAY UNLESS ORDERED THERE IN RESPONSE TO CALL.

CODE 6: OUT FOR INVESTIGATION

CODE 7: OUT OF SERVICE TO EAT

CODE 7B: OUT OF SERVICE TO EAT AT HOME

CODE 8: FIRE BOX PULLED

CODE 9: JAIL BREAK

CODE 12: PATROL YOUR ASSIGNED DISTRICT AND REPORT EXTENT OF DISASTER DAMAGE.

CODE 13: ACTIVATE MAJOR DISASTER PLAN TO PERFORM MAJOR DISASTERS DUTIES.

CODE 14: RESUME NORMAL OPERATIONS (USED ONLY WITH A CODE 12 OR CODE 13)

CODE 20: NOTIFY NEWS MEDIA

CODE 20D: REQUEST DEPARTMENTAL PHOTOGRAPHER.

CODE 99: EMERGENCY SITUATION. EMERGENCY BUTTON IN MOBILE UNIT HAS BEEN DEPRESSED. NO VOICE CONTACT.

Lying Methodology

At numerous times, you will be confronted with a situation in which you will need to lie or bend the truth in order to preserve information. The best way to lie is to tell the truth. When asked if you've been smoking drugs in the house, answer 'yeah of course I have. And I throw the butt out the window so you wouldn't know'. This must said in a sarcastic manner. If they question you again, reply, 'Do you really think I have?' If asked again - 'If you think I did then I have already been convicted and whatever I say will not change your opinion'. This way you avoid the question. And because you are in fact telling the truth, you cannot be accused of lying in the future if the subject comes to light again. However, it must be stressed that this method should never be used against authorities such as the police. They will take everything at face value. The main points to be stressed are that, when wishing to keep the truth, one should always act naturally, both in attitude and body posture. A lie can be detected when the subject becomes defensive. This can include a strong, demanding manner of speaking, and a defence body position such as crossing the arms. Eye contact should be kept at all times. However, if the subject is known to lack confidence and rarely make eye contact, this should not be invoked; the natural, daily manner should be adopted. Likewise, the eye contact should not be piercing and demanding itself. Simply just looking at the questioner will provide the desired result. You should aim the point of eye contact between the eyes of the questioner. This provides the contact the questioner is looking for and reduces the ability of the questioner analyzing the subject as no direct eye contact is being giving. This method also provides a more relaxed state for you.

Movement is also a give away to a lie. Fidgeting, rocking and playing with body parts, such as the fingers, face, hair, etc. Project a sense of nervousness which can also be connected to guilt. Having said this, the subject, by no means, should keep excessively still, or in a stiff posture. You should remain calm and relaxed at all times. This will aid in the natural flow of the answers rather than a nervous approach.

Many figures of authority will back up their own statements with false accounts in order to gain the truth. The subject should also back up the statements used. The closer to the truth they are the better they will work. You should always approach the situation as though they are the only one involved in a particular incident. If the questioner refers to 'statements' made by your colleagues you should disregard any of these statements as they are more often a fabrication in themselves. Likewise, any apparent 'witnesses' to the events should also be considered fabrications. This is an attempt to instil doubt into the subjects mind, and once this has settled in the questioner can break it down to the truth. Another method used by authorities is to raise their voice, threaten and otherwise instil fear into the subject. You should remain calm and relax and dismiss any such approach. At no point should you become irritated or loose control as this is the point at which mistakes, confusion and errors are made.

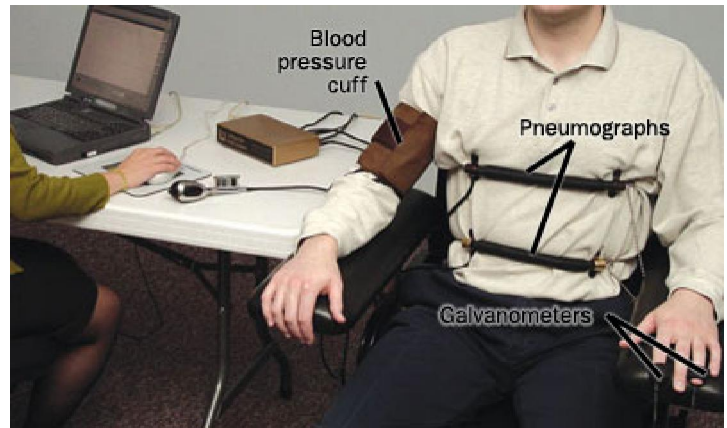
In order for the questioner to believe what the subject is saying, the subject must come across in a convincing, confident and believable manner. There must, however, be no cockiness projected at any time by you. For this to be executed successfully, you must, also, believe what they are saying. This means that even when the questioner demands the subject is wrong, they must stand their ground and demand, in return, that they are right. As soon as the slightest amount of doubt falls on either party, they have lost. If an awkward question is asked, you must have the ability to improvise in a very short amount of time. This can often be aided by a slow answer explaining the difficulty in answering the question. This will provide the subject with more time in which to come up with the answer. Other aids in providing an answer to a difficult question can be by the use of objects in the room; these will provide cues to which you can base the answer upon. The full recollection of events should complement each other. Extra points that were not mentioned before should not be added in at a latter date as this will project a sense of fabrication towards the questioner. The recollection should also never change. Changes in the 'story' can be easily picked up by most people who will then question that fact by cross-referencing it with previous statements. This will result in a poor reasoning, and cast a lot of suspicion over the subject. A well used method is to base the fabrication on an actual event. This way the answers will be provided in a much clearer manner as the event truly took place and will you in providing a false account as the events took place in your mind. Therefore, to you, the statements are not in fact false.

Another well used method, for the purpose of fabrication, is to answer a question with a question. This may not be a direct question but an attempt to avoid answering the original question. Above all, the subject must remain calm, relaxed and believe in what they are saying.

Lie detector tests

When you are subjected to a lie detector, they are measuring your physical responses to psychological stimuli. It's something like watching you to see if you blush. There are four levels they can measure.

1. Your response when you are just sitting there, not being asked anything.
2. Your response when you are asked a question you would have no reason to lie about. "What is your name?"
3. Your response when asked a question they consider personal or embarrassing to most people. "Have you ever wondered what it would be like to have sex with your mother?" only the government would have enough nerve to actually ask this.
4. Your response to the questions they suspect you might lie about.



What they are looking for is whether your #4 responses are closer to #2 or #3, and if the difference is significant with respect to #1.

-If your response level to #3 is much higher than any of the others, you are clearly telling the truth about #4.

-If your responses to #1, #2, and #4 are low, and #3 is high, they think you are telling the truth.

-If your responses to #1, #2, #3, and #4 are all the same, they think that you are either a psychopath or extremely well-adjusted and telling the truth.

-If your responses to #1 and #2 are low but #3 and #4 are high, they think you are lying.

-If your responses to #2, #3, and #4 are high, they think you are very nervous and they call the result "inconclusive."

This last result is easiest for most people to fabricate. You would simply need to think about something embarrassing each time they ask a question. You must not relax, except between questions. A more risky alternative would be to try to relax during the questions you're going to lie about, but not during the "embarrassing" questions. If successful, this would produce the "normal truth" result they prefer to see most. If it failed, it would give the "lie" result. If you take some form of tranquilizer beforehand, you may be able to relax enough to get the "psychopath" response. This can be achieved by emptying out a dissolvable plastic shelled medication tablet such as a paracetamol. This could then be filled with marijuana, diazepam or similar tranquilizer. The capsule would then be reconstructed and taken shortly before the lie detection test is due to begin.

One practice method would be to wire your self to an ohmmeter. One wire wrapped around the left index finger, the other wrapped around the right. If the reading drops from (for example) 100 K-Ohms to a third of that, a lie has just been recorded. You should practice lying through these means to become skilled.

However, the best method to pass a lie detector test is to not have to take one at all. Normally if the authorities want you to take a lie detector test, then will want you to sign a piece of paper saying they are not responsible for anything that happens to you (i.e. electric shocks from sweating, internal physiological damage, etc.) However, if you believe that a lie detector test request is immanent, writing up a form saying that they are most defiantly responsible for anything that happens to you and inserting a large figure of money will usually result in the lie detector test being dismissed. This is due to the fact that they have you sign a release form; this means that people in the past have been subjected to damage of some way and sued the test administrators. Therefore, if you hold them responsible the chances are that you will not be asked to take the test.

Another way to beat a lie detector test is to believe in what you are saying. People who are compulsive liar can beat lie detectors with little effort, because in their own mind everything they say is the truth to them. This is the mind set you must get into if they are going to beat the test.

"Chicago is the capital of the United States."

That is false, but can be answered yes on a lie detector test and have it come up as the truth, because in the mind it is believed that Chicago is the capital of the United States.

Another method is to be completely at ease when you are taking the test. Control your breathing and take the same amount of time in between each question. A good method is to inhale twice and exhale twice before answering each question. Another way to do this is to count back from four each time you are going answer. This allows you to concentrate on the counting of numbers before you answer the question.

Remember, you know what you have done, so don't be surprised when they ask you something regarding that event. That will be coming, so must be expected.

When a lie detector test is given, they will need to establish a base line, to gauge the rest of the questions off of. Normally they will need one truth and one lie. They will ask you "Is XXX your name," and "Are you from Mars". You will need to answer yes to both questions. One good method to displace the baseline is to load the "yes" question. Asking your name is 95 times out of 100 what will be asked. A good way to make sure they can't use this on your baseline is believe your name is something other than what they will ask. For instance, if they ask your name, i.e. Peter Brown You can add something to your name like Peter Browning. That way when they ask you 'is this your name', and you say yes (You will be required to say yes) you are actually lying to them. If you lie, they can not establish a baseline. They do not know you are lying so they establish the baseline off of this. The results after such a test are extremely confused and it is extremely difficult to decipher it.

The Art of Escaping

For the most part, the escape route should be the same as the penetration route. It should be retraced stealthily, as if one were entering instead of leaving; indeed, this is penetration outwards. The reason for using the same route is that it is less likely to be discovered. Also, since the route has been used once, it is far more familiar. Great care must be taken not to let ones guard down during escaping.

No one can plan for all contingencies, but one can try. To this end, at least two other escape routes should be available, one directly opposite and the other veering ninety degrees from the original path. These are to be employed in the event of the primary routes discovery.

In selecting the primary route, seek a means to employ stealth. In selecting alternatives, look first for means to employ speed and cover. Second look for areas where distractions can be created. If possible, locate and prepare an escape route from the guardhouse for use in case of capture. Bear in mind that when being pursued, it may be necessary to stand and fight. Select points along the way that have advantageous high ground. In short, any spot where the enemy will be hampered by obstacles can be used to ones advantage.

Crashing Out

The first principle of escaping is to do it as quickly as possible. The longer you remain in enemy control, the less likely you are to escape. Should you be discovered or captured in will be necessary to consider crashing out.

Locked doors which open outwards may be kicked open using a side or stamp kick. Direct the force at the door jamb with the bolt.

The shoulder can also be used to pass through locked doors. When striking with the shoulder, apply pressure as near the centre as possible. This will bend the door, pulling the lock away from the frame springing it open. Doors with panels will shatter, causing you to fall forward. It is necessary to execute a forward roll out to avoid losing momentum. Striking with the shoulder may also be used against flimsy doors which open inward. To accomplish this feat requires a short running start to gain momentum and impact.



A third possibility is closed windows. Again it is essential to execute a forward roll on impact to avoid injury and maintain momentum. In the case of diving out, you will land on your hands which will collapse allowing the shoulders to take the brunt of the impact.

Diving through windows is not recommended, though it may be necessary if it cannot be compromised. In this event you should cross both arms over the head, to protect it, and dive forward. Extend the arms to break your fall once clear of the window, not before. Sufficient momentum must be generated to clear the window sill, as jagged glass in the frame will slash you. NEVER dive through large windows. The upper portion will fall and spear you before you can clear the space. In this case break the window first and then make your escape.

Drop Toe Hold

The following is employed when one is detained in the military frisk position.

(Enemy coming from left)- Note that the enemy hooks your leg with his left leg ready to sweep you should you resist. His left hand presses your back, locking his vertebrae and causing him to lift his pistol over his arm.

As pressure is applied to your back, tuck your arms in and twist to your left rear. Break this fall by seizing the enemy's right wrist, pulling him forward and turning the weapon to the outside. Fall on to your left hip, whilst driving your left knee behind his left knee. Catch his left ankle with the crotch of your right knee. Performing the classic scissor take down. Drive your right palm up into his left hip socket. Watch the weapon as he may accidentally get off a shot.

Pull down and push up with your hands. Swing the enemy's body weight to the right slamming him into the wall, car .etc.

This technique must be executed with blinding speed.

Handcuff Switch

The enemy moves in and orders your hands atop your head. He moves into position behind you and reaches up to take your right arm into a hammer lock, needed to put on the cuffs.

The enemy pulls your arm behind your back. This is the best moment to attack since he has to either reach for his cuffs or holster his weapon. His attention will be distracted.

Step to the right with your foot, pivoting on the ball of the right foot, and reversing the enemy's wrist lock by lifting it over your head and seizing his arm. Slap the enemy weapon to the outside with left hand by crossing the body. This is known as a cross push block. If he has holstered his weapon, strike him in the rib cage as you turn.

Slide-step using your right foot to a position even with the enemy's. Step to his rear with your left foot, maintaining your grip on his wrist. Pull downward in a semi-circular arc with your right hand twisting the enemy's right arm into the hammer lock. Seize the enemy's left wrist from behind to prevent his executing a similar reverse.

Tearing Off the Finger

Whilst facing-off with the enemy, slap down with the right hand, clamping the pistol. Be sure that the web of the hand falls between the hammer and the firing pin, to prevent discharging a round, and the weapon must be deflected down and to the left side. Berettas and the like also cease to work when the top slide is pushed back, with revolvers, holding the cylinder prevents it from turning and therefore firing.

Having grasped the pistol twist the barrel back toward the enemy trapping his finger in the trigger guard. If the enemy resists, which is probable, step back and pull down with the hands. The finger will dislocate at the knuckle and the finger can easily be torn off using the metal edges of the trigger guard.

Escape from a Headlock

From a right side head lock; Pinch the ulna or radial nerve in the enemy's wrist to slightly release his grip. Turn to the enemy body. Reach up from behind with the left arm and clamp your hand over the enemy's mouth. Ensuring the top edge pushes into the philtrum, just below the nose, causing great pain should he resist, Step out and forward with your right leg, pivoting around and pulling the enemy round to the left. Drop to the right knee keeping the left knee pointed up drop the enemy down pulling his head past the knee. This will break his back and sometimes cause instant death.



Standing Switch

Should the enemy seize you about the waist in seeking to capture you, it's possible to reverse positions with him or escape by employing the standing switch.

As the waist cinch is secured, drive your left arm down along the inside of the enemy's knee. This locks his elbow between your hip and triceps. Toe-out with the left foot and drop the left shoulder.

Pivot on the ball of the foot, swinging the right leg for added momentum. This action will certainly break the waist cinch or dislocate the enemy's elbow. Step behind the enemy with your right foot, maintaining a grip on his thigh with your left hand. From here you may step behind with the left foot and cinch him, or slide up and apply the Japanese strangle.

Wheel Throw

Should the enemy seize you by both wrists, free your hands by rotating them to the outside line. Aim to break the enemy's grip where the thumb and index finger meet as this is the weakest point. Step forward with the left foot, striking with double palm heels to the enemy chest. This will drive him slightly back, breaking his balance to the rear. Grip the enemy lapels with both hands. If lapels are not available, cup both hands behind his head.

Maintaining your hold on the enemy, sit down near your left heel, pulling him forward and onto you -taking advantage of his natural reaction in trying to save himself from being pushed backward- kick up with the right leg. Strike the

enemy groin or Hara (diaphragm area).

Use your grip to the enemy to support him over you. This prevents his falling forward too fast and striking you with his head. Place the left foot in the enemy's Hara and push up strongly with both legs, lifting him off the ground.

Push the enemy clear allowing him to back-fall to a head to head position above you. The impact alone of this fall is sufficient to drive the air from his lungs and incapacitate him. Using your grip on the enemy to maintain your momentum, execute a back roll swinging the feet overhead, tucking the head to one side, and pulling with both hands.

Completing the back roll, land your buttocks on the enemy's chest, driving the air from his lungs and crushing the chest cavity. With both knees landing on his biceps, rupturing the muscles, execute a palm heel strike to the chin, snapping his neck.

Twin Dragon Fist

These techniques are used when the enemy is successful in cornering you and launches a fist attack. They result in the enemy's permanent blindness, making possible your escape.

Should the enemy throw a right arm punch, fall back slightly and counter with a mirror block. Your right arm comes across your body, palm inwards then pushes the enemy strike across his body as you come back across your own body. Twist the wrist to face palm out just before the strike connects. Aim for the wrist, thus striking the ulna nerve and numbing the enemy arm.

Immediately grasp the enemy wrist, with the same hand, pulling him forward. As he loses balance and comes forward, extend the left hand palm down, with the index and middle fingers outstretched. This forms the Twin Dragon Fist. Do not stiffen the fingers as this will cause them to break on impact. Do not force your fingers forward; rather impale the enemy eyes onto them. No great amount of strength is required- only accuracy.

If the enemy is more cautious and launches a left jab or hook fall back slightly executing a right shoulder block. The arm comes across to the left of your body palm out. As it comes back across, as before, twist the wrist to face palm in, blocking the attack. Keep the arm bent. This attack strikes attacks the radial nerve. This action opens the enemy centre line to attack.

Before the enemy's arm can be recovered from his left jab, strike out from the right arm with the Twin Dragon Fist, attacking the eyes. Imitate the action of a serpent attacking. Use the left arm to perform a depressing forearm block (push the enemy jab down with the left palm) pulling it slightly across the body to stop any counter attack.

Multiple ID's and Personalities (USA)

It is useful to be able to transform oneself into many different characters, therefore, existing without a true identity. To begin in a new form of identity, the one must first acquire a fake identity card. This can be done by:

The first thing is to find out who exactly you'll become. The most secure way is to use someone's ID who doesn't use it themselves. The people who fit this best are the deceased. Now you must go to the library and look through old death notices. You have to find someone who was born about the same time as you were. Also, it is best to choose someone that has the same first name as you, at least. This is so that you will react naturally if you are called. It is also wise to get the same first letter of the deceased persons to match your own. This is so that if you have to sign for anything then your signature will flow naturally. You should go back as far as you can for the death because most states now cross index deaths to births so people can't do this in the future. Go down to the library and look up all the death notices you can, if it's on microfilm so much the better. You might have to go through months of death notices though, but the results are well worth it. You've got to get someone who died locally in most instances the death certificate is filed only in the county of death. Now you must go down to the county courthouse in the county where they died and get the death certificate, this may cost you a small amount. Look at this paper; it could be your only way to suddenly disappear when the right time comes.

Now check the place of birth on the death certificate, if it's in the same place that you are then you are ready to go. If not, you can mail away for one from that county but it might take a while, the librarian at the desk has listings of where to write for this stuff and exactly how much it costs. Get the Birth certificate, it's worth the extra money to get it certified because that's the only way some people will accept it for ID. When you're acquiring these documents the forms ask for the reason you want it, put in the word "Genealogy". If the Death certificate looks good, wait a day or so before getting the certified birth certificate in case they recognize someone wanting it for a deceased person.

After this, access a computer and wire it up to the printer and print out some mailing labels addressed to you at some false address. Take the time to check that this address is real. Hotels that rent by the month or large apartment buildings are good, be sure to get the right zip code for the area. These are things that the authorities might notice that will trip you up. Take some junk mail and place your new labels on them. Now take them along with the birth certificate down to the library. Get a new library card. If they ask you if you had one before say that you really aren't sure because your family moved around a lot when you were a kid. Most libraries will allow you to use letters as a form of ID when you get your card. If they want more tell them that you have mislaid your wallet. You should get your card straight away or you may have to wait a short while. Most libraries ask for two forms of ID, one can be your new Birth Certificate, and they should allow letters addressed to you as a second form. Now you've got a start, but it isn't perfect yet. You should have two forms of ID now. Throw away the old letters, or better yet put them inside the wallet you intend to use. Go to the county courthouse and show them the new ID and get a state ID card. Now you will have a picture ID. This will take about two weeks.

You can also apply for a 'new' national insurance card claiming that you had lost your original. In the United Kingdom you must be over 16 years of age to receive an NI card.

You should also access a computer and type out some initials for a sport or university for example, add some colour and skew it diagonally. Then, using this as the background for your 'picture', add on the details as below:

(Title of club, college etc) _____ || Surname:..... | Picture | Forenames:..... ||
 Address:..... || || D.O.B:..... | _____ |
 Number:.....

You can also add on the instructors' signature if it's a club and an expiration date. Print this out on some thin card and get it laminated.

You can now go and get a new bank account and apply for a new passport. When applying for the new passport you must intercept the mail for the address that is on the ID. Alternatively you can organize a drop off point using an abandoned building saying that you have just moved.

When you send away photographs that will be put into new ID's such as the passport. Use a different look. Dye your hair and cover up or give yourself distinguishing features. Be sure to replace or cover them back up when you are using the ID's. Make a number of false identities so that you may never need to use your own identity.

Tear Gas

A person who could make tear gas or some similar compound could use it with ease against a large number of people. Tear gas is fairly complicated to make, however, and this prevents such individuals from being able to utilize its great potential for harm. One method for its preparation is shown below.

MATERIALS

10 grams glycerine
2 grams sodium bisulphate
Distilled water

EQUIPMENT

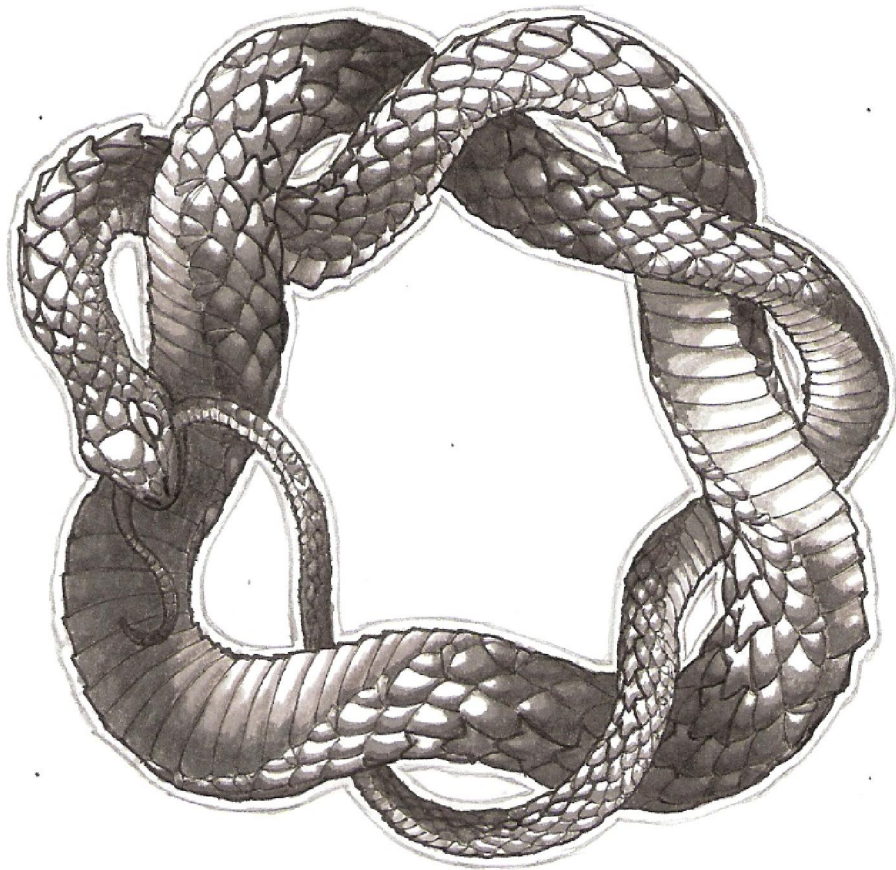
Ring stands (2)
Alcohol burner
Erlenmeyer flask, 300 ml
Clamps (2)
Rubber stopper
Glass tubing
Clamps holder
Condenser
Rubber tubing
Collecting flask
Air trap
Beaker, 300 ml
Gas mask



Procedure

1. In an open area, wearing a gas mask, mix 10 grams of glycerine with 2 grams of sodium bisulphate in the 300 ml Erlenmeyer flask.
2. Light the alcohol burner, and gently heat the flask.
3. The mixture will begin to bubble and froth; these bubbles are tear gas.
4. When the mixture being heated ceases to froth and generate gas, or a brown residue becomes visible in the tube, the reaction is complete. Remove the heat source, and dispose of the heated mixture, as it is corrosive.
5. The material that condenses in the condenser and drips into the collecting flask is tear gas. It must be capped tightly, and stored in a safe place.

Poison



Poison

This section covers poisons as a means to kill, or incapacitate. Though most are considerably easy to produce/obtain caution must be taken when handling any of these poisons as it is illegal in most countries to be in possession of some of these substances or items.

The general precautionary measures for handling poisons are to use latex gloves, a facial mask and to make sure not to consume or inhale any of the poisons in question, additionally when handling poisons cover all exposed skin surfaces that you fear may come into contact with the poison with a coating of Vaseline. This way a casual exposure won't kill you. Since these poisons do require, for the most part, manufacturing or some kind of alteration to their physical state it is important to keep all utensils clean and, for extra safety, away from any food or eating utensils. The worst thing is that you accidentally poison yourself due to negligence, so keep all poison related items separate from the rest of your property; the best situation is to have a separate building altogether for the concoction of these poisons. Also try and dispose of any unnecessary materials, but try to avoid doing so in some random field, just because you're making poisons doesn't mean you can't be nice to nature.

If you think that you have been self poisoned immediately visit a hospital. If the poison was ingested the consumption of regular coal will help remove it from your system, but you must still see a doctor. If you have ingested a poison and no coal is on hand you can consume more of the poison, this will eventually induce vomiting and remove the poison from your stomach, but remember that this method is extremely dangerous and could result in your death.

If making a gaseous poison; check at least three times that your system is closed, so that no gas leaks out into the building or area. Remember that some gases linger and can poison you months after you made the poison in question. General symptoms of a gaseous poison are headaches and trouble breathing, should you experience these leave the area immediately. Most times the poison will eventually leave your system, however long this might take, meaning you can avoid a trip to a hospital, but should the symptoms be severe see a doctor immediately.

To sum up: be as cautious as possible, don't use your utensils for anything else but poison manufacturing, and where as much protection as possible.

This section is divided into two parts: the first deals with inorganic poisons and organic poisons that are not obtained from organisms. The second part deals with plant poisons and animal poisons.

Inorganic/non-natural poisons

Chlorine Gas

Chlorine is an extremely deadly gas which is easy to make. Remember: don't make it in your home or you could poison yourself. Make it wherever you want to cause mayhem and sickness.

MATERIALS

Household Ammonia
Chlorine bleach (not chlorine free)

EQUIPMENT

One large jar
One small bottle
A rubber stopper
Masking tape



Procedure

1. Put both the bleach and ammonia in bottle in a one to one ratio, fill the bottle; do this with all due haste. On top of the bottle tape the jar so that the gas collects in the jar.
2. Find an obscure area to put the thing; this is a precaution as you could be overcome by the chlorine.
3. Once the reaction is complete, and you can see that no more chlorine is forming, get the rubber stopper ready and then in one swift movement rip the collecting jar off and plug it with the stopper. Remember that chlorine is heavier than most of the air around you so you need to be fast to prevent it from leaking out

Note:

If you can get a purer supply of ammonia, do so. Household is impure, but it's the best most people can do. Household ammonia only has about 30% active ammonia. Also, you cannot use Mr. Clean or some other cleaning agent; it has to be household cleaning ammonia. This can be bought at any drug store, or grocery market.

Carbon Tetrachloride

Carbon Tetrachloride is used in making phosgene gas which is highly lethal and was used in World War I.

Carbon Tetrachloride can be easily obtained from fire extinguishers or grease cleaning fluids found in auto supply stores.

MATERIALS

Carbon tetrachloride (an amount of fire extinguishing powder)

EQUIPMENT

Bunsen burner

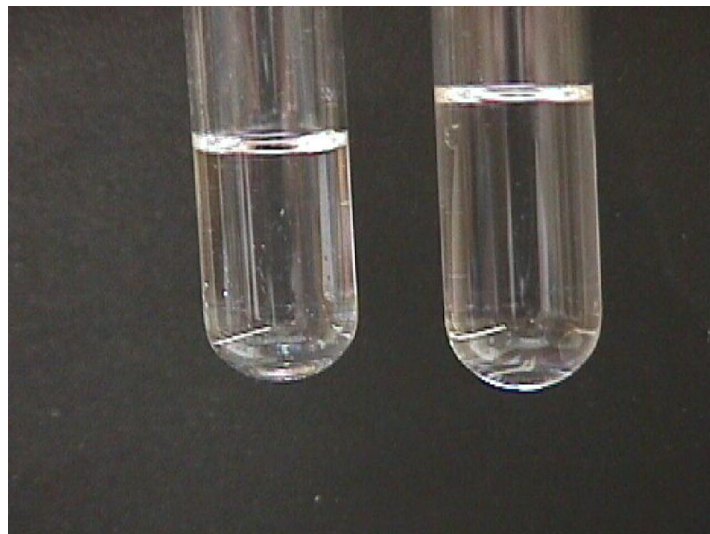
Flask

Glass canister for gas collection

Rubber stopper

Procedure

1. The gas is made by heating carbon tetrachloride over a flame or hot plate or Bunsen burner.
2. It is possible to collect the gas so that it can be used later, but as always this is a dangerous task. Place the canister over the flask and tape it down, then get the rubber stopper ready and then in one swift movement rip the collecting jar off and plug it with the stopper. This gas, like chlorine, is heavier than the air around you so you need to be fast to prevent it from leaking out



Note:

The gas is only effective in a closed room. A good way to utilize this is to set a pan full of it on a heater. People seeing it will just think its water often placed on heaters to keep the air from being too dry. Carbon tetrachloride has the smell of musty hay and will most likely be ignored or someone will bring there can of Lysol and spray the air with it.

Nicotine

Nicotine is an abundant poison. Easily found on tobacco products, as it is the pesticide used to protect the plant. In concentrated form a few drops can quickly kill someone.

MATERIALS

Chewing tobacco/snuff/ pipe tobacco

Distilled water

EQUIPMENT

Filter paper

2 jars



Procedure

1. First acquire a can of chewing tobacco, pipe tobacco or snuff. Remove the contents and soak in water overnight in a jar (about 2/3 cup of water).
2. In the morning, strain into another jar the mixture through filter paper. Then wrap the filter paper around the ball of tobacco and squeeze it until all of the liquid is in the jar. The tobacco is no longer needed and can be disposed of.
3. One of two options can be introduced. The first makes the nicotine more potent:
 - a. Allow to evaporate until a sticky syrup results in the jar. This is almost pure nicotine.
 - b. Heat over low flame until water is evaporated and a thick sticky syrup results.
4. Put a few drops in a medicine dropper or equivalent, and slip about 4 or 5 drops into the victim's coffee. Coffee is recommended since it will disguise the taste. Since nicotine is a drug, the victim should get quite a buzz before they are truly disposed of.

Note:

If the syrup is too sticky, it can be diluted with a few drops of water.

Nicotine Sulphate

This is a very interesting poison. It is obtained as an insect poison found under several names. One of the most common is Black Leaf 40, found at any garden store. It is 40% nicotine sulphate.

It is most effective if it is evaporated to thin syrup using a similar method described above. Nicotine sulphate is absorbed through the skin. An effective way to use this is to carry it around in a soft drink then "accidentally" spill on intended subject. If they do not wash it off in a matter of seconds they will be dead in a matter of minutes.

Ethylene Glycol

Ethylene Glycol is simply antifreeze such as Prestone, Zerex, etc. It has a sweetish-like taste to it, similar to the honey melon flavour in some bottled water products, and can be easily concealed in someone's soft drink. At a party, ethylene glycol can be easily poured from a container such as a kool-aid pitcher into the party punch*. The lethal dosage of this is about four ounces and death incurring effects resemble the characteristics of drunkenness.

Materials
Anti-freeze

Procedure

1. Place a generous amount of antifreeze in into victims drink

**Note:*

Ethyl alcohol is effectively an antidote for ethylene glycol poison so placing it in alcoholic drinks will null its effects

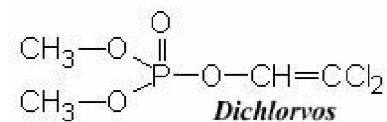


D.V.D.P

DVDP is an acronym for Dichlorovinyl Dimethyl Phosphate. It is a contact poison and incredibly deadly. It rivals Prussic acid.

MATERIALS

Shell No-Pest strips
Paint thinner



EQUIPMENT

Beaker
Rubber stopper

1

Get a pack of Shell No-Pest strips and set them in a beaker similar, like a Miracle Whip jar. Then cover the strips up with paint thinner.

2

Let this mixture sit overnight. In the morning there will be a commonplace looking, oily sludge. This is in fact pure DVDP.

Note:

When handling cover all exposed skin surfaces with a coating of Vaseline.

A way to use it would be to say apply it to a doorknob or a steering wheel with a Q-Tip. For handy use, it can be placed in a nasal spray bottle and carried around. If you take this route, then wear glove and stand upwind of your target

Potassium (or Sodium) Cyanide

This is an almost instant killer with very little taste. It only takes a few grains to kill and there are 437 grains to an ounce. Put it inside of salt shakers in your target's home or carry it around in a little bottle with a half and half mix of water/cyanide (pre-dissolved) just waiting to be dumped in someone's beer.

MATERIALS

Potassium ferro cyanide (a blue pigment)

Potassium carbonate (used in soap and glass production)

EQUIPMENT

Adjustable heat source (preferably torch)

Crucible



Procedure

1. Mix, evenly, 8 parts of Potassium Ferro cyanide and 3 parts of potassium carbonate.
2. Heat a crucible red hot and pour the mixture in. It will melt and begin to bubble. Play the torch flame on it to keep it hot. When it stops bubbling; the reaction is complete.
3. Pour the fluid off onto some flat, enamelled surface. While it is still warm, break it up and store it in a dry place.

Note:

For sodium cyanide: substitute sodium compounds instead of potassium

Aspirin (Acetylsalicylic Acid)

This is easy to get hold of, and preferably use soluble ones, and dissolve them. A dosage 20-30+ grams (too many cause vomiting) is fatal, however this is not recommended as fatal dose varies wildly and could cause liver & kidney damage instead of death. It causes projectile vomiting after about 10 hours. Medical help is generally effective; May cause bleeding in stomach/upper intestines. Time to death is variable.

MATERIALS

Aspirin pills or solvent 20 doses

EQUIPMENT

Teaspoon

Procedure

1. If using pills: grind them into a fine powder using the back of a spoon
2. If using solvent: simply open the packet
3. Place the powder into the drink of your target, wait for any fizzing to subside, and make sure no powder is un-dissolved on the bottom of the drink container



Paracetamol

(Acetaminophen/Tylenol)

Decidedly simple to acquire and requires no fabrication

15+ grams (20+ is better) within 10 hours causes fatal damage, but 2 weeks until death. Horrible side effects during this time some of which are: acute toxic hepatitis, renal failure, cerebral edema, intra-abdominal bleeding, aspiration pneumonia, haemophilia,

Too small a dose causes severe liver damage. Accidental deaths from this are very common. There are few if any side effects before the damage becomes fatal; occasionally vomiting and nausea.

MATERIALS

Acetaminophen / Tylenol

EQUIPMENT

Teaspoon

Procedure

1. While grinding any of the Acetaminophen / Tylenol will make the dissolving process faster, it is not necessary.
2. Place the lethal amount of paracetamol into the targets beverage



Petrol

20 ml, if injected, is fatal within Seconds, if not, minutes. Easy to obtain, however administration is difficult. The common name for this in America is gasoline

MATERIALS

Every-day car petrol

EQUIPMENT

Syringe with volume increments



Procedure

1. Draw the petrol into the syringe until it reaches the 20 ml marker or more
2. Surprise the victim and inject the petrol into them

Note:

One could also use LPG (propane/butane) on skin surface since these are light enough to be absorbed through the skin. But, once again, administration is difficult

Potassium Chloride

This is a widely available salt (Sylvite; Muriate of potash) that, when dissolved in a solution of water and injected, causes death within minutes. 20 millilitres of dissolved substance should be sufficient to cause death.

It Causes heart attack as a great excess of potassium in the blood interferes with nerve signals, and stops muscles and nerves from working. So when it reaches the heart it simply stops.

It May be difficult for coroner to realize it was poison rather than a natural heart attack.

MATERIALS

Ordinary tap water

Potassium chloride

EQUIPMENT

Tea spoon

Glass cup

Syringe with volume increments



Procedure

1. Using the back of the spoon crush the potassium chloride into fine particles
2. Place the powdered potassium chloride in the a glass of water and stir until it can no longer dissolve in the water
3. Draw 20ml or excess into the syringe, and then inject it into the victim

Paraquat

Paraquat is a herbicide found in many weed control products (e.g. Gramoxone). If consumed the victim will experience multi-system organ failure; with death occurring within hours to a few days. However, should an insufficient amount be administered, it will selectively accumulate and persist in the lungs and slowly eat away at them while the victim spends several weeks gasping for breath in terrible pain before they expire. There is currently no antidote, and even people who manage to get lung transplants find that their new lungs are eventually destroyed as well, since the poison accumulates in the fat surrounding them. It is widely used as a means of suicide in the third world.

MATERIALS

Paraquat containing herbicide -Gramoxone-

EQUIPMENT

Latex gloves

Procedure

1. Simply take the herbicide and sprinkle it over the food or drink of the victim in a large amount. Calculating the exact amount is difficult as the herbicides differ, so use as much as possible.



Vinegar Poison

This is a very simple poison to make with almost no materials needed.

MATERIALS

Vinegar

EQUIPMENT

Copper/ lead container with lid



Procedure

1. Take a lead or copper container and store vinegar in it for a long time – about 4 weeks- it will eventually turn to into a deadly poison.

Natural/biotic poisons

Castor Bean

When you consider that castor oil is used as a food additive in candy and chocolate it's disconcerting to discover that the fruit of that plant, the castor bean, contains a super toxic level of the poison ricin. As little as one bean, well chewed, could prove fatal. However, according to figures from the American Association of Poison Control Centre (AAPC) only two Castor Bean fatalities were recorded in the period from 1999 to 2004.

MATERIALS

Castor beans

EQUIPMENT

Mortar and pestle or knife



Procedure

1. Obtain castor beans, enough to satisfactorily kill
2. Cut up the beans and place them in a salad, or grind them, or simply feed them whole to the target.

Puffer fish Venom

The poisonous part of the puffer fish is the tetrodotoxin found in its ovaries. This poison is not destroyed by cooking although experts say if the entrails are removed before cooking the fish becomes harmless. Used in the Japanese delicacy fugu, puffer fish can only be cooked and prepared by specially trained and licensed chefs. Even so, from 1955 through 1975 there were more than 1,500 fatalities caused by eating improperly prepared fugu.

MATERIALS

Puffer fish

EQUIPMENT

Knife
Collecting pan
Cooking pan
Dexterous gloves



Procedure

1. Obtain a puffer fish, from either fishing or a Chinese specialist restaurant. Be careful in handling the fish so that the spines do not penetrate your hand. Wear some hardy gloves
2. Carefully cut open the fish and look for the intestines. Find the ovaries and cut them out, should you not know what they look like simply remove the entire intestinal section of all filamentary organs (i.e. all the long fiddly bits)

Alternatively search through the waste of the aforementioned restaurant for the organs

3. Cook and serve these parts, without washing them, to the victim.

Hemlock

Hemlock was supposedly the poison that was used to dispatch Socrates. Whilst Descartes may have said, "I think, therefore I am," Socrates is meant to have lifted his mug of Hemlock and said, "I drink, therefore I'm not." In Water Hemlock the highest concentrations of the poison cicutoxin –this is similar to nicotine– can be found in the root and one bite of this can cause death in adults. Water Hemlock causes convulsions and death. Poison Hemlock causes muscle failure and death.

MATERIALS

Water hemlock or poison hemlock

EQUIPMENT

Collecting plate

Knife

Latex gloves



Procedure

1. While wearing the latex gloves, cut up collected hemlock plants:
2. The poison itself is located in every part of the plant of both types, and approximately 100mg of the poison needs to be consumed to cause fatality in adults.
3. Serve the plant in a salad, but note that the roots give off a pungent odour that will be detected by the victim if not disguised

Oleander

This is another simple poison that can be easily made. Bear in mind that it does show up easily on toxicology tests

MATERIALS

Oleander twig

EQUIPMENT

Motor and pestle



Procedure

Take a twig of this bush and grind it into a fine powder. Place the powder in the salt shaker or substitute it for any other seasoning within 3-4 hours of making it, sooner rather than later. Or simply use it as you desire.

Digitalis

Digitalis, an extract of foxglove with a low fatality rate

Death is caused by a heart-attack.

Symptoms include: nausea, vomiting, abdominal pain, diarrhoea, headache, and slow irregular pulse. Also, sometimes, trembling, convulsions, delirium, and hallucinations. It's difficult to take a fatal amount because vomiting usually removes it.

MATERIALS

Foxglove

Tap water

EQUIPMENT

Pot

Heat source

Saucer

Knife



Procedure

1. Simply consuming foxglove will cause death; however, a concentrated extract works better.
2. Chop up the foxglove with the knife in to as small pieces as you can manage, preferably do this in the pot.
3. Place into the pot the foxglove pieces and cover it with water. Place the pot on top of the heat source and heat until the water boils
4. Allow most of the water to boil away, leaving approximately 100ml remaining.
5. Collect the remaining water and administer it to the victim

Yew tree needles and Laurel leaves

Yew tree needles and Laurel leaves are both extremely deadly.

MATERIALS

Yew tree needles and Laurel leaves
Isopropyl alcohol (rubbing alcohol)

EQUIPMENT

Mortar and pestle
Coffee percolator
Measuring glass
Saucer



Procedure

1. To extract the poison from the evergreens, grind up the foliage with a mortar and pestle and fill up a coffee percolator with it.
2. With the measuring glass measure 237 millilitres of isopropyl alcohol in the pot and percolate for about 1/2 hour. If the alcohol boils off then add some more.
3. You need to distil the water off of the alcohol. When the process is done, distil of the alcohol until you only have a couple of millilitres of residue left. Then put that on a saucer and let it evaporate.

Rhubarb

Rhubarb leaves are deadly. Cooked, they take about an hour to kill, but when raw almost immediately.

MATERIALS

Rhubarb leaves

EQUIPMENT

Knife

Procedure

1. Chop up some leaves and put them in the stew or on the hamburger.

Note:

You have to grow your own rhubarb because commercial suppliers normally take the leaves off.



Miscellaneous



Light Bulb Bombs

Written by: *Pandora's Assassin*

These homemade explosives are simple to make, they come with there own full circuit and ignition system. Some light bulbs the glass can be taken off by heating the metal bottom base with a blow torch or gas stove. This should be done very carefully, since the inside of the glass is an air tight vacuum. When the glue gets to the right temperature it can be easily pulled off from the metal base.

As for other light bulbs it is necessary to heat the glass with a blowtorch or oxy-acetylene torch. In either case, once the bulb and its base had cooled down to room temperature or lower, the bulb can be filled with an explosive

Black powder is a sufficient explosive material for the job. Or about 1/2 inch from the bottom filled with gasoline for the napalm effect.

If the glass was removed by the base then it should be glued back on with epoxy once the powder was inserted. If a hole was created in the bulb itself, then good ol' duct tape will hold the explosive material in there just fine.

Most importantly! Before putting the light bulb in the socket make sure line has no power. This can be tested with a regular light bulb.

This is a common practice by methlab users and terrorists. Someone approaching a dark room wouldn't think twice.

Kill the lights.

Loss Prevention

Written by: *MrNatowski*

Alright, so anyone who's been caught at a major retail store knows that they take your license and enter it into a database. This database is so that if you ever get caught again, at that store or another, they can look up your name and see that you've been caught before. If you've been caught before they'll call the police, if not they will sometimes just issue a civil demand. This is in most cases at least.

When I was in an LP office I think the name of the system was something along the lines of ASIS. I did some research and found out it's an FBI sponsored database that something around 38 retailers are using.

My question is, does anyone have a list of retailers who use this system, or can you list 1 or 2 that you know for a fact does? Actually a better question would be (To anyone who's been caught before) do you know any stores that DON'T use any sort of database like this?

Also, feel free to share any information on prosecution policies in certain stores. Some of this info could be wrong but this seems to be the general policy on stores from what I've gathered. If you notice any errors or have additional information about a particular store I'll edit it in.

Aeropostale: No chase policy/Doesn't prosecute/No LP, staff has little or no LP training/Cameras are not actively monitored

Abercrombie & Fitch: No chase policy/Sometimes prosecutes but often will just ask for merchandise back without civil demand/Only LP is staff, some care, some don't/Cameras are not actively monitored

American Eagle: No chase policy/Will prosecute/Limited LP but will occasionally use plain clothes/Cameras are not actively monitored

Best Buy: Has active and good LP. Will follow you into the restroom if they suspect you, they will also call the police the second they see you conceal something. There is a stationary guard at the entrance who monitors cameras throughout the store.

Burlington Coat Factory: Somewhat dangerous.

CVS: No chase policy but will attempt to get your license plate/Will prosecute/Store managers will sometimes act as plain clothes LP/Cameras are not usually monitored

Dicks Sporting Goods: Poor LP

Dillards: Very dangerous.

Fred Meyers*:

Hollister: Same as Abercrombie & Fitch

H&M: Chase policy and prosecution policy unknown/Very good LP for a small store, even in small stores will use plain clothes or a security guard/Camera status unknown

King Supers: Good LP

Kmart: Will chase.

Kohls: Dangerous store to shoplift at, has active LP who make fitting room stops.

Lord & Taylor*: Will chase you/ Will either prosecute or issue civil demand depending on circumstances/Extremely good LP, plain clothes are used and are often off-duty cops/Cameras are actively monitored.

JC Penny*: Will chase you/Will either prosecute or issue civil demand/LP is decent but not as good as Macys, occasionally uses plain clothes/Cameras are actively monitored

Macys*: Will chase you/Will either prosecute or issue civil demand/Above average LP, plain clothes are common/Cameras are actively monitored

Meijers: Will chase.

Mervyns: Dangerous.

Sears*: Will chase you/Will prosecute, sometimes issues civil demand/Extremely good LP, uses plain clothes/Cameras are actively monitored

Sephora: Will Chase/Will issue civil demand and call police, may prosecute depending on circumstances, will issue a trespass order for 1 year/No plainclothes/No monthly quota on shoplifting apprehensions/Very well and actively-monitored cameras that are full colour, and can pan as well as zoom in/nothing has a security tag/There is one dedicated employee who monitors all the cameras, and has radio contact with all (or just the LPs) staff members in the store/There are generally more than 2 LPs active in the store with the camera guy behind the scenes/LP is well trained and even regular staff has a degree of LP training

Staples: There are two kinds of store layouts. The old store layout consists mainly of rows of aisles, and the new store layout has more of a maze layout like Bestbuy. The cameras in the stores with old layouts are mostly fake, while the newer stores employ several low-profile cameras designed to monitor internal theft. In both stores the cameras are not usually monitored.

Stop & Shop: Chase policy unknown/Will prosecute/Uses plain clothes LP and staff will often look for shoplifters/Cameras are often monitored and are numerous

Target*: Will chase you/Will prosecute, sometimes but rarely issues civil demand/Extremely good LP and employees are given an incentive to look out for shoplifters/Cameras are actively monitored and are very high quality

Walgreens: No chase policy/Will prosecute/Does not have active LP but the staff will sometimes try to act as LP. They aren't supposed to and can not legally stop you/Cameras are not usually monitored although there is usually one employee in the back room near the cameras, so be aware of that.

Walmart*: Will chase you/Will either prosecute or issue civil demand/LP often poor but ranges from store to store/Cameras are actively monitored/Has a policy not to prosecute under \$25

**Stores marked with an asterick are known to enter shoplifters into a national database.*

Dealing with LP

Written by: *MrNatowski*

I hate seeing stories of people screwing themselves over because they don't know their rights. Here's a quick run-down of shoplifting and what to do if you get caught.

First, LP are only legally allowed to stop you if they:

1. See you (In person or on camera) conceal an item.
2. Maintain a constant visual on you after you conceal the merchandise.
3. Watch you pass all points of sale.
4. Confront you while still on their property.

In some states (You should look up the law in yours) you have committed a crime the moment you conceal an item. In other states you haven't done anything wrong until you actually leave the store. This is important.

Also, if you haven't stolen anything (Or they can't prove you've stolen anything) and someone accuses you of theft, that's illegal. Most stores have very strict policies on who they can and can't confront, since making a bad stop can cost the store thousands if they are taken to court.

Next, security can't follow you once you're outside of the store's property. Most stores take this very seriously, since chasing a suspected shoplifter into the streets means that if the person gets injured running away from LP, the store gets to pay out the ass. Normal policy is to call the cops once the suspect leaves store property.

If you run from the LP, don't touch them. One light shove means the difference between a misdemeanour theft and a felony aggravated robbery (Sounds scary doesn't it?).

Keep in mind that sometimes LP don't play by the rules. They love to break the rules or at least bend them. One trick is to pull out a badge and shove it in the shoplifters face and state that they're police. What they fail to mention (If you looked at the badge that they flashed for half a second) is that the badge probably says "Macy's police" or something along that nature. These people are NOT police and have no authority over you. Again, laws vary by state. Some states allow security guards to take reasonable measures to stop shoplifters, but this is only if the other criteria have been met (Watching the item concealed, constant visual, pass all points of sale, still on store property). In most cases, they do NOT have the authority to touch you. They do NOT have the authority to search you without your consent (Which you should never give). You do NOT have to sign any papers they give you.

LP thrive off of fear. There are entire books written on how to intimidate shoplifters into confessing. The first thing they'll do is say they know you've shoplifted there before. They'll say they have your picture on the other side of the wall, every store in the area is looking for you, they have video evidence of you stealing dozens of times. Statistically speaking, you probably have stolen before if you got caught. You probably have stolen from that store several times, and you're probably thinking everything they're saying is true. There's no use denying it, it'll just piss them off and make your life harder.

This is all 100% bullshit. 90% of the time they have jack shit on you. They may not have even SEEN you steal anything, but are sure enough in their minds that you have and are now going to grill you until you confess. Everything is a game to them. They will do everything they can to scare you. Even the layout in LP offices is usually designed to intimidate you. You'll see statistics showing how many shoplifters they've caught and cartloads of stolen merchandise.

At this point one of two things will happen. They'll call the police or they'll collect your information, ban you from the store, and require you to pay a fine (Usually called a civil demand). Your information will

Website: <http://www.zoklet.net/bbs/>

be entered into a government sponsored database that most major retailers participate in. If it's your first time caught, they may let you off with a civil demand. If you're already in the database and you've been caught several times, they may call the police. Often they'll tell you to either admit that you've shoplifted before today, or they'll call the police. You should remain calm and make a rational decision when deciding what to do. Hopefully you've already done your research on the law at this point. Think carefully about if any of your rights have been violated, or if they're lying about any of their evidence. You can ask to see the video evidence they have, and if they're bullshitting they'll probably get pissed off. In many states if you were stopped and didn't attempt to leave the store, the entire case will be thrown out.

If you think you have a shot of fighting it, let them call the police. Unless the stolen amount was several hundred dollars, you'll most likely receive an NOA (Notice to Appear) from the cop. This means you won't be arrested, but by signing a statement you agree to show up in court. If you fucked yourself over and you think you don't have much of a chance, you can choose to take the civil demand. The fine can be up to 10 times the amount stolen. In most cases the fine will be between \$200 and \$500, but again this can vary from state to state.

In most states the store has a period of one year to collect the fine from you before they can no longer take legal action. Many stores are bad about this and the law firms who represent them will send you a Civil Demand notice 6-10 months after the incident. Usually you'll receive a first notice telling you how long you have to pay the fine. If you don't pay the fine in time, you receive a second demand notice threatening legal action. A month or two later if you ignore the letters you'll get a notice informing you that you now owe them 2 or 3 times as much to pay for court fees.

This is standard, and often these letters are just scare tactics. Stores send out thousands of civil demand notices every year, and in most cases only a couple dozen cases will actually be taken to court. If you stole \$20 of merchandise, they probably won't follow up on your civil demand notice. If you stolen hundreds it's harder to say.

When making your decision of what to do, keep this in mind. Retail fraud is separated into three categories.

3rd degree Retail Fraud (Misdemeanour): Under \$100. Up to 91 days in jail and/or \$500 fine.

2nd degree Retail Fraud (Felony): \$100-\$1000. Up to one year in jail and/or fine.

1st degree Retail Fraud (Felony): \$1000 or more. 1-5 years in jail and/or fine.

In short, research the law in your area. Some states have mandatory sentencing laws. Other states give the judge more leniencies in determining fines and sentencing.

Finally, if you're going to steal, remember that \$100 is the line between a misdemeanour and a felony. Remember that LP only have as much power as you give them, and be smart about what you do. You can't get in trouble for what can't be proven. Be smart and don't let the store security (Who get paid 9 dollars an hour) intimidate you. Make rational decisions and use common sense. Remember, there may be cameras in the parking lot. 😊

Barcoding with Barcode Magic 3.1 Guide

Written by: *theinvader*

Barcode Magic 3.1 was produced by BulletProof software a few years ago. It's pretty damned old and not updated, but it's so brilliant and great at making barcodes that it's still in use.

A license can be bought for \$79, but it's almost too easy to download a key generator for it.

Here's a reg. code if anyone needs one (ONLY WORKS ON THE TRIAL VERSION FROM <http://www.barcodemagic.com/>).

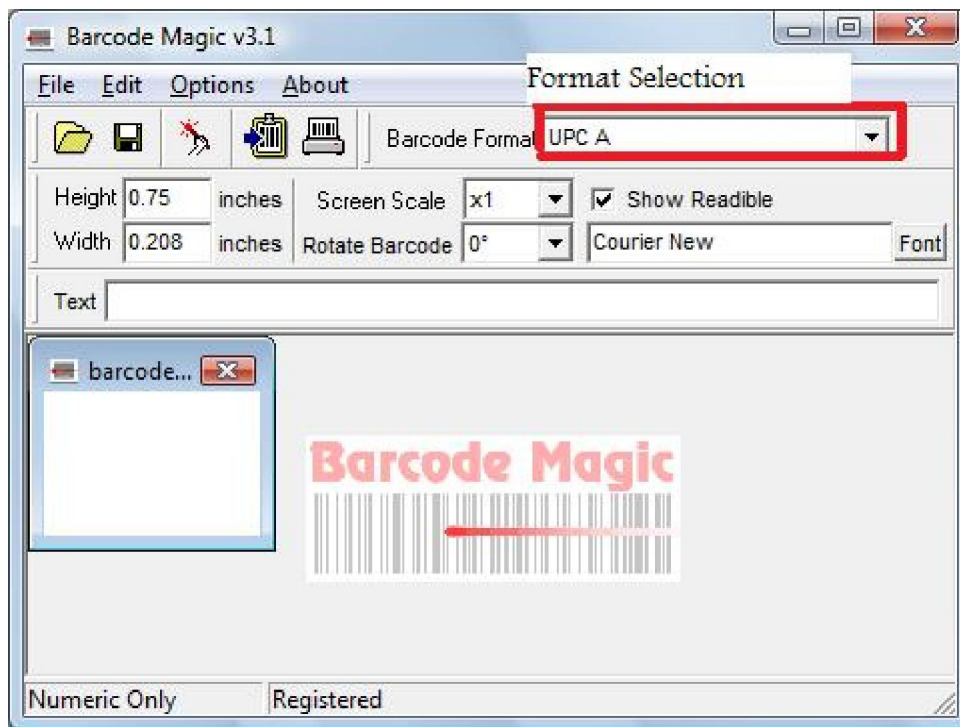
Name: Zoklet

Serial: BM-2196-92

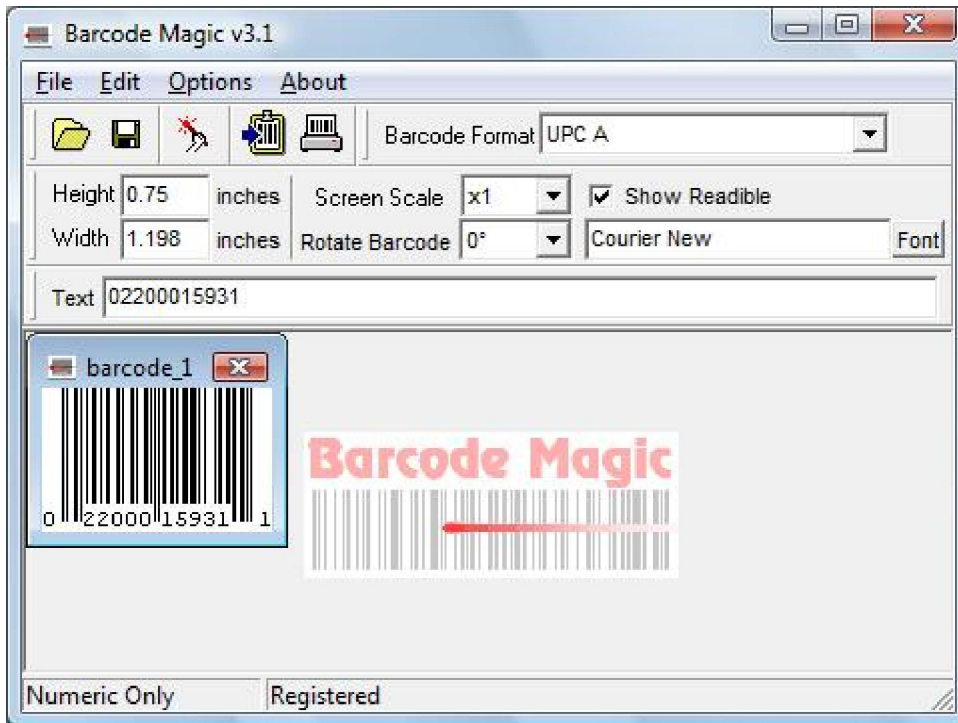
That was directly copied and pasted from my info, and verified with a keygen made by "ScareByte". Barcode Magic 3.1 will be referred as BM3.1 or simply BM in the rest of this post.

To make barcodes:

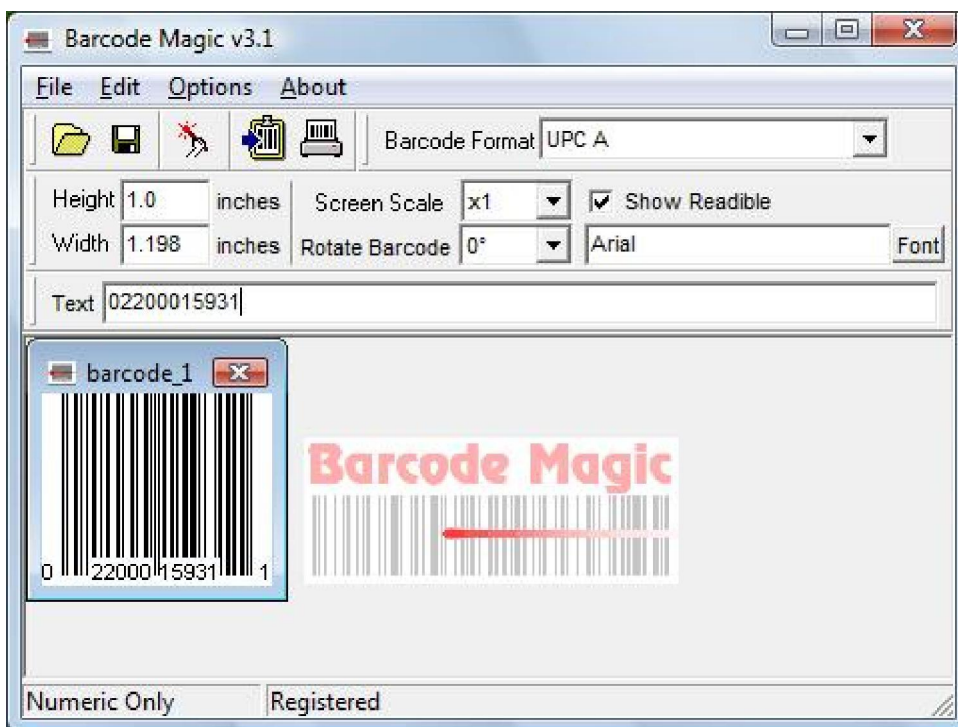
1. Download and register (or buy, but that's too fucking expensive for BI) BM 3.1
2. Acquire some barcodes that you wish to reproduce.
3. Select your barcode format (US stores= UPC-A or UPC-E, UK = EAN13)



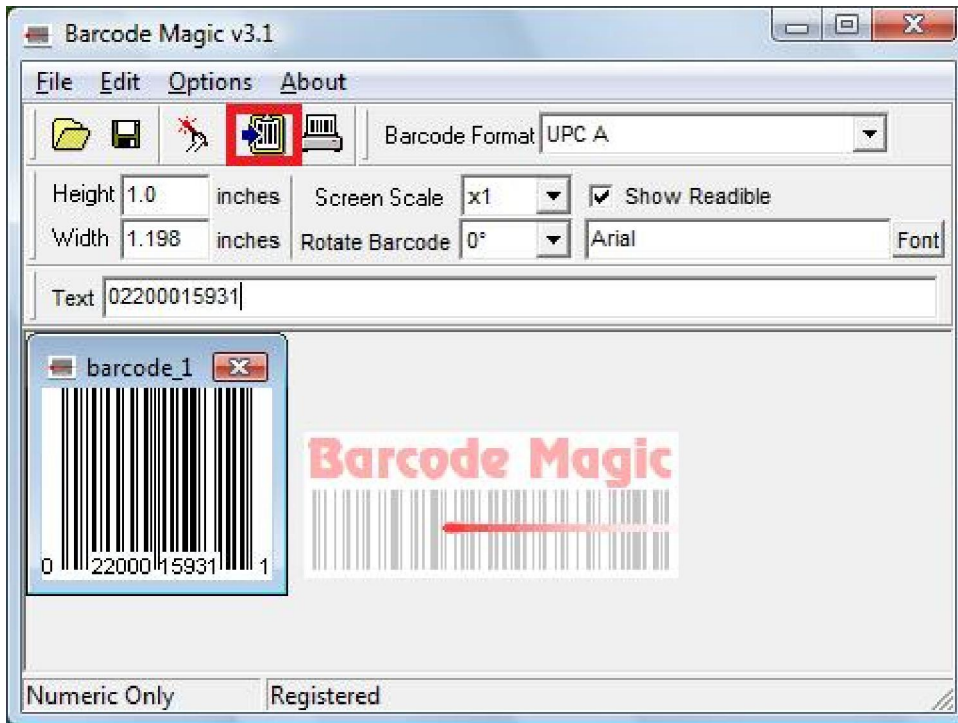
4. Type in a barcode you wish to reproduce. (example is Altoids Spearmint UPC-A)



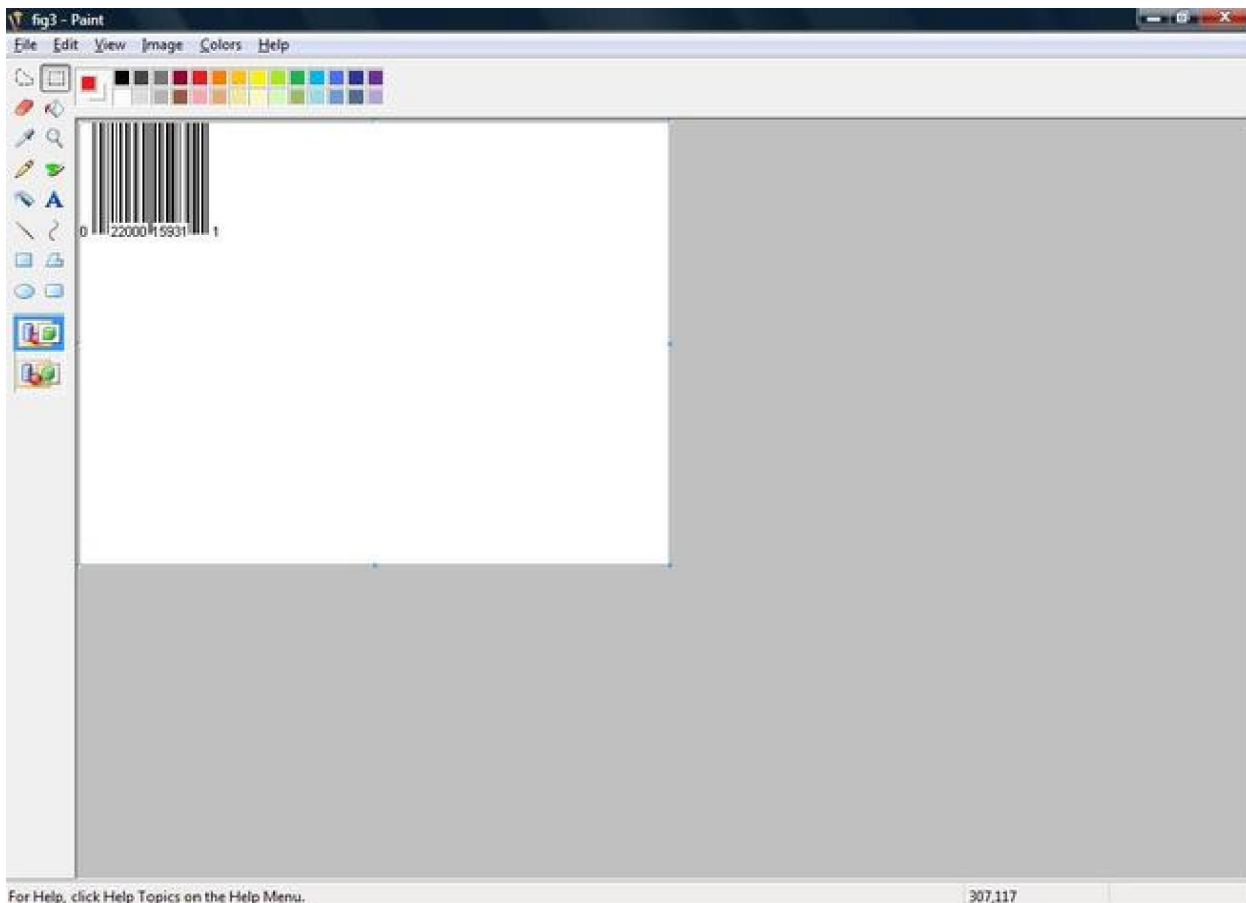
5. Adjust size/font settings as necessary. Width cannot be changed normally. Height is usually 1 or 1.25 inches (2.54 or 3.175 centimetres). I personally use Arial fonts as it looks the best. I haven't found a font that looks just like the numbers on real barcodes.



6. To make more copies/print the barcode, don't use the printing engine in BM(it's shit) use Paint/Photoshop. Press Ctrl+C or the clipboard with an arrow on it to copy the picture to the clipboard.



7. Paste into a new Paint/Photoshop window. I don't have Photoshop, so I will be using Paint.



8. Manipulate and print as necessary.

That's a simplified breakdown of producing barcodes with BM 3.1. This guide was created as 313 didn't know how to use BM.

I hope to see more barcoding tips on Zoklet, and good luck with your savings

The Grocery Store Shoplifting Guide

Written by: *nigma*

Naturally, shoplifting is illegal, and you are warned that its not my fault if you get caught.

Items Required for Shoplifting:

The guts to do it. A grocery store that you probably shouldn't come back to.

Tips for Shoplifting:

Grocery stores are different from your average Walmart superstore because if you're stealing from a grocery store, you're probably not trying to steal something big. Let's say you're stealing condoms. A lot of people do. That doesn't mean that you *can't* steal something big, because large orders of food can be stolen with relative ease. There's a guide for large orders of food down below.

The best time to shoplift is between 3:00 and 7:00 on a Friday, or on any holiday. That's because the more people, the better. When managers are busy herding customers through the checkout process, they focus less on the customers in the rest of the store and more on the customers at the registers. Shopping at 10:00 PM on a Tuesday is probably going to get you noticed.

If you're trying to steal condoms, or something small, don't head straight for the HBC (Health and Beauty Care) section. Grocery stores know that people try and steal condoms, among other things. When you walk in, go around the perimeter of the store.

If you're stealing something small, which you probably put in your pocket, the best way to get out of the store is to buy something. Buy a soda; its \$1.00, versus your stolen \$12.00 Trojan condoms. A paying customer is much less likely to be questioned.

For legal reasons, stores usually won't follow you out into the parking lot. However, they can get your license plate number. So if you really want to be incognito, use someone else's car, or park at the back of the parking lot. If the store is close by, walk.

Dress like you're average. Don't wear a hood in the store. Don't glance past your shoulder every five seconds. The primary key to shoplifting is to look like you know what you're doing, and if you're acting like a sketch, then its going to be very obvious to any manager that you're indeed sketchy. To look legit, talk to someone on your cell phone with a charismatic attitude.

Don't hit the same store twice. In fact, don't even hit the same franchise twice (i.e. go to Target, then go to another Target).

If you know someone saw you, but the item on the shelf and walk out the door. Legally, there's nothing they can do.

Self-checkout is your best friend. Try and use the one that is farthest from the self-checkout cashier.

The Large Order Shoplifting Technique:

You need some grocery bags and an old receipt, preferably a long one.

Walk into the store with the grocery bags (the paper bags, or the reusable ones) and put the bags in the shopping cart.

Go shopping. Put the food right into the bags. Cashiers and managers don't mind this because they know that some people like to organize their food into bags because of personal preference and such. So just put the food right into the bags.

With the receipt in hand, all you have to do is walk right out the door. Keep the receipt visible in your hand.

For best results, do this on Christmas Eve, or on Memorial Day weekend.

The Free Money Technique:

Buy something. It doesn't matter what it is, as long as you know you can steal another one.

Come back the next day and steal the same item.

With your receipt, return the item and get your money back. So essentially you got the item for free.

This is extremely fucking risky, so don't do it more than once a month.

Make Your Own Finger Prints

Written by: *Drizzt*

If you were in need to disguise your own finger prints, but leave fingerprints, how would you do it? Many scenarios could require this, let alone just wanting to frame someone else for, well, a distasteful course of action. **Edit:** *Only older laser printers will leave print raised enough for the latex to take on ridges. The newer ones almost completely transfer ink to the paper leaving minimal, if any residues.*

Materials required:

Patience

Liquid Latex

Laser Printer

High-res scanner

Vaseline

Flexible metal (*to make moulds, I find Some artistically bent and cut wire does a nice job*)

Non absorbant paper

First:

Obtain the finger prints of your victim. This can be done easily enough, however you will require all five prints (for framing anyhow, to simply have a different finger print for say, a pawn shop form you could do with thumb and index finger.) Anything that someone must touch with every finger tip will do, as long as the surface is smooth. A drinking glass, a steering wheel, a leather couch. Lift them with your own means as it wouldn't be difficult.

Second, what to do?

You scan the finger prints. High resolution scanning is ideal; however, it doesn't have to be perfect in all cases. You scan the image touch up in a photo editing program, and print. You want to touch up any thicker lines

or extremely rough lines. Also, fix broken edges, but pay attention because some will be natural. In order to be successful, you will want to print on a plastic-like paper. Transparencies or sticker paper will work well enough.

Third, z0mg I r print?

Okay, you've printed your prints (*lol.*) You'll need an extremely shallow oval mould. More like a cookie dough cutter, but fit it around the prints with a little extra room. Coat the prints with a very thin coating of Vaseline. I mean **EXTREMELY** thin. Think Asian dick thin. Think fucking nano thin. Although this is more or less the most difficult part of the process, it's not extremely necessary. It avoids a hassle later on though.

After coating with Vaseline, if you chose to, fill the mould with liquid latex. All you do from there is allow the latex to cure. If your Vaseline was thin enough, it will take impressions of the ridges created on the paper from the ink. If you chose not to use Vaseline, your prints will be more pronounced, but you have to remove the latex before it completely cures. This can make for some unrealistic warpage and distorted lines.

Fourth and final:

You now have a set of prints for one hand, you would be extremely lucky to acquire both hands. The latex should be thin enough to go unnoticed on your finger tips, adhere it with make-up glue or liquid latex. You can now go about your happy criminalization! Before you use, it's wise to rest your new finger tips on a slightly oily surface, your face, or touch oily food, it's up to you.

I in no way condone any mistreatment of this tutorial for actual criminal use. (*right...*)

How to Use TamperData to Get Intangible, Easily Resalable Stuff for a Cent.

Written by: *Purple Sprite*

I wrote this here screenshot-heavy guide to learn you niggas how to defraud websites and scam intangible shit (cd keys, game time and xbox live points cards/subscriptions, etc.) that you can resell later.

First off, you're going to need a couple things..

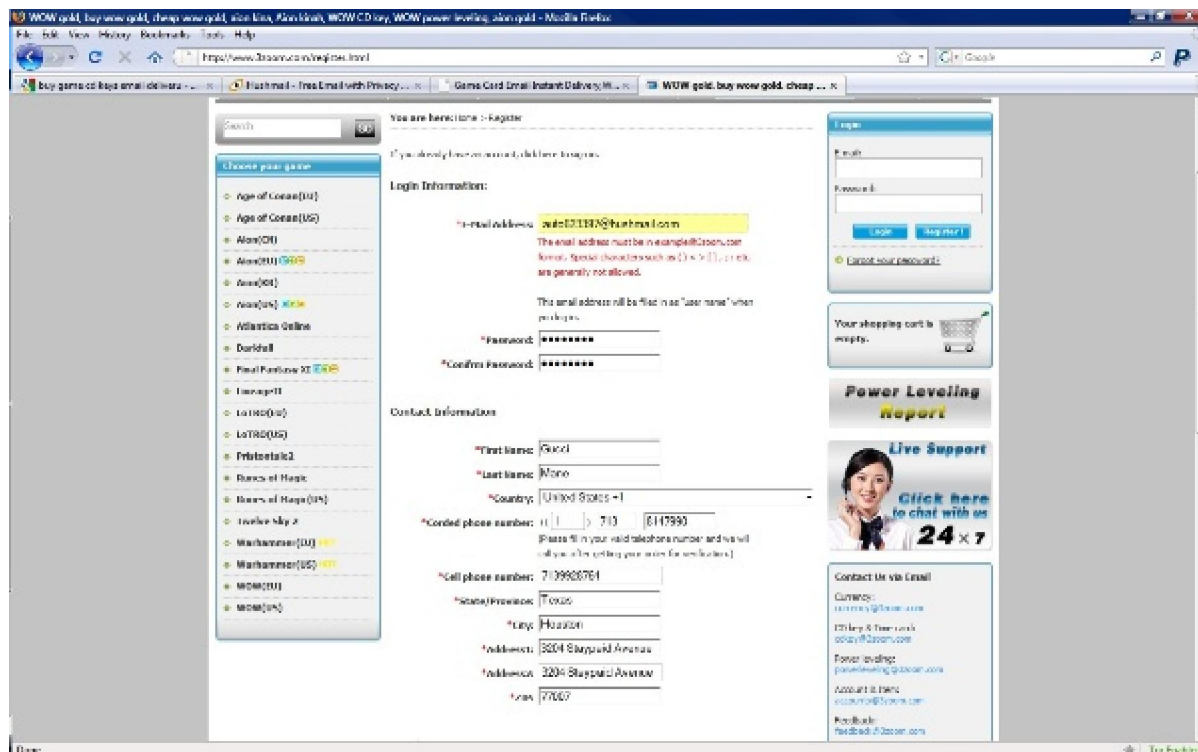
Firefox: <http://www.mozilla.com/en-US/firefox/firefox.html>

Tamperdata: <https://addons.mozilla.org/en-US/firefox/addon/966>

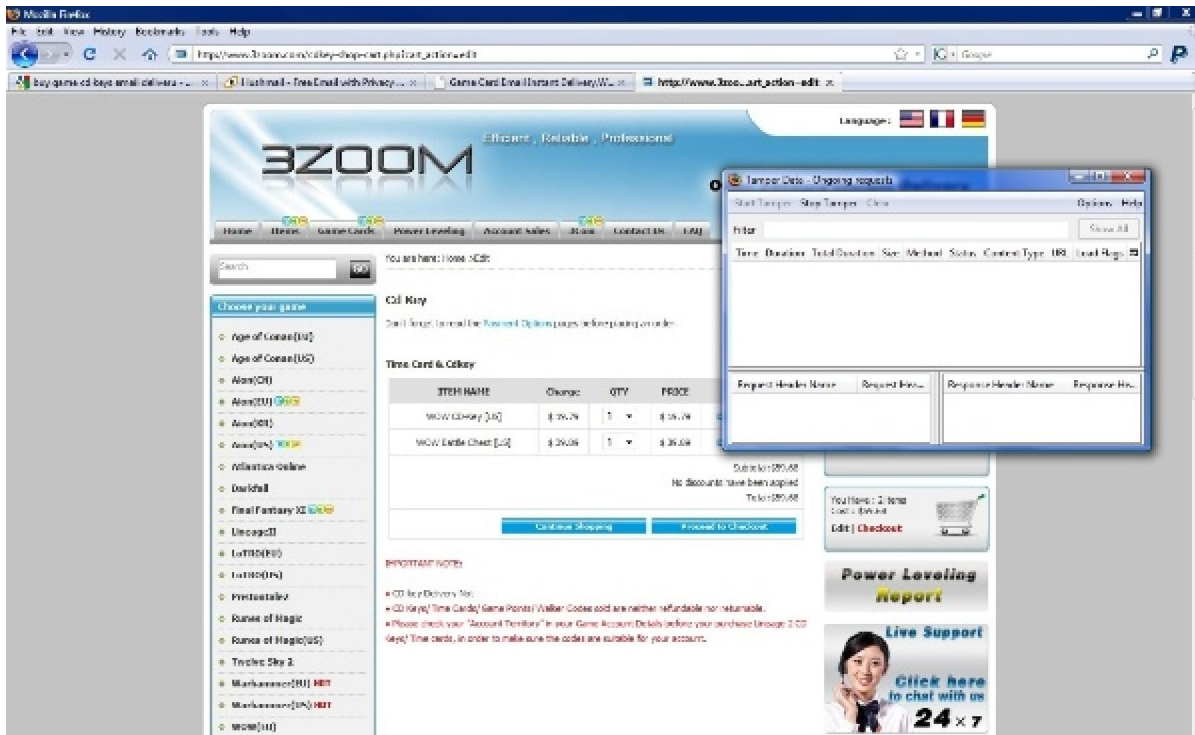
Paypal, preferably with false information

Alright you've installed what you need, now to find the target. You can do to any site for just about anything, but most likely won't receive the shit you buy unless it's an automated delivery system, (again, think intangibles.) I generally target websites based in China that sell World of Warcraft CD keys and time card codes that are delivered via email. I do this strictly because these items are incredibly easy to sell. Just google "world of warcraft cd keys instant delivery." and find a shitty site to rob. For sake of example, I'm going to target www.3zoom.com

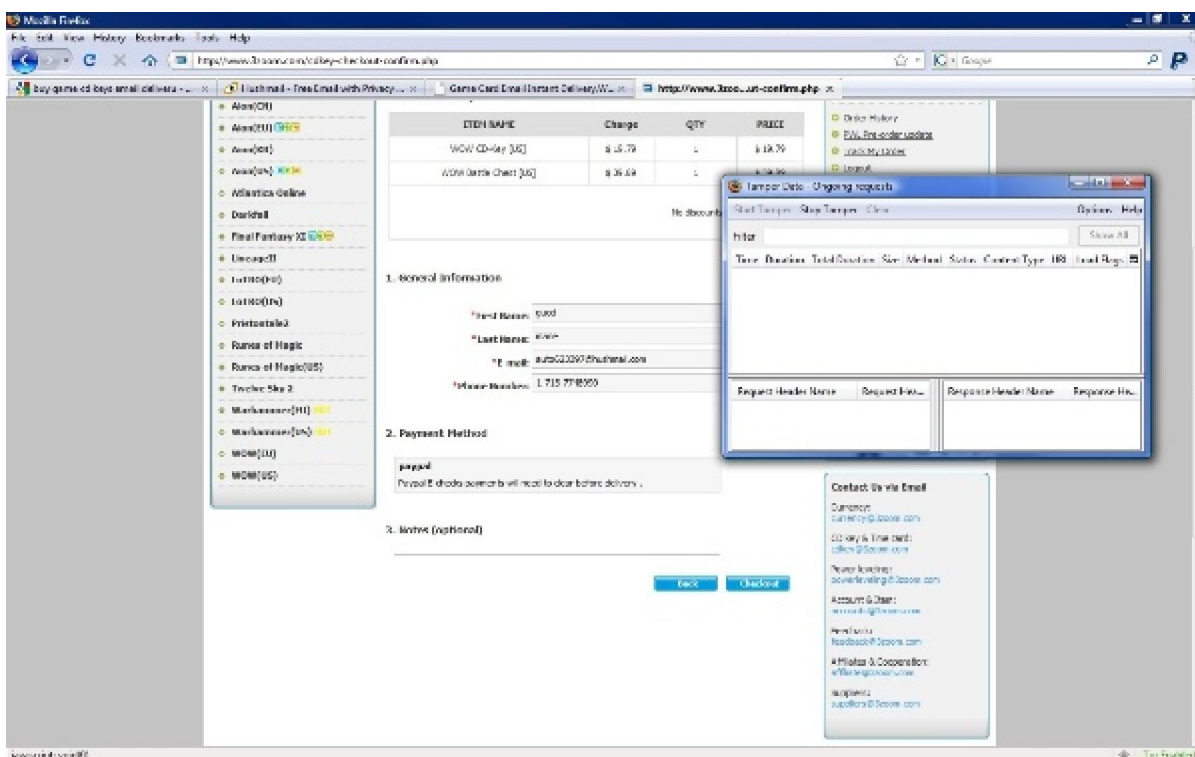
Step 1: If required, make an account, use the same name that's on your paypal



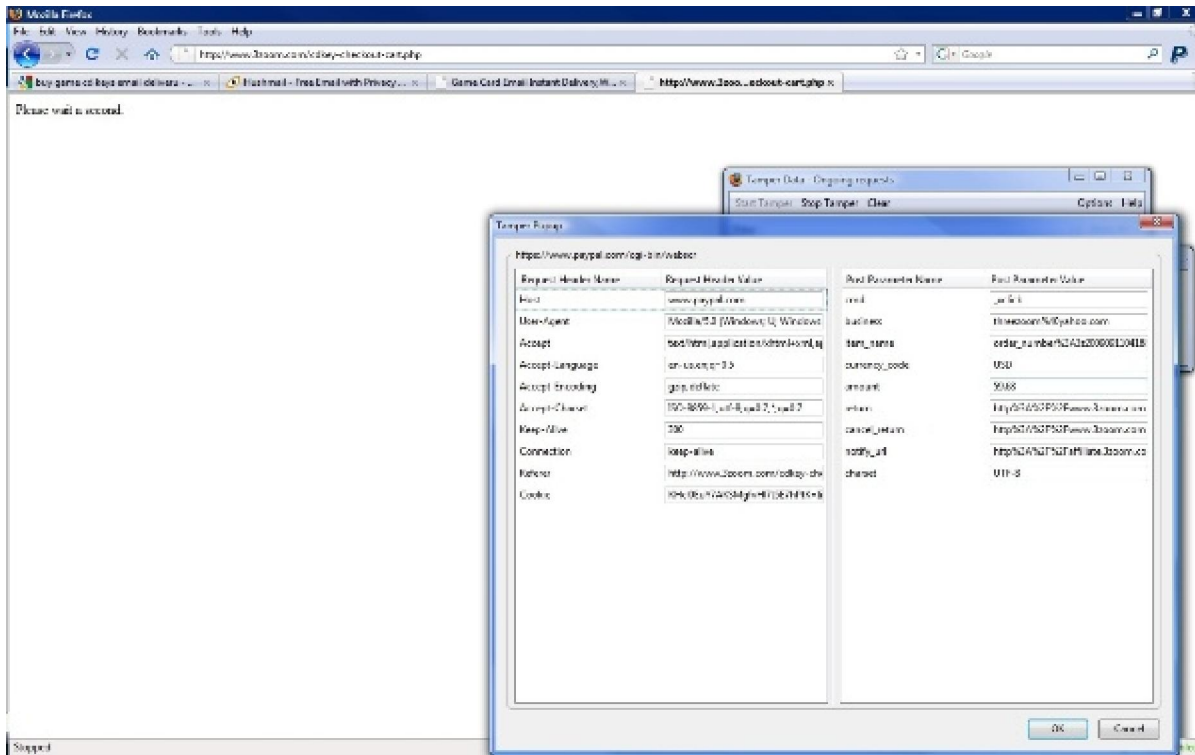
Step 2: Add what you want to buy to your cart, but try to keep it under \$50. You don't need to have Tamper Data open yet



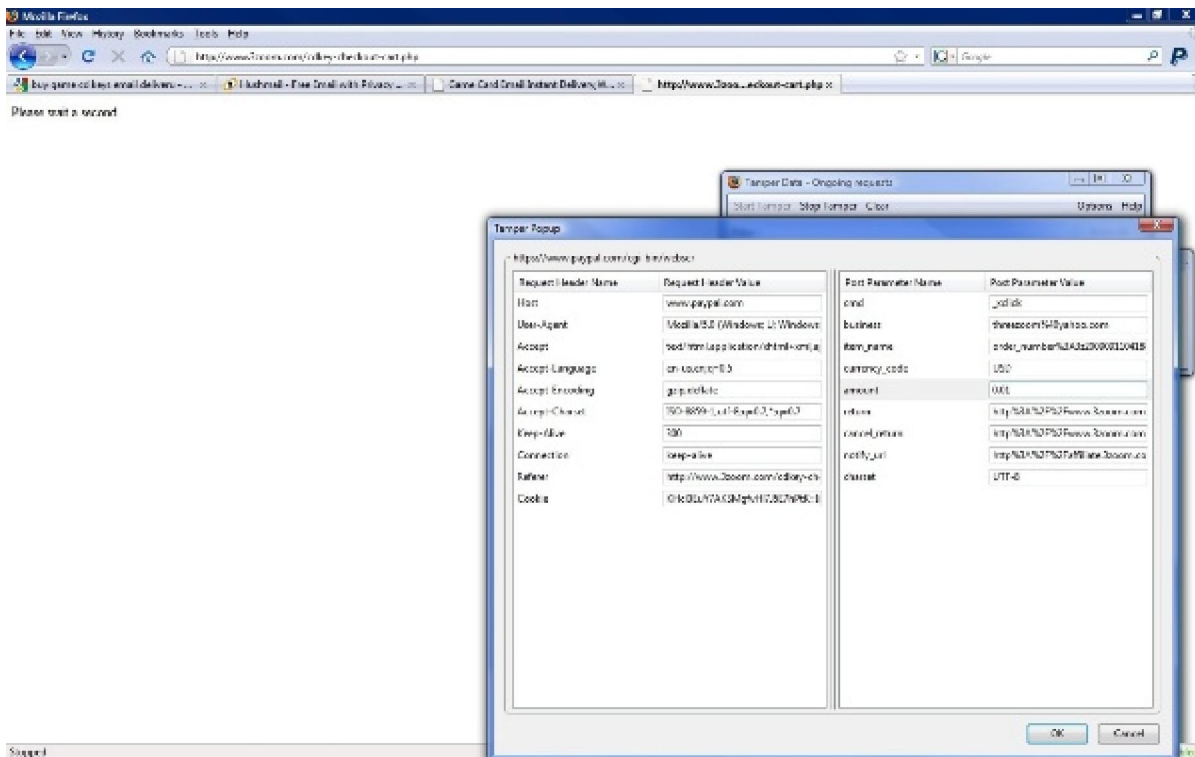
Step 3: Once you're at the final checkout page, DON'T click the checkout button yet. Go up to Tools > Tamper Data and click "Start Tamper"



Step 4: Click checkout, now just keep clicking tamper until you get a window like this. You're looking for the "Amount" field. If it's not encrypted, it will show the total cost of the items you are buying.

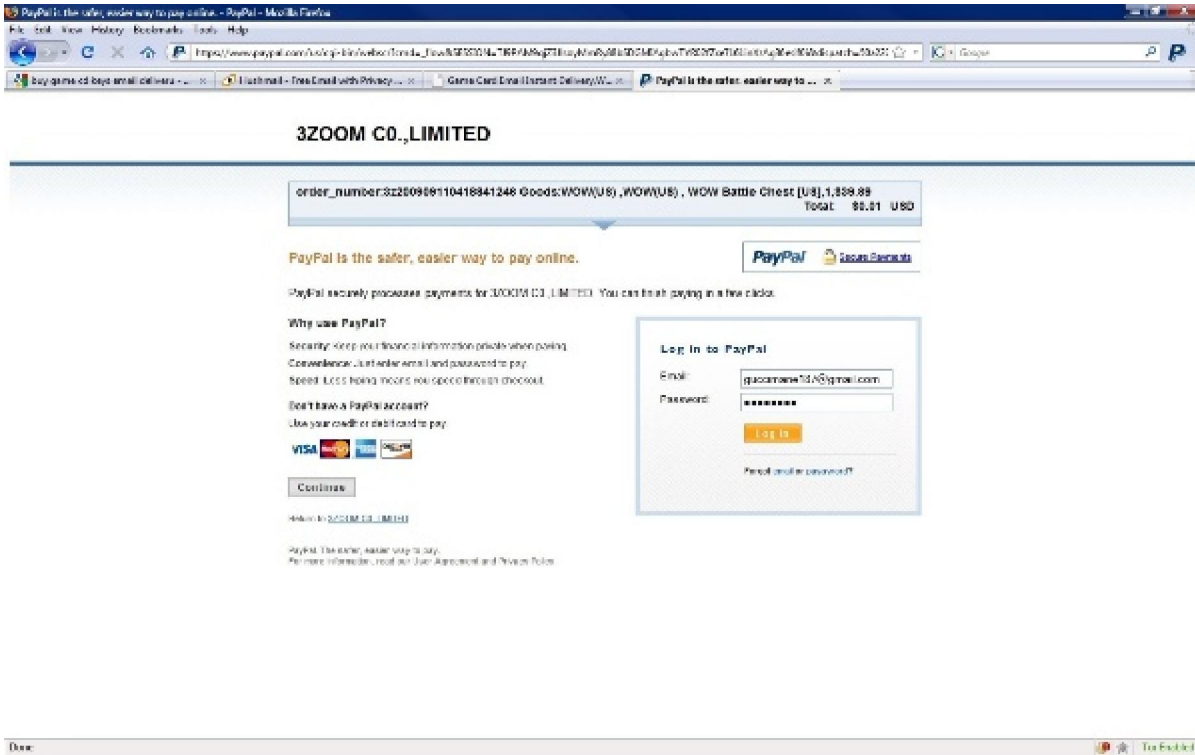


Step 5: Select the amount and edit it to whatever you want to pay, like so.

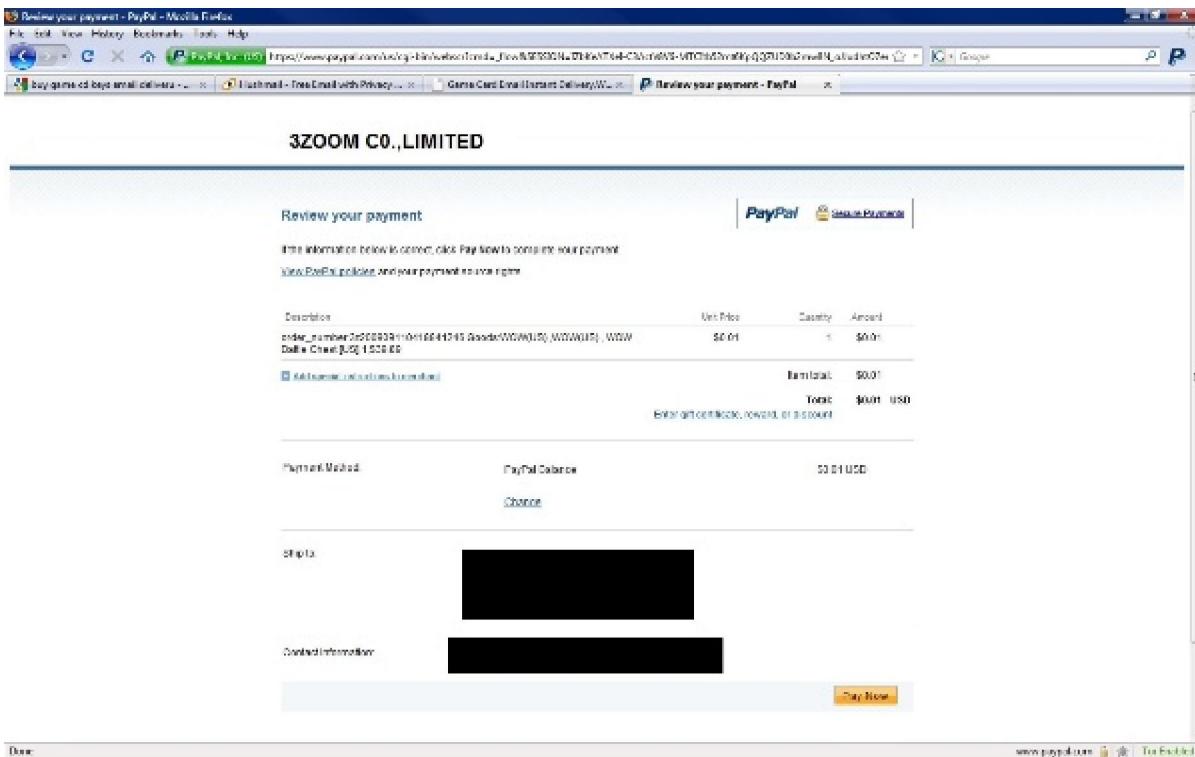


Now click okay and uncheck the "Continue Tampering" box on the popups and press submit.

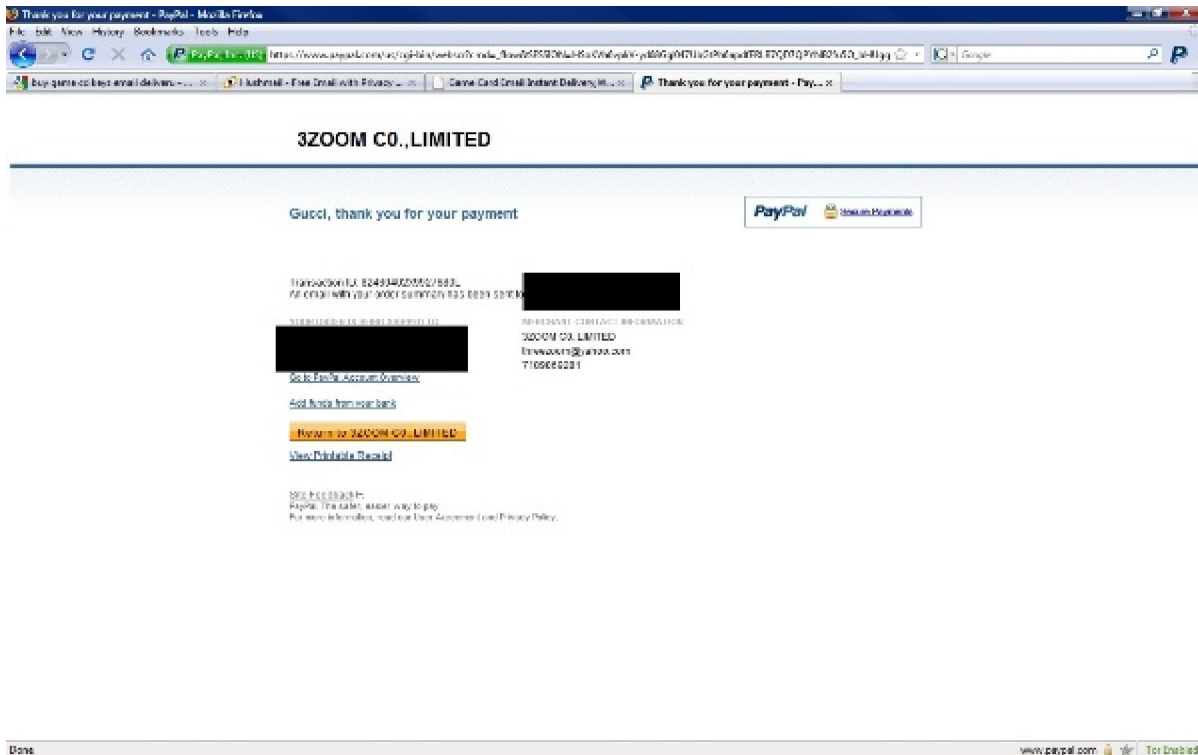
Step 6: It will bring you to this page, notice the total amount in the top right.



Step 7: Enter your password, you'll be brought to this page



Step 8: Pay that penny, nigga



Don't forget your receipt..

Transaction ID: 82460402X9927680L	Placed on Sep. 10, 2009	
Payment For	Quantity	Price
order_number:3z200909110418841246 Goods:WOW(US) ,WOW(US) , WOW Battle Chest [US],1,\$39.89	1	\$0.01 USD
Subtotal:		\$0.01 USD
Total Amount:		\$0.01 USD

That's all there is to it. Now, most of these sites will require a phone call confirmation, so you can either use <http://www.inumbr.com/> to spoof yours, a gophone, skype, or even your own phone number if the company's whois comes up with a Chinaman. The ghettoer looking the site, the more likely this will work. I find that if I spend 5 cents on 5 different sites, I'll get one or two of the orders actually delivered. If all goes well, you will receive an email with a picture of the scanned cd key.

Places to sell the CD Keys:

http://www.markeedragon.com/forums/ubbthreads.php/forum_summary

<http://buysellmmo.com>

<http://realpoor.com>

High Res Links:

Step 1: <http://i28.tinypic.com/foj81w.jpg>

Step 2: <http://i29.tinypic.com/muhj7c.jpg>

Step 3: <http://i27.tinypic.com/i6e2op.jpg>

Step 4: <http://i26.tinypic.com/20794rd.jpg>

Step 5: <http://i28.tinypic.com/2eyjar7.jpg>

Step 6: <http://i28.tinypic.com/z6fdd.jpg>

Step 7: <http://i28.tinypic.com/mr8vti.jpg>

Step 8: <http://i31.tinypic.com/mcunut.jpg>

Step 9: <http://i31.tinypic.com/a1u2e1.jpg>

Tor

Written by: slim-ov-derby

Now most of you will know about tor, if you don't then I recommend reading this site;

<http://www.torproject.org/>

The thing is you can't just download it, let it run and expect to be as anonymous as you think. yes Tor selects the best routers of its own, but if you actually check you'll find that alot of them are in the US and Germany. If you have 3, hell even 2 nodes from the same country and range then the traffic is easily correlated; also the exit nodes are not encrypted and the entry node knows your IP, so imagine how easy it would be for them if they were in the same country.

To make sure you don't get a bad circuit you want to edit the torrc file.

Not all nodes are always available so you'll have to keep checking to see which ones are available.

<https://torstat.xenobite.eu/>

(and the link whilst using Tor: <http://eodys67qpzyvyxm5.onion/torstat/>)

Or you can check them in the *view network* window if you use vidalia.

Also this link lists all of the suspicious nodes that have been blacklisted by Tor as stings, I'll explain what to do with this later.

http://en.linuxreviews.org/Bad_Tor_exit_servers

Now on with choosing the nodes.

The first nodes you choose will be the entry nodes, choose fast ones; if you're using vidalia (which I recommend) then you can see their speeds in the view network window, you can sort them by speed. Choose fast nodes that are in a foreign country (you actually never want to use any node that is in your origin country anywhere in your circuit).

```
EntryNodes node1,node2,etc
```

Now you want to specify only the nodes you wrote above will be used or Tor will use other nodes if yours are down.

Do this by adding this line to your file;

```
StrictEntryNodes 1
```

Now you'll want to choose your exit nodes. I recommend choosing Russian, Ukrainian or Japanese nodes if you can get any, they are unlikely to be interested in what you're doing. I recommend staying away from Nigerian nodes, as while they won't give a fuck about what you're doing they will be sniffing for passwords and login details. Too choose your nodes add this line;

```
ExitNodes node3,node4,etc
```

Like with entry nodes, specify to only use these ones you've chosen.

```
StrictExitNodes 1
```

Now we want to add the nodes that we never want to be used in a circuit; these will include nodes from your own country, unnamed nodes and any that are acting suspiciously. There are plenty of Tor forums out there on the entwork that discuss these type of nodes as well, so keep an eye out.

```
ExcludeNodes node5,node6,etc
```

Note that the node1,node2 etc should be changed to the actual names of your nodes. I know most of you would know this, but there are some idiots who would just c/p everything from this into their file.

Website: <http://www.zoklet.net/bbs/>

Going back to what I said earlier about the entry and exit nodes being in the same country; make sure they're not.

You can't choose middle nodes, so just be careful and keep any eye ou. The middle node doesn't know who you are or what you're doing though.

Once the file is edited and saved, restart Tor so the changes work. Go and check that your IP is changed (http://www.ip-adress.com/ip_tracer/).

If it still uses unwanted nodes then delete the router-cache and restart Tor.

C:\Documents and Settings\loginname\Application Data\Tor\
Delete the cached-status, cached-routers and cached-routers.new files.

Always b on the look out to see if your nodes are still up and which ones are available. Like with your proxies, you should change them regularly.

If you're still paranoid and want that great deniability factor in your favour (comes in great handy when downloading **Certain Pornographic** content) then run your own exit node.
http://en.linuxreviews.org/HOWTO_setup_a_Tor-server

Also coming for great deniability is truecrypt, and of course flash drives which can be disposed of or hidden easily. I'll go into them at another time though.

I will also say, like with other proxies, it will be wise to disable javascript and flash, or you could terrify them with the help of proxifier; but I won't go into that, I recommend just disabling them.

Tor is useless if you are logging into something that's linked to you in anyway, shape or form from the same nodes; unless the account was created on Tor itself.

If you want advice on setting up such applications like IRC and instant messengers through Tor then check this out
<http://www.hermann-uwe.de/blog/howto...-some-pitfalls>

In most cases it's just about redirecting it to go through the port tor uses (9050)

```
Server: 127.0.0.1  
Port: 8118  
socks 5 / server: localhost port: 9050
```

It's pretty simple.

By the way, if you're using eMule for any such things 😊
Empty out the incoming folder. It is not private. Companies search that folder for copyright violations along with your IP address.

It helps you with the deniability factor if it comes to that.

I don't recommend Tor for scams involving credit cards for the following reasons.

A lot of tor nodes are blacklisted on sites where you place credit card orders. Even if you set your own nodes it's not worth it to risk it. More availability to the area it is in with the actual sock proxies, which will help you. You want it to be constant wth that type of thing instead of changing from one location to

the other. And if you have a 3, hell even 2 nodes from the same country and range then the traffic is easily correlated; and I'm sure you know the entry and exit nodes aren't encrypted as well.

Do not get me wrong, I love tor and use it as well as freenet and i2p each for individually different purposes; tor serves well in a lot of areas, just not for certain scams.

If you're going to torrent, please don't use Tor for that, it puts a lot of strain on the server. Use i2p for torrents instead.

Note:

*Managing your entry nodes like that is highly discouraged. Tor is smart enough to pick geographically diverse circuits, and by manually overriding that, you're hurting your anonymity. The same goes for ExcludeNodes. While it can be useful for known bad exits that aren't yet flagged by the directories, there is **no reason** to blacklist nodes because you think they're operated by the NSA or something -- all they can do in that point is give you bandwidth.*

Note also that the fact that the exit node can read your content is not an issue if your content is encrypted to begin with. For instance, I'm on Zoklet right now via https. If I was on Tor, then the exit node would see my content in "the clear" as far as the Tor network goes, but "the clear" for the Tor network is encrypted for me.

An absolute must with Tor is disabling all code that runs on the client-side. This means javascript, flash, java, etc. I have a special Firefox profile I have in an ecryptfs store that has no plugins at all (the less code to potentially exploit the better) and a few choice extensions, including Torbutton, CookieCuller (though cookies are disabled in the browser as well), ForceHTTPS (primarily for URL rewriting), and FireGPG. – By [Prometheum](#)

Everything you need to know about Carding

Written by: *slim-ov-derby, Acetrace*

Carding: Carding: Online, Instore, Going through vendors and advice, Phishing for change of billing addresses

Including drops and what you need to know; Huge guide written by me

Any major updates done to this carding text, it will cover the basics of most carding knowledge. Going into absolutely everything would mean having to go onto ID theft and fake IDs which can be classed as 2 different categories of their own.

What I'm going to cover:

Online Carding

- A quick overview of what online carding is
- SOCKS and why we use them
- Finding a cardable site and what cardable means
- Carding "non cardable websites" with fake CC scans and other fake documents

Carding while on the job

- Getting CC, CVV, CVV2 through use of mobiles
- Skimming whilst on the job
- Using carbonless receipts to get details (pretty outdated method)

Trashing

- Trashing for receipts and credit reports (pretty outdated although still works)

Phishing over the phone

- Phishing over the phone for details

Keylogging for CVV2s

- Hardware keylogging

Carding Instore

- What instore carding is (very brief)
- How it's done
- How to act and present yourself instore

Carding over the phone

- Carding over the phone

IRC

- Services provided in IRC
- Advantages to using IRC for info
- Disadvantages
- How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)
- Vendors and how to approach them
- How to rip in IRC (EVERY vendor, reliable or not has ripped some n00b who acted like they knew what they were doing)
- :::WU BUG BULLSHIT and how to rip n00bs and gain more:::

Phishing for Change of billing

- What COB is and why it's useful
- Use through phishing pages
- Use through keylogging

Drops and what you need to know about them

- Drops and what you need to know about them

What carding is

Carding summed up quickly is the act of obtaining someone's credit card information, from the CC#, CVV, CVV2, CVN, and the billing address, along with the expiry date and name of the person the card belongs to along with a signature.

Online Carding

Online carding is the purchasing of goods done over the internet with the CVV2.

Now for you n00bies you're probably wondering what a CVV2 is, it's simply just the database of basic info for the card such as the card type (e.g. Mastercard) First and last name, address and post code, phone number of the card owner, the expiry date (and start date if it's a debit card or prepaid CC), the actual CC number and the CVC (card verification code, which is the 3 digits on the back of the card).

This is the format you usually get them in when you buy off IRC:

```
:::MC ::: Mr Nigerian Mugu ::: 1234567890123456 ::: 09|11 ::: 01/15 ::: 123 ::: 123 fake street, fakeville,
::: Fake City ::: DE24 TRH ::: 01234-567890 :::
```

SOCKS and why we use them

Now with ANY fraud at all you have to take precautions so you don't make it easy for anyone to catch you in your wrong doings. As usual I swear against TOR for carding/scammin because most nodes are blacklisted by websites and because TOR cycles through various different proxies; and even if you configure it to go straight through an exit node of your choice it's still not worth it. You can use JAP but make sure you're using some constant sock proxies from the same city, town or area that the card is from; also go wardriving and use a VPN (don't trust anyone off IRC with these, you'll have to do some searching around yourself for a highly trusted one and one which won't comply with LE).

You can get good SOCKS from anyproxy.net (people are selling accounts for the site in IRC all the time), that's the best place but even I ended up losing the account eventually (unknowingly I was sharing it with some Nigerian dude who became selfish).

So we use SOCKS because they stay constant. But don't let that get your guard down, you want FRESH proxies everytime you card.

Finding a cardable site and what cardable means

Basically a cardable site holds these characteristics and what you should be looking for to determine an easily "cardable" website:

- The top one you need to look for on the site's TOS is that they send to any address and not just the one registered on the card (although you can easily get around this if they don't, with a COB, photoshopped verification (will go into detail later) or some social engineering over the phone).
- The next important to look for is if they have a visa verification code or mastercard secure code (most of the time if you ask your vendor they'll include them in your CVV2 details textfile), if they do have one of these you have to put in and you don't have them then don't waste your time
- If they ship internationally (for obvious reasons, but you can just stick to local websites and order to your local drop)

- If they leave packages at the door when no one's in, or around the back in a safe area (I know of one site in the UK that has all these qualities including this one, it is perfect for carding clothes)
- Also you can't forget to see what other security checks they need to do (if they need to call you up to verify or want a utility bill, passport or a scan of the actual CC)

It is hard to find websites online now that have most of these qualities, therefore we have to use COBs and photoshop to help us along the way, which is what I'll go into now.

Carding "non cardable websites" with fake CC scans and other fake documents

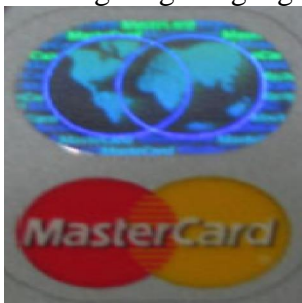
Okay so say you come across a site that will deliver to another house not registered on the card, but they want verification either through phone or scans of a utility bill, credit card or passport.

For this you'll want to get a pay as you go deal for a cheap shitty mobile all in fake details (say a nokia 3210, brick LMAO!), or you can use spoofcard.com to your advantage to help you. Hell if the person's details you're using is local to you and you're daring then go to their home and beige box from there; it'd be very convincing.

If they speak to you over the phone have all details in your mind about the item you're carding, have some bullshit story if you're having it sent to a diff address such as a family member's birthday and you need it there as quick as possible as it's a last minute thing, or some shit like that. If you're carding multiple sites at the same time it's easy to get them mixed up, so make sure who it is calling you 1st.

For CC scans and how to do them check the attachments at the end of this file, they explain so much better than I could. How you use them is once you've made them like the tuts have said to do, you then tilt them a little bit so it does actually look like a scan. To make it even more believable put some paper in the scanner (dark shade if you must), scan it and open in photoshop and then put the shopped CC scan of the front onto it and then do the same with the back, then send the scans to them via e-mail or post. Same goes for utility bills (can be got through trashing or your own, and then edited in PS).

Do not use the same designs when making your CC scans, otherwise it will become too obvious. To give you a head start on mastercards (what I recommend for n00bs to go for) I'm giving you a globe hologram image so you won't have to buy them in IRC; unfortunately all of my visa hologram pics are shit, but I'm working on getting a good one soon.



Carding whilst on the job Getting CC, CVV, CVV2 through use of mobiles

Believe it or not giving your information out to anyone anywhere is not a wise choice, you can not trust anyone in this day and age. Yes there are carders working on the inside in places where there are a lot of people around flashing off their plastic cash and using them freely without a care in the world. The most common of places for a carder to work at are brand label clothing stores such as Limey's, Charlie Brown's and all the other trendy shops.

Ever noticed when yourself or someone else has paid at the desk with a debit card or credit card that they

bring out a keypad from under the desk, then put your card into it and have the buyer input the pin? Think again when they take your credit card and go under the desk with it to get the keypad, they are doing more than just that; just because they're not taking the card and running off with it does not mean they're not stealing your information. A friend of my dad used to card and work in a clothing store, he used to have a piece of play doh stuck under the desk and he used to press the card onto the piece of play doh, unfortunately he began doing it too much and because he'd gotten away with it so many times he became careless and got caught out by a co worker and from what I know he is still doing time. The moral is, be careful with the play doh method. The unfortunate thing is you can only get the full info of 2 cards at the max, and you don't know exactly if you're pressing over the info of another card already put on to the play doh. Also you can't get the CVC through this method, I was just giving a classic example from the olden days.

But there is a new wonderful invention called cameras, video recording, and mobile phones and they are even all working on the same thing. It's best to test it out 1st and have a camera on your phone that is at least over 2 megapixel and allows long enough video recording times. The phone is set to video record and on a lighting if needed, and taped underneath the desk for you to record both sides of the card for all the information you need, as well as being quick you can get a lot more than 2 on, depending on how long each recording lasts, you may need to start more than one recording.

You need good reason to be going under the desk to get the chip and pin machine, so make the desk look cluttered up and put shit in the way of everything, such as coat hangers and various other items; or you could just flat out bullshit the customer and say that the chip and pin machine on the desk isn't working so you need to get the other one, take their card and then go under searching the desk and quickly show it to the camera phone and then get the chip and pin machine and put the card in it and then hand to the customer to put in their pin as normal, unaware you have a CVV2 to later use when shopping online.

Skimming whilst on the job

For skimming you'll want a mini portable MSR500M reader that can be fitted on your waistline belt or of course once again under the desk, if you're a cashier. But you'll also want a MSR206 writer if you plan on writing the tracks to an embossed CR-80 piece of plastic later (you can make these yourself but embossers are expensive and it's an expensive procedure, so wait a while until you do that yourself and buy them from IRC (be careful, people like to rip with plastics, or you'll get shit quality if you don't watch out).

If you plan to just sell the dumps on IRC then that's fine, but you'll still need the PIN as well, so if you're a waiter you can get a cheeky peek at them putting their pin into the chip and pin device while you keep hold of it slightly (have them put the pin in while they're sat down and you're standing up). It's much easier to skim in a restaurant rather than clothing retail, as you don't have to think it out and set it up as much. You can keep the MSR500M in your front pocket of the uniform you're wearing and pretend to be giving the card a clean on the sleeve (bullshit and say the device won't read it), while really you're giving it a swipe into your reader. This way the person doesn't even get suspicious because you don't take their card out of sight with them. I guess you could do that technique with clothing retail too when you get their card in your dirty little hands, but peeking for the PIN is harder or you'll have to have a friend shoulder surf for it (or if they're on the next register have them use a sony cyber shot c902 camera phone and pretend to have them talking on the phone while really they're recording the person next to them putting in their PIN; cybershots are really inconspicuous looking with their cameras and VERY clear [5mpixel]).

I'll go into detail what to do with the dumps you have later in the instore carding section.

Using carbonless receipts to get details (pretty outdated method)

If the store you work at hasn't gone carbonless on the transactions information then you can get most of the info from the receipt you get a copy of for yourself and note down the pin on this as well when/if you

get it.

Trashing

Trashing for receipts and credit reports (pretty outdated although still works)

Ever heard the expression "Another man's trash is another man's gold"? That's exactly what this is. You'd be surprised how many people haven't heard of a paper shredder or bonfire. They just dump their financial records containing SSN's/NI, full name, address, bank, credit card number, CVV, CVV2 etc. All on forms people couldn't be bothered to dispose of properly because they thought they were JUST old records. Again carders work on the inside again for when they want to do trashing, a lot of janitors wear rags but you'd be surprised how secretly rich most of them are (along with the other shit they steal from work as well). But also from this if there is not enough info for you on the forms then there is definitely the phone number of the mark on the form that they've scrapped; almost always, and if not then there is enough info on their to look them up in the phone directory. Then of course you use social engineering skills over the phone to get the extra info that you need. If you know of a store that is not carbonless, then go trashing in the bins at the back of the store for the receipts with the credit card details on it.

Phishing over the phone

Phishing over the phone for details

Ever had telemarketers ask for your credit card info over the phone? (this is if you haven't already hung up by just hearing a nigger or paki on the phone) chances are they're a carder. Believe it or not there are people actually stupid enough to fall for these obvious scams. Even more people fall for this if they believe that the caller is from the credit card company itself or part of the secret service or credit fraud investigations; the FBI, CIA and police have nothing at all to do with credit card fraud believe it or not. If you sound professional or part of an important group such as investigations then people are more likely to comply with you if they believe that their card has been used for credit fraud purposes and have to give their credit card info and billing address for verification. The best time to call up the mark is when they are at work as it'll take them by surprise and they'll be wanting to get it sorted asap so that they can get back to work. Also if it's "serious" then the secret service don't wait for you to finish work before they question you. Play along well to the part you're pretending to be. Some social engineering skills are required and you must gain the experience of lying to people yourself. Before calling up the person find out as much information about them as you can.

If you've stolen a CC from someone personally you can call them up pretending to be their bank and tell them there has been some suspicious charges made to the credit card from places such as South Africa, Nigeria, Turkey, Russia; places like that, get them to confirm their details (milk as much as you want out of them, ask them bullshit security questions such as their mother's maiden name, address, etc; you may as well, it'll make it easier to get a COB for you to use).

You can also get their PIN out of them if you want as well by either straight out asking them to confirm it, or be crafty and after you've told them to verify their PIN you're putting them through to a different department; then play some cheesy music down the phone for a few mins, have a female voice recording (use AV voice changer) asking them to input their PIN on their dialpad (this won't be as suspicious); get these recorded so they can be decoded with DTMF decoding hardware/software later (although it's expensive). Guessing DTMF tones is pretty easy too, but you need to know what each tone sounds like, it's preferred to use decoding software to ensure you have it correct.

If you try hard enough you can get full info about anyone over the phone (I suggest using spoofcard for this).

Keylogging for CVV2s

Hardware keylogging

First of all it's best if you use hardware keyloggers here that you put into the keyboard of a computer belonging to an area where a lot of people are going online a lot and logging into e-mails, ebays, paypals etc, pretty much giving you enough info for you to go searching through if you get in their e-mails, or maybe you're lucky enough to get someone who is buying something online anyway. Get the keyloggers from here:

<http://tyner.com/datalogger/keycatcher.htm>

And come back within 2 days time or so and collect the keylogger after doing some browsing yourself (as to not look suspicious just coming in and then leaving a few seconds later).

Or of course you could set one up in a business and do the classic call in and do some social engineering from the credit card company or secret service and have them go to the bank online and have them log in to verify, or maybe even have them log in to a fake bank online made by yourself that will collect anyone's info who logs in on it.

Carding Instore

Instore carding is the act of skimming a credit card and writing the dumps and track1+2 to a CR-80 piece of plastic and then either cashing out at the ATM or shopping for goods instore, as long as you have the PIN as well through whatever method you choose to use.

How it's done is through the use of thejerm software or any other magstripe utility software (thejerm is the best to use). And you do it like this:

1. Load up thejerm's software
2. hit settings tab
3. hit "Defaults" in Leading Zeros box
4. hit "75 bpi" in Set Track 2 density box
5. go bak to actions
6. hit LoCo or HiCo in Coercivity box, depending on which you want to do
7. input your tracks 1 & 2 (without the % ; or ? symbols because the program already does it for you)
8. hit Write Card and swipe your card. (i usually do a read card afterwards to make sure everything went ok)
9. GO SHOPPING!!!

Download thejerm from here:

<http://rapidshare.com/files/154030787/thejerm.rar.html>

Now how you should act when you go carding instore is pretty much common sense, but some people get caught up in the moment with nerves, cockiness or just too much weird amounts of excitement.

Simple what you do, make sure you KNOW the PIN for the card you're using before you go, don't be

stuck at the counter trying to remember it. If you're going to be carding expensive goods then dress smart for the occasion, wear brand named clothing (that you've previously carded :P) or even a suit. It would look suspicious someone with a hoodie going into a store and buying a Louis Vuitton watch, so walk in with style. When you go instore, you ACT like you are using your own card, because essentially that's what it is (well it is now anyway lol) no looking shifty and don't look at the fucking cameras; the cameras mean nothing anyway, they don't know your name or where you live, they're not being watched half of the time, so stop worrying about the fucking cameras; remember you're doing nothing wrong. When you go in, don't rush take your time, browse around some other items. Find the item you want to card and even ask the employee simple questions about it (if it's a TV or comp just ask questions about certain specs and if it's good for playing video games on). You'll be most nervous at the checkout, just act as normal as you always have been, don't make too much small talk but be polite and civil. Once you have the good sin your hands don't bolt out the door, just say thank you and then casually walk out the door, get to your car and then celebrate all you want.

Carding over the phone

Okay 1st of all do not be a dumb fuck now, do not call from your own phones at all. For extra lulz you could use a beige box and call from someone else's phone but that's a totally different game all together and is also a major felony to go against you on the chance that you do get caught so we'll keep it simple and use a payphone (it's not AS risky to phreak these but the only recent red box tones I have are from the year 2007 and I'm pretty sure they'd have changed the system again...bastards, I'll check sometime though 📞) to call them up. Do not put on a stupid voice at all, the salesman/woman will know and it'll be a cause for investigation during the mailing of the goods or the requesting of them. Just be calm, cool and talk to them as you normally would if you were ordering with your own card. They'll ask for a name, name as it appears on card, phone number, billing address, expiration date, method of shipping, and the product that you want to buy. Also when trying to not seem so shifty be sure to ask questions such as if they can deliver the next day or 1st class, and if they can order it to your "relatives" house so that it can be there for their birthday; maybe even ask if they can write a message to go with the gift as well on your behalf. The next day postage is said so that they have less time to look up details on the order. Some cards will have difficulty shipping to any address other than the billing address, but it doesn't hurt to try. If they start to question you then just answer the questions and talk your way around the situation with your social engineering skills; don't just run away from the questions or hang up straight away, otherwise that is cause for suspicion and they may investigate. If all goes well you should have your item of choice delivered to your drop location or a house of someone else's address who you don't know and call them up saying that you called up the store and they've sent the package to the wrong address and it is still sending there, and ask them if they could kindly keep and sign for the package and you'll pick it up after work (this is a last resort and only to be tried if you're good at talking to people, which you should be if you're a carder). I recommend checking out the section on drops later on in this text.

I recommend using spoofcard for verification over the payphone, if they need to verify (if they won't send without some verification which is usually the case).

IRC

Services provided in IRC

IRC is the main gathering for fellow carders, scam artists and rippers. To put it in a nut shell, IRC is THE black market, unlike craigslist and eBay which are just black markets. You can get anything illegal off IRC from CP to warez to CC details (which is what we want).

To concentrate on carding though you can buy:

CVVs

CVV2s

SSNs

Utility bill scans

CC scans

COB (a service to get someone to call up the victim's bank and get the billing address changed to your drop)

Payment for using someone else's drop and then sending to you

Spyware

Fake ID/ ID scans

DUMPZ

Phisher pages

The list really is endless

There are a lot of advantages to using IRC networks and channels which I'll go into now:

- The channels are often underground and not known to many people, so they're harder to stumble upon by some random guy.
- The messages can be encrypted so they can't be read by anyone happening to be on the network sniffing the traffic. This makes it harder for investigators to uncover.
- Easier and quicker to communicate with mass amounts of like minded people.
- Variety of channels to go to if one doesn't suit you (there are MILLIONS and new ones being made every second, guaranteed).
- And of course a variety of services, if you need something you can bet someone from the other side of the world will be willing to share or/and sell to you.

There are a lot of disadvantages though, IRC is the equivalent of a backstreet alley, you'll be fine if you stay cautious, here's what you should be weary of:

Viruses

- If you don't have strong anti viruses and firewalls you will get infected (no norton shit, kaspersky and NOD32 are what you want)
- Do not accept random .exes or any file for that matter
- It is easy to get ripped off, choose your forms of payments and who you deal with wisely

How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)

Here is the most commonly asked question I get asked by n00bies and fellow carders; where do you find these channels?

If I'm being totally honest the best place to find out about them is through Nigerians; no bullshit that is where I found out about a lot of the carder channels I used, also how I found out about forums and their IRCs too such as cardersplanet, darkmarket etc. How I found him out was just on a normal scam bait I was doing, it wasn't a long one, but in the end he tried phishing me so I tried back and we had a laugh about it; I was straight up with him and told him I wanted to get deeper into the game, I looked up to his

type of people and wanted to get rich/successful (I also shared the double claim secret about paypal with him which got him trusting me a little bit) he then sent me an invite to cardersplanet (this site was full of Nigerians). Eventually I went in the IRC (admittedly got ripped a few times) then started vending myself under various diff nicknames, then moved onto different sites like darkmarket and cardingzone when I'd got invites for them (although cardingzone is shit it's good to get in the IRC for starting off, you'll get invited to better forums the more you hang out in IRC, trust me). Don't ask me for invites to cardingzone, I was banned for ripping (I didn't rip anyone 🤡)

The quicker way is to use these and search for certain keywords:

www.irclinux.org

www.irctrace.com

www.ircllog.org

ircarchive.info

www.irc-chat-logs.com

<http://www.irseek.com/>

And of course don't forget google.

I'm only going to give you one clue for searching through google for a carding IRC, and that word is "undernet".

Fellow carders don't like revealing their IRCs, and for obvious reasons.

My advice is find a scammer through e-mail, and chat to him; be witty with it but be respectful to a fellow fraudster.

Vendors and how to approach them.

Vendors are the people in IRC who are selling and providing the services for you. There are certain ways you should speak to vendors otherwise they're going to rip you (remember this is the black market, this is just like going up to a random drug dealer in the street and not knowing what you really want or what you're getting into; you'll get ripped off). Ask as many questions as possible of what you want to know, if you're buying a CVV2 ask to see proof of their details working (get them to make a small purchase somewhere; they should show you a before and after and the limits that are there on the card [there are methods out there of checking your balance; you can even get it through text/sms]. This is a market so remember there are more people that will be willing to buy from that vendor, it's open for all, you can get a full load of info including dumps for as low as £3/\$5, drops usually go for £7; if someone is saying higher prices don't be afraid to haggle down to these prices or a little bit lower. COBs go for a little bit higher in ranges of £15-£20 because the vendor needs to get full info on someone and then change the billing address through the bank to where ever your drop is.

Now when you go in the channel don't fucking say or request anything, shut up and see what the vendors are saying they have to offer and then send them a private message and talk to them. If any "vendor" messages you 1st trying to push onto you to buy from them then they're most likely a ripper; however don't piss off the rippers or assume someone is a ripper because you never know who is going to be there to help you out later on down the line or who might be pissed off enough to fuck you over.

I can't give any big advice on not getting ripped in IRC because you don't personally know anyone in there at all, you just have to take your chances (expect to get ripped your 1st few times going in there, just don't go to them again, because if they get away with it once they'll definitely try again if you go back to them).

DO NOT BUY ANY WU BUG (Western Union Bug); it is a massive ripper technique which is bullshit. The WU BUG used to work but was patched a looong time ago, most of the time now you'll get nothing or you'll end up with a rootkit on your comp. Rippers always say ridiculous prices for these too such as \$200+; but if someone says lower prices it's still bullshit and most likely a rootkit/trojan/keylogger going to be installed on your machine while you get some useless program that does nothing.

Ripping

Easy as hell to do, not much photoshop skills needed really either.

Bullshit and say you're selling full info (you're getting the info from fakenamgenerator.com or any credit card gen program; of course they don't fucking work), if they want to see proof just use your own legit CC or another stolen CC to buy something and show them proof of you buying it, except photoshop the details to that which you're going to be giving him later. Take payment through Western Union ONLY (since e-gold isn't around anymore), then just send him the bullshit info.

If they want the report to go to their phone via SMS then just spoof a text with an sms bomber saying some bullshit reports. Then get the payment via WU.

To get victims you message them 1st, message out in the whole channel 1st and then PM random buyers (look for ones requesting).

::::WU BUG::::

seriously this is bullshit, all people are doing are showing buyers fake screenshots made in PS or are actually making quick programs themselves and taking screens of them and then selling them, although essentially they're useless. You want to do this, but you want to actually send them a file as well, but bind a keylogger or trojan to it; not only can you rip them out of their cash to buy your infection but the info you get from spying on them will be so much more as well ranging from their info to other stolen CC info, you'll have a backdoor on what they do and can exploit it.

If you can't be bothered making fake screenshots then get them from other rippers trying to sell them, get them to show you pics, vids and info; then use it for yourself and rip some n00bs.

Phishing for Change of billing

A billing address is the details used for a person's bank account and most often their credit cards and everything else too, this includes their phone number too.

What a change of billing (COB) is in a nutshell is changing the billing address registered to the card to your drop address you're gonna be using. When you want to card BIG at various online websites the orders will look more legit that you're not sending it else where other than the one registered to the card (obviously after you've changed the billing address), meaning the delivery of your goods will be quicker and will require a lot less verification.

Most of the time you change the billing address over the phone but SOME banks will let you do it online; when you phone up to change it you use spoofcard.com or the pay as you go mobile phone you're going to be using when carding, or beige boxing :P

When changing the billing address you need to know as much info as possible about the person's billing address you're changing, because the bank is going to ask you 3 security questions you set (such as mother's maiden name) before they change it.

You can phish for details over the phone (see the phishin over the phone section above), however it's best to use keyloggers and phisher pages for this with a MIX of over the phone.

Use through phishing pages

2 methods here, 1 including over the phone, one isn't.

The method without the phone is to just send a ton of e-mails out to random people and send them a html e-mail telling them they need to update their information before the account is suspended or their account with the bank will be cancelled, you have them go to a phisher page off the template and the phisher pages "requires" them to answer security questions like their mother's maiden name, their pet's name, you know those type of questions.

Another method is to call them up pretending to be the bank and saying there have been different ip ranges logging on their account and they need to confirm their details online, link them to the phisher page and have them fill in the details; have the phisher page redirect to the actual online bank's login page; then ask if they've done that over the phone, tell them to wait a minute while you confirm and check it all out, say it's all clear and tell them to log in, they'll think nothing of it and you now have the answers to their secret questions which you can give to the bank itself when you go to change the billing address.

Use through keylogging

This is my favourite method and what I told S_E last night in IRC.

You have a hardware (or software) keylogger set on someone's comp, use sock proxies when logging into their online bank account and then change their password, call them up pretending to be the bank and then get them to go to the actual online bank link and fill in their forgotten password options (answering secret questions) or of course get them to go to your phisher page and fill in the details (this is if you want to add more fields to get more info) then pretend to be checking it all over, then change their password again to some random letters and numbers and give it to them to log back in (it doesn't matter because they're keylogged and you'll get their new login if they change the password again anyway), you'll have all their info logged down too for you to answer your questions when you call the bank.

Best time to do all of this is around the 10th day of the month (people usually get their credit reports at the start of every month), this will give you plenty of time to card enough for the remaining days until they see they're not getting their reports coming to them anymore (if you're crafty you can pretend to have cancelled the online bank account for them after they've gave you the info you need to know; I used to do this method and keep it going without them knowing).

You need as much info as possible when calling up the bank to change the billing address.

Drops and what you need to know about them

Drops and what you need to know about them

What drop locations are and what they're used for

Well simply a drop location is an abandoned house, or any house that is not under your name or any of your details. You can lead young children into these to make a sexy time with them, get items delivered to them that you want no one else to find about or risking finding, or just use it to squat in if you have no where else to go. Basically they are used in ways of keeping your nose clean and are used by mostly scam artists and sex offenders.

How to find a drop location

There are many ways of finding a drop location for use, whether it temporarily or permanently (although I suggest swapping and changing locations because my main last one I used got raided or broken into and is boarded up and too hot to use); I will suggest 3 ways on how you can find some for you to use.

One final tip is don't bother going for houses that are boarded up at the front where it is visible to passers by (it's okay if round the back is boarded up)

Website: <http://www.zoklet.net/bbs/>

Way #1

As just mentioned you can go about it many different ways but one of the ways the way I prefer to go about it is you should be looking around some older housing estates and more ghetto areas (could also tie in with the sob story you feed to a paedophile/child predator you are possibly scamming). For example in Derby there is an area called Sinfin, but now there is 2 parts to it and they are New Sinfin and Old Sinfin. Old Sinfin is the are you would want to go to, because it's older it's most likely to be alot more houses abandoned or deemed unsafe (it's bullshit).

Or if you were lucky like I once were then you could ask around your mates if there are any empty houses in their area. If there are then you're in luck and can even have your friend keep tabs and watching over it for you and give you details so you can keep it all under wraps and safe. It may be alot riskier with neighbourhood watch morons, and nosey neighbours, but it's still ideal and a little bit less suspicious than the abandoned houses in the older estates, and this is because the older estates usually have all abandoned houses close by, where as the odd one out covered with a street filled with inhabitants will seem less suspicious to the postman.

Way #2

Now this is a temporary way of finding a drop location, but is sometimes an effective ways and means of getting what you need but has a bit more risk to it; and personally is a way I have never used even till today.

Have you ever been eavesdropping on a conversation between a neighbour and one of their family member's or friends', or been down the pub and heard the common as muck chavs boasting about a holiday they are going away on for however long they say they're going away for?

Well listen out for these type of conversations. Because them away on holiday means the house is most likely going to be empty for however long they're going away for. So if you already know where they live then that's great the job is made easier; if you know their first name and surname then look them up in the phone directory and find their address to go along with the number. If you don't know where they live, or their name then just listen out to see if you can hear their names come up in conversation; just remember that if it's in the pub it's most likely local to it that they live, so you could easily find out by following them home and seeing.

Way #3

Possibly the safest, easiest way of finding, and quickest way to get a drop location.

Most areas have houses up for sale am I right?
Or houses that are up for bidding on, am I right?

Well they have a website with a full list of your local area(s) that have houses up for bidding on and for sale.

For example I would search Derbyhomefinders and look at the list on their site.

All of these houses are empty and often do not have a sign up outside them either (if they do then just take it down and hide it somewhere for the time being).

The advantage to using the lists to find the drop locations to use is it will usually say when the bid is up or if the house has been sold (this lets you know that it will not be ideal to use that certain house now it's most likely to be inhabited) and will have the houses on there that are still being bidded on and that are still up for sale, these are the ones you want to be using.

The best thing about this though is that you have a full list of many different drops to use (like I said

earlier it's best to switch drop locations and use many different ones) and it is updated with new ones coming up and tells you full which ones are over and not usable.

You just need to know your agencies for housing and find their website.

Obtaining and using drop locations

You're probably thinking now I've got/found one that's great and everything but how the fuck do I keep it a secret?

For way 1

this much is obvious that you do not tell anyone except your partner if you're doing a team bait, and 1 trustworthy friend to keep tabs on it if you are doing a bait on your own, and also the paedophile, but only when he asks. But there is alot more to it than that, also maintaining your abandoned house and making the postman think someone living there.

Appearance isn't everything at all in any case and it isn't for this either, but of course you try to make yourself look as best as you can. The same principles are applied to keeping an abandoned house; you should atleast try to get a new lock put on the door which you will also have a key for; just so that if any druggies go there before you then they will have a tougher time getting in (of course it's ideal you don't get somewhere known to druggies but this is an example of what use it could have) but also if there is a fucked up lock on a door then it's pretty damn obvious only low life scum or some criminal(s) are using the place, so buy a new lock for the door and get it fitted on, whether you do it yourself or get assistance from a friend who knows what they are doing.

Now as for overgrowing plants and weeds, you can only do so much without being suspected. Do not use a lawn mower, use clippers and hack it as short as you can. It's best to get all of this done when everyone is at work during the day time; but in reality it isn't ideal at all and most criminals don't tend to bother with this. Instead they will make it seem someone is in but is just too ill to do anything with the garden or is just a lazy fucker. They do this by often writing up a note and sticking it to the door or leaving it on the floor near the door saying something such as "No milk today please" or "Not in, please leave packages at post office".

Write a few letters to yourself as well ready to come on the same day as the parcel, this will make it look like you get mail and not just the one off suspicious package now and then.

Now 2 alternatives, you can either get to the abandoned house and take the mail from the mailman while acting like you live there (you must look the part as lazy or disabled if you have ingrown plants in "your" garden) or you can leave a note saying to take any packages to the post office for pick up because you are at work or something along those lines.

One final rule is do not be in and out of the hideout everyday or whatever, visit probably 2 or 3 times a week.

Way 2

Now there are 2 ways to go about this; you can either just get to the house early in the morning a little bit just before the postman arrives and be at the house outside pretending you're just about to leave and then sign for the package (if you need to) and collect it off the postman and then be on your way after he's gone. Or if you're good at bypassing alarms (I have a guide on burglary) or the house has no alarm then you could bump key in at night time (not recommended) or during the day time the day before when everyone else will be at work aswell, and hide out there for a bit (hell even take some food that is left in the fridge and feed yourself since you're spending the rest of the day and early morning there). Basic rules are don't have tv on too loud if at all, or if you do then put head phones on into the tv if it's that old of a model, and leave everything how it was left an say upstairs so incase any neighbours or anyone looking after the house while the owners are away come in then you have time to hide.

Obviously if it's a package you don't have to sign for then you can stick up a note on the door early in the morning before the post man comes saying to leave it round the back or whatever excuse you wanna make up.

Way #3

Easy, just as previously except you don't have to be as cautious and often the alarms are disabled for that time being anyway so you don't have to worry as much if you bump key into it.

As also stated previously in this guide, if there are any up for bidding/for sale signs then take them down and just get them out of the way.

You can even go to this one the night before instead of day time because no one is hardly going to be watching over this unless it's in a neighbourhood watch area (in which case you chose the wrong area anyway, you dumbass).

Some basic tips to keep in mind

-- Be there before the postman! can't stress this enough, it's too fucking obvious if you're late.

-- When signing for packages, if you need to, then sign a fake signature (the sig can be any made up fake shit) with your hand that you don't write with, so it's harder to trace incase things go tits up later on down the line.

-- Take anything in any guide with a pinch of salt, things may be different circumstances for you and your situations; guides are to be used as basis's.

CC scan tutz:

<http://www.zshare.net/download/51706978a8180d65/>
<http://www.zshare.net/download/51707169cc576e5d/>

Also will say the main reason we use SOCK proxies:

Sock proxies can receive and send most types of internet traffic such as e-mails, java, flash etc; sock proxies are more private as well and much more secure.

Socks traffic is anonymized as it is sent out and the incoming traffic is filtered.

You can run most programs through SOCKS easier as well.

Bear in mind it's wise to disable java, and flash and have your cookies cleared before and during use of the proxies as they can reveal your identity.

Disable Javascript, until you need to use it (usually when submitting info).

You can find socks(5) proxies online, scanning them to see which ones are still high in anonymity and are working is done through certain scanners you find online.

I use accessdiver to check all my proxies from the lists I got.

If I ever get a log in for any proxy again (if I decide to start carding again) then I'll be sure to share some lists sometime.

In fact you can actually buy them off the anyproxy.net website, except they're cheaper in IRC.

An extra tip about drops: You can order it to any address you want really, call them up saying they got the address wrong and are sending it there instead (say you live on a street that sounds similar to theirs), ask if they can sign for it and keep it there until you can pick it up after work. This is the best method.

Also bear in mind about instore carding for the UK, because of chip and pin it's ALOT harder to skim ATMs, you have to use the old ones that are in some paki shops. They're hard to find but they do still have them in places. For an example of what atm type I'm on about search for the skimming video that The Real Hustle did.

END

Credits

Writers and compilers

Bakayar
Silas the Stricken
[Dfg](#) [Guide Compilation]
Pandora's Assassin
MrNatowski
Purple Sprite
slim-ov-derby
Acetrace
Drizzt
Σigma
theinvader

Images collected by

Bakayar
Silas the Stricken
Maj. A hole
[Dfg](#)

Publishers

[Dfg](#)
[Bad Ideas](#) community forum

Sources

The propagation
The assassin
Pi and Styxx
Mr. Swarts
Lazarith
Vortex
DR. Badmind

Special thanks

[Dfg](#); without whom this would not have been conceptualised, let alone made

Zok; for the use of his bbs; saving the totse archives, and trying to make them better

All those who moderate the totse archives

And last but in no way, on earth, least the bad ideas community, new and old members, those who have left and those who have lingered. The sources are just a small example of how far our collective knowledge has taken us.