أكاديمية التعلم
Academy Of Learning

الأمن السيبراني

مجلة وثائقية عن الأمن االسيبراني وتطوره في المملكة العربية السعودية

مثلث الأمن السيبراني

الهجمات السيبرانية وأهداف الهجمات

الاساليب المستخدمة في الهجمات

أمن المعلومات

التصيد و التشفير

نظم التشغيل وعلاقتها بالآمن السيبراني

مخاطر الكوكيز

مفهوم الآمن السيبراني

تطور الآمن السيبراني في المملكة العربية السعودية

الإصدار الاول / يناير 2024

أكاديمية التعلم
Academy Of Learning

أكاديمية التعلم
الخبر _فرع الكورنيش ,المملكة العربية السعودية
رجب1445 ه _ يناير 2024 م

الآعداد والتنفيذ:

C S GROUP

Mona Al Amri

Noora AL Dossary

Mowaddah Abdulaziz

Moudi ALShuwaeir

Shouq ALshammari

Musherah ALShanfari

Najla ALQahtani

Fay ALQahtani

Mashail ALShammari

أكاديمية التعلم
Academy Of Learning

إهداء

نهدي هذا المشروع إلى
إدارتنا ومعلماتنا الذين لم
نكن لنصل لولاجهودهم
معنا ودعمهم المستمر
وتعاونهم ولهم جزيل الشكر
والتقدير

المحتوى

نحن نعيش في زمن الابتكارات العلمية والتقنية غير المسبوقة وأفاق النمو غير المحدودة ,ويمكن لهذة التقنيات الجديدة مثل الذكاء الاصطناعي ,وإنترنت الأشياء في حال تم استخدامها على النحو الآمثل ,تجلب للعالم فوائد ضخمة ,وفي الوقت ذاته فقد ينتج عن هذه الابتكارات تحديات جديدة مثل تغير أنماط العمل والمهارات اللازمة للتأقلم مع مستقبل العمل وكذلك زيادة مخاطر الامن السيبراني وتدفق المعلومات مما يستوجب علينا معالجة هذه التحديات في أقرب وقت لتفادي تحولها إلى أزمات اقتصادية وإجتماعية. [1]

صاحب السمو الملكي الامير محمد بن سلمان ولي العهد ونائب رئيس مجلس الوزراء وزير الدفاع
قمة العشرين 2019 أوساكا ,اليابان

الأمن السيبراني

إن قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر فأصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعايشه في العالم مؤخرا، حيث يشهد العالم المتقدم بكافة أرجائه تطور كبير لا يمكننا بأي حال أن نغفله، لذا أصبحت تلك الدراسات التكنولوجية في مجال الحوسبة الرقمية مقصد الكثيرين من الدارسين المتميزين حول العالم، ولكن يوجد جانب آخر مظلم لذلك التطور الرقمي الذي نشهده، يمكن أن يجعل كبرى الدول والشركات والمؤسسات التجارية والاقتصادية مهددة بالاختراق، ولعل هذه من أسباب أهمية دراسة الأمن السيبراني، والذي يعمل على حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات, وماتقدم من خدمات ,وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول واستخدام أو استغلال غير مشروع ويشمل مفهوم الآمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

ويحتوي نهج الأمن السيبراني الناجح على طبقات متعددة من الحماية تنتشر عبر أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي يرغب المرء في الحفاظ عليها. (1)

ولادة الامن السيبراني

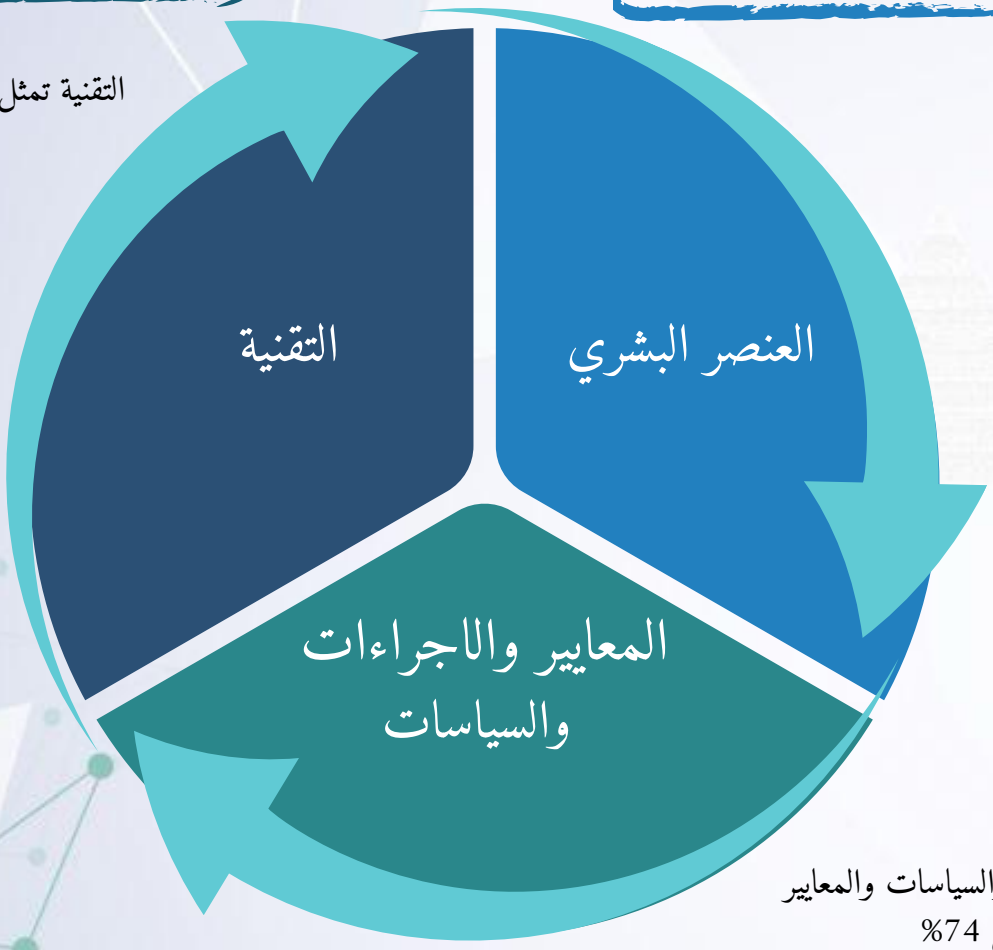
بـدأ في 1980 انتشـار البرمجيات التجاريـة لمكافحة الفيروسـات، وهي أدوات بسـيطة تُجري عمليات بحث منهجية لاكتشـاف تسلسـل رموز الفيروسـات، ولكـن مـع ازديـاد عدد الفيروسـات إلى المئات، سـرعان ما أصبحت هـذه البرمجيات غيـر فعالـة، وغيـر قـادرة على مجـاراة تغيّر الفيروسـات لصعوبـة تحديثهـا دون توفّر شـبكة اتصال عالمية واسـعة الانتشـار.

عناصر الأمن السيبراني الاساسية

تأهيل العدد الكافي من المتخصصين والمؤهلين في الأمن السيبراني (بالتعليم والتدريب توعية غير المتخصصين)

- استخدام التقنيات والحلول المناسبة
- التهيئة المناسبة
- المراجعة المستمرة للتقنيات

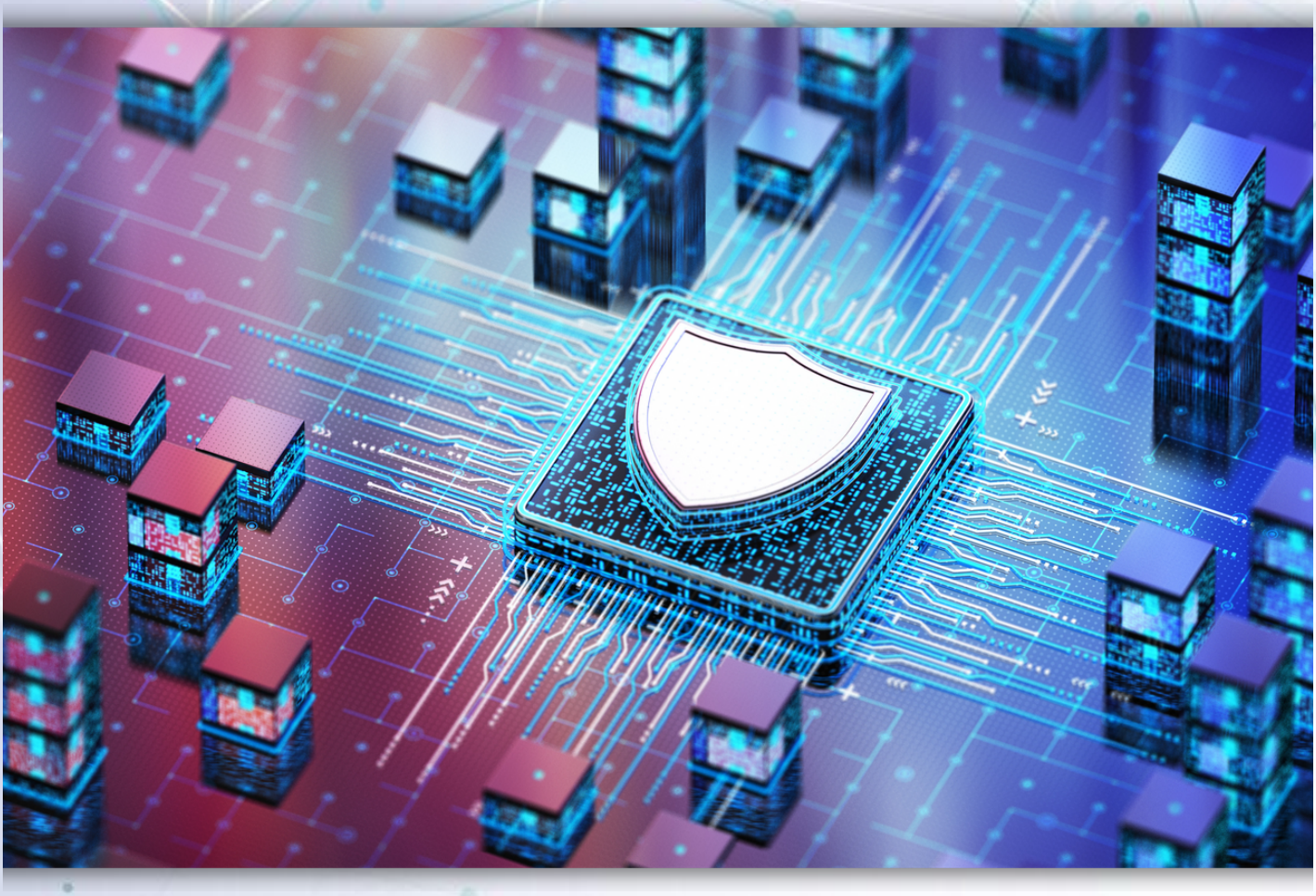
التقنية تمثل 26% من الحماية



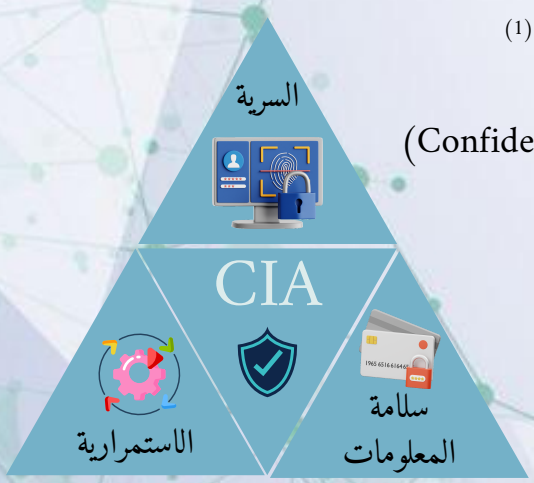
العنصر البشري والسياسات والمعايير تمثل 74% من الحماية

- حوكمة الأمن السيبراني
- بناء إستراتيجة الأمن السيبراني وتطبيقها
- تطوير سياسات وإجراءات الأمن السيبراني(1)

مثلث الأمن السيبراني



مثلث الحماية CIA هو أحد الأنظمة والنماذج التي تتبع الأمن السيبراني بشكل كبير في تأمين المعلومات والبيانات، وترى أنه أحد النماذج التي تعتمد بشكل كبير على بعض الأركان الهامة والتي يجب أن يتحلى بها أي نظام أمني، وبالطبع يسعى العديد من الناس للتعرف على ما هو هذا النموذج الأمني للاستفادة منه بشكل كبير(1)



1-السريةبمفهوها الشامل للمعلومات والانظمة والاصوال وغيره(Confidentiality)
2-سلامة المعلومات وضمان مصدرها(Integrity)
3-الاستمرارية وتوفر الانظمة والمعلومات عند الحاجة لها(Availability)

مستقبل الأمن السيبراني كبير بحكم أننا في كل يوم نعزز علاقتنا مع التقنية وكل تقنية جديدة هي المستقبل

د-موضى الجامع
أكاديمية سعودية وباحثة في الأمن السيبراني
مدير عام تطوير كفاءات الاتصالات وتقنية المعلومات في أكاديمية STC

من أشهر الاختراقات الإلكترونية "السيبرانية" القضية التي حازت على أوساط شبكات التواصل الاجتماعي والشوارع الأمريكية وهي قضية التأثير على الانتخابات الأمريكية عام 2016 .

الهجمات السيبرانية

الهجمات والجرائم الإلكترونية ليست جديدة ولها تاريخ طويل يعود لأواخر الثمانينيات، وتحديداً عام 1988، عندما أراد روبرت تابان موريس، ابن عالم التشفير الشهير روبرت موريس، أن يعرف عدد الأجهزة المتصلة بالإنترنت.

يمكن تعريف الهجمات السيبرانية بأنها العبث بأحد ركائز الامن السيبراني وهي:

1. إفشاء المعلومات أو وصول غير المصرح لهم سواء للمعلومات أو الانظمة أو الشبكات .
2. العبث بسلامة المعلومات أو مصدرها.
3. تعطيل الانظمة أو منع الوصول للمعلومات وقت الحاجة لها.(1)

أهداف الهجمات السيبرانية

الهجمات السيبرانية لها عدد من الأهداف العامة التخريبية والتدميرية للانظمة والبنية التحتية:

1. اهداف سياسية مثل:الحرب السيبرانية والتجسس السيبراني.
2. أهداف شخصية مثل:نشر المعلومات الخاصة للاخرين وانتحال شخصية.
3. أهداف تجارية ومالية لزعزعة الثقة والمصداقية للمنافسين.[1]

التصيد

أصبح التصيد الاحتيالي عبر السنوات أكثر تقدماً بشكل كبير. ويقدر أن حوالي 32% من كل عمليات الاختراق تتضمن تصيداً احتيالياً وحوالي 64% من المنظمات تبلغ عن تعرضها لمحاولات للتصيد الاحتيالي لمرة واحدة على الأقل في تاريخها.

يتمثل التحدي في التصيد الاحتيالي في إنه قد يكون من الصعب اكتشافه حيث تصبح الأساليب أكثر تعقيداً، خاصة مع استحداث الذكاء الاصطناعي. قد تكون فتح رسالة بريد إلكتروني للتصيد الاحتيالي مرة من دون أن تدرك الأمر حيث إن مجرمو الإنترنت يعتمدون على الهندسة الاجتماعية لإقناع الضحايا غير المرتابين بفتح المرفقات المشبوهة.

التصيد الاحتيالي هو طريقة خطرة وفعالة لعمليات الاختراق. ويعمل التصيد الاحتيالي عبر إرسال مجرمي الإنترنت الرسائل للأشخاص أو الشركات تتضمن رابطاً أو مرفقاً ضاراً. ويكون الهدف من ذلك أن ينقر المستهدفون على الرابط، وهو ما قد يقوم بتنزيل برنامج ضار أو يقودهم إلى موقع الويب غير شرعي لسرقة معلوماتهم الشخصية. ويمكن ارتكاب هجمات التصيد الاحتيالي، بعدة طرق استناداً إلى المهاجم والمعلومات التي يحاول الحصول عليها. [3]

من الاساليب المستخدمة في الهجمات السيبرانية

- رسائل التصيد الاالكتروني والهندسة الاجتماعية.
- استغلال الثغرات في المواقع الإلكترونية و التطبيقات.
- نشر البرمجيات الخبيثة عن طريق وسائط التخزين.
- هجمات البحث الشامل لاستغلال كلمات المرور الضعيفة.
- حجب الخدمة.(1)

البرمجيات الخبيثة

يقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض, و الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها,و يمكن يتصنف أنواع البرمجيات الخبيثة على النحو التالي:

الفيروسات Viruses فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف برامج معينة ، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة

الديدان Wormsديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها

برامج التجسس Spywares هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس المستخدم يجهل هذا الغزو.

أحصنة طروادة Trojan Horses وهو من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة. تقوم بخداع المستخدمين من أجل تحميلها وتطبيقها على أنظمتهم يتم تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار.

هجوم XSS لايستهدف المخترق موقعك بدرجة أولى، وإنما يستعمله كجسر للعبور إلى الضحايا الذين يتصفحونه، حيث يستغل ثغرة في موقعك يتسلل من خلالها إلى زوار موقعك للهجوم عليهم.

هجوم CSRF يتم الاختراق عن طريق رابط أو كود برمجي في صفحة من الموقع بحيث يقوم المستخدم بطلبها، عن طريق صورة مثلا ,مثال: بينما يقوم المستخدم بتسجيل دخوله إلى صفحته في البنك، يقوم المخترق بإرسال رسالة عبرموقع آخر، فبالتالي يتم تنفيذ الطلب في صفحة البنك.

من أخطر الفيروسات البوت نت Botnet هو مجموعة من أجهزة متصلة ببعضها عبر شبكة إنترنت، قد تكون هذه الأجهزة حواسب أو هواتف ذكية أوخوادم أو أجهزة أخرى تعرف بإنترنت الأشياء، وجميع هذه الأجهزة المتصلة تكون مصابة ويتم التحكم بها عبر نوع من البرامج الخبيثة، وفي حالات عديدة قد لايدرك المستخدم أن حاسبه يتعرض لهجوم.

فيروسات الفدية حيث متوسط الفدية التي يطلبها قراصنة هذا النوع من الفيروسات قد تصل إلى قرابة 300 دولار أمريكي.

الهندسة الاجتماعية هي فن التلاعب بالبشر وخداعهم بهدف الحصول على البيانات لكشف معلوماتهم أو حساباتهم السرية دون علمهم وذلك باستهداف نقاط الضعف البشرية

(3)

بعض الحوادث السيبرانية على مستوى العالم

توقفت 60محطة فرعية في أحد المرافق الكهربائية عن العمل
لمدة90 دقيقة لاحد الدول ,مماأدى
إلى انقطاع التيار الكهربائي عن 230,000نسمة (2015)

سرقة معلومات من أحد الشركات الائتمانية
لاكثر من140 مليون شخص (2017)

تمت سرقة 81 مليون دولار خلال التلاعب
بأحد أنظمة أنظمة المعاملات (2016)

ستكسنت:تم تدمير أجهزة طرد مركزي نووية
بواسطة هجوم إلكتروني (2010)

سرقة معلومات أكثر من500مليون عميل لاحد
الفنادق العالمية (2014-2018)

سرقة بيانات من شبكات أحد القوات المسلحة باستخدام
ذاكرة بيانات فلاش تحوى برمجية خبيثة (2008)

(1)

التشفير

يحكم معظم الناس لصق الأظرف قبل إرسال خطاباتهم، وإذا سئلوا عن سبب ذلك فستأتي بعض الإجابات الفورية من قبيل: «لا أعرف حقيقةً» و«لأن الجميع يفعلون ذلك» قد تشمل الإجابات الأخرى الأكثر تعقُّلا إجابات من قبيل «منع الآخرين من قراءة الخطاب»

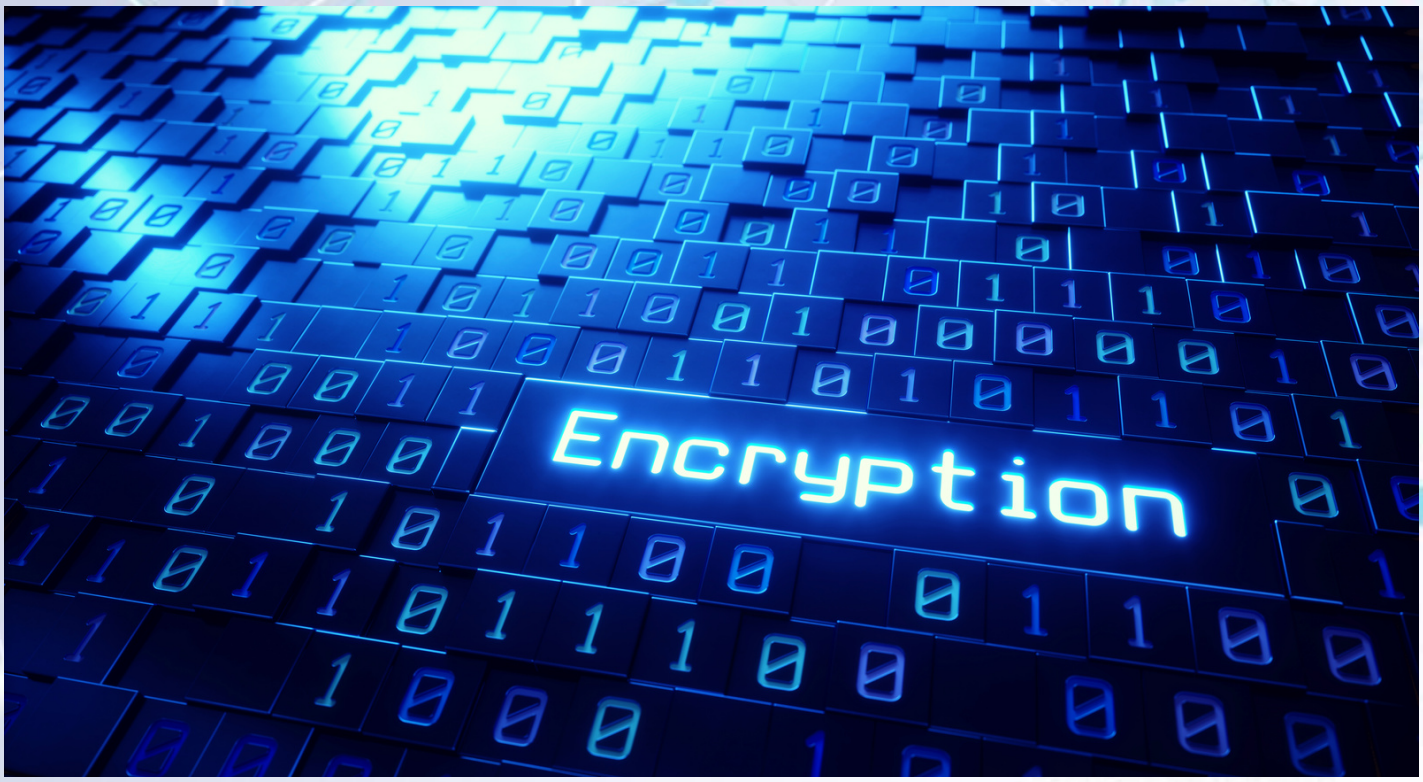
يعتبر استخدام البريد الإلكتروني بالنسبة إلى الكثيرين حاليّا بديلا لإرسال الخطابات بدلا من البريد العادي. والبريد الإلكتروني وسيله سريعه للتواصل لكن بطبيعة الحال لا توجد أظرف لحماية الرسائل، بل يُقال عادةً إن إرسال الرسائل عبر البريد الإلكتروني يشبه إرسال الخطابات عبر البريد العادي دون أظرف. من يردإرسال رسالة سرية أو مجرد رسائل شخصية عبر البريد الإلكتروني، فسيحتاج إلى وسيلة أخرى لحمايتها. تتمثل إحدى هذه الوسائل في استخدام التشفير وتشفير الرسائل.

إذا وقعت رسالة مشفّرة في أيدي أشخاص غير المتلقين المعنين، يجب أن تبدو هذه الرسالة غير مفهومة, لم ينتشر استخدام التشفير لحماية رسائل البريد الإلكتروني على نطاق واسع بعد.

إلا أن ذلك يحدث حاليا وعلى الارجح سيزداد انتشاره في الواقع.

تقدمت مجموعة من أعضاء البرلمان الأوروبي بتوصية في مايو ٢٠٠١ بضرورة تشفيرجميع مستخدمي أجهزة الكمبيوتر في أوروبا لرسائلهم الإلكترونية بغرض «تفادي تجسس شبكة التنصت البريطانية-الأمريكية» (2)

التشفير



التشفير علم راسخ كان له أثر تاريخي كبير لأكثر من ألفَي عام,جرت العادة أن الحكومات والمؤسسات العسكرية كانت بمنزلة المستخدمين الرئيسيين، وتأثير علم التشفير على التاريخ موثّق توثيقا جيدا.

يختلف المؤرخون على المصدر الرئيسي للتشفير وظهوره، فمنهم من يرجعه للحضارة الرومانية وآخر للفينيقية و آخر إلى الحضارة المصرية القديمة، ولكن ما لا يختلف عليه أن جميع هذه الحضارات كان لها طرق خاصة تستخدمها للتواصل بشكل آمن بواسطة تشفير الرسائل.

وتتمثل فكرة أي نظام تشفير في إخفاء المعلومات السرية بطريقة يصبح من خلالها معناها غير مفهوم بالنسبة إلى أي شخص غير مصرح له بالاطلاع عليها, يتمثل الاستخدامان الأكثر شيوعا للتشفير في تخزين البيانات بأمان في ملف كمبيوتر أو نقْله عبر قناة غيرأمنة مثل الانترنت في كلتا الحالتين، حقيقةكون المستند مشفرا لاتمنع الاشخاص غير المصرح لهم بالوصول اليه ,ولكنها تضمن عدم تمكنهم من فهم مايرونه.(2)

حماية أجهزتك من الاختراق

كثرت عمليات القرصنة في الآونة الأخيرة لسرقة بيانات المستخدمين وبيعها لجهات ثالثة من أجل الحصول على المال. وهذا ما يؤكد أهمية تأمين البيانات من هجمات القراصنة وحماية الخصوصية على تثبيت التحديثات الجديدة بأسرع ما يمكن.

من الضروري المحافظة على أن تكون التطبيقات والأجهزة الذكية التي تستخدمها محدثة دائما بأحدث الإصدارات والبرامج الثابتة. فغالبًا تشمل التحديثات معالجة للعديد من الثغرات الأمنية التي قد يستغلها القراصنة لتنفيذ عمليات اختراق بياناتك.

قم بتأمين أجهزتك بطرق قوية ، من المدهش أن ثلث مستخدمي الهواتف الذكية على الأقل لا يهتمون باستخدام رمز مرور قوي بل يستخدمون أبسط رموز المرور المكونة من أربعة أرقام لتأمين أجهزتهم ودخول المواقع. هناك العديد من الطرق لتأمين وإلغاء قفل الهواتف وأجهزة الكمبيوتر والأجهزة اللوحية – وهي الطرق البيومترية مثل التعرف على الوجه وبصمات الأصابع والعين وكذلك طريقة إستخدام الأنماط وغيرها لذلك يجب عليك إعداد رمز مرور قوي لتأمين أجهزتك والاستفادة من ميزات الأمان العالية.

تأكد من تفعيل جدار الحماية Firewall بأجهزتك ، يعتبر جدار الحماية Firewall جزء هام جداً من حماية جهازك، حتى إذا تمكن القراصنة من اختراق جهازك ومعرفة موقعك وعنوان IP التابع لجهازك، فإن جدار الحماية يمنعهم من الوصول إلى نظام التشغيل والشبكة. الجدير بالذكر أن أنظمة ويندوز Windows وماك Mac الحديثة تحتوي على جدران حماية مدمجة لتعريف منافذ الإنترنت الصادرة والواردة.

لا تثق بشبكات الواي فاي Wi-Fiالعامة ، يستخدم القراصنة والمتسللون شبكات الواي فاي العامة للتجسس على المستخدمين الذين ينضمون إلى الشبكة أو في بعض الأحيان يقومون بإنشاء شبكات honeypot وهي عبارة عن شبكات وهمية مصممة لسرقة معلوماتك.

حماية أجهزتك من الاختراق

قم بمسح بياناتك من على الأجهزة القديمة التي ستتخلص منها ، من المعروف أن مسح البيانات والملفات من الأجهزة بطرق التقليدية لا يضمن التخلص النهائي منها، وذلك لوجود الكثير من الطرق والبرمجيات التي تساعد على استرجاعها حتى بعد مرور الكثير من الوقت بعد حذفها

احرص على استخدام كلمات مرور قوية لحساباتك على الإنترنت

كلمة المرور الخاصة بك هي خط الدفاع الأول، لذلك تأكد من إعداد كلمة مرور آمنة وفريدة لكل حساب، إذا كنت تشعر بصعوبة في التعامل مع كلمات المرور الكثيرة أو ترغب في تطوير كلمات مرور أصعب يمكنك استخدام برنامج مدير كلمات المرور password manager، وهو برنامج يمكنه تخزين كلمات المرور وإدارتها لكل تطبيق أو خدمة أو موقع تستخدمه، حيث أنه يعتبر مثل خزانة مقفلة على جميع بيانات المرور الخاصة بك.

استخدام خاصية المصادقة الثنائية Two-Factor Authentication ،المصادقة الثنائية 2FAتعتبر طريقة مميزة لاستخدام خطوة تحقق إضافية إلى عملية تسجيل الدخول الخاصة بحساباتك الأكثر أهمية. فبدلاً من تقديم اسم المستخدم وكلمة المرور فقط لتسجيل الدخول إلى أحد الحسابات يتم إرسال كود جديد مختلف إلي هاتفك لتستخدمه في كل مرة تقوم فيها بالدخول إلي حسابك.

احرص على استخدام خيار شبكة الضيوف،يرغب الأصدقاء والعائلة دائمًا في استخدام شبكة الواي فاي Wi-Fi الخاصة بك عند زيارتك، فبدلاً من استخدام الشبكة الخاصة بك التي ترتبط بها جميع أجهزتك، يمكنك تخصيص شبكة خاصة لهم في جهاز التوجيه، والتي تعرف باسم شبكة الضيوف. تتيح لك هذه الميزة مشاركة اتصالك بالإنترنت مع ضيوفك في حين إبقائهم خارج شبكتك الأساسية، مما يمنعهم من رؤية الملفات والخدمات المشتركة، لذلك قم بإعداد شبكة الضيوف الخاصة بك باستخدام اسم شبكة مختلف وكلمة مرور مختلفة وقوية.

(ملفات تعريف الارتباط الكوكيز) Cookie

ملف نصّي يقوم الخادم بتخزينه على القرص الصلب لجهاز المستخدم عن طريق المتصفّح عند زيارة المستخدم لصفحة الويب. يتمّ تبادل ملفات الكوكيز
بين الخادم وصفحة الويب عن طريق بروتوكول نقل النص التشعبي.
محتويات الكوكيز: هناك محتويات أساسيّة يجب أن تكون متواجدة في أيّ ملف كوكيز مخزّن على جهاز المستخدم. هذه المحتويات تشمل:(اسم الملف. مُحتوى الملف- عنوان صفحة الويب التي قامت بتخزين الملف- تاريخ انتهاء مفعول الملف- نوع اتصال الإنترنت

عند إدخال بيانات دخول ما مثل تويتر أو فيسبوك, يعرض المتصفح اشعار " تذكرني على هذا الكمبيوتر " في حال قمت بالضغط عليه, سيقوم موقع الويب بإنشاء ملف تعريف ارتباط cookies لهذا الموقع وفي كل مرة تقوم فيها بزيارة الموقع قد تحتاج فقط إلى إدخال كلمة المرور الخاصة بك أو قد لا تحتاج إلى تسجيل الدخول على الإطلاق.
تُستخدم ملفات تعريف الارتباط أيضًا لتخزين تفضيلات المستخدم لموقع معين على سبيل المثال ، قد يخزن محرك البحث إعدادات البحث في ملف تعريف ارتباط.
لماذا نشعر بالقلق الشديد من ملفات تعريف الارتباط؟
السبب في ذلك هو أن العديد من مزودي الإعلانات مثل (Google وشركاتها) يعملون مع الصفحات أو المواقع التي يقومون بإدراج الإعلانات فيها لتضمين موردًا صغيرًا مضمنًا في كل منها يُطلق عليه "beacon" بحيث يحافظون على ربط ملفات تعريف الارتباط دائمًا بالنطاق نفسه وبهذه الطريقة يقومون بتتبع المسار الخاص بك في كل صفحة تقوم بزيارتها.


خطف الكوكيز
التلاعب بمحتويات الكوكيز
سرقة الكوكيز
مشاركة الكوكيز بين المواقع
التعقب والتجسس
مخاطر ملفات تعريف الارتباط Cookie

أمن المعلومات والأمن السيبراني

يعمل الامن السيبراني وامن المعلومات على حماية البيانات من الاختراقات والهجمات وأي خطر محتمل الحدوث. وعلى الرغم من أن هنالك تشابهًا كبيرًا بينهما من حيث المفهوم إلا أنهما مختلفان بعض الشيء ففي الوقت الذي يعمل أحدهما لحماية البيانات في مكانٍ واحد، يقوم الآخر بحماية البيانات بشكلٍ عام.

الأمن السيبراني يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية وخاصة الإنترنت، حيث يعمل مختصو الامن السيبراني على حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكلٍ عام، كما يحاول مختصو الأمن السيبراني ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات بالوصول إليها

أمن المعلومات يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه وليس حماية الحاسب كله.

السيرفر والامن السيبراني

كلنا نعلم مدى أهمية نظم التشغيل للحواسيب وأيضا نعلم أن أكبر شركة منتجة لنظم التشغيل هي من إنتاج عملاق البرمجيات الأمريكية مايكروسوفت التي تسيطر على ما يقرب من 70 % من السوق العالمي لنظم التشغيل في العالم وأنظمة تشغيل مايكروسوفت في الصدارة حتى منذ صدور أول نظام تشغيل الذي كان يحمل اسم ويندوز 1.0 في عام 1981 وبدأت مايكروسوفت بالتدرج في إنتاج إصدارات ويندوز ومع تطور الإنترنت وانتشاره بات من الضروري إنتاج أنظمة تشغيل تدعم الخوادم Servers فما هي تلك النظم التي تدعم الخوادم ؟

السيرفر والامن السيبراني

الويندوز سيرفر هو أحد منتجات شركة مايكروسوفت مثله مثل أي نسخة ويندوز ولكنها مزودة بإمكانيات مخصصة وبرمجيات خاصة لإدارة وإنشاء الشبكات نظام Windows Server هو منصة قوية تلبي احتياجات إدارة الشبكات والخوادم بشكل شامل من خلال تاريخه المتطور والإصدارات المتعددة، أصبح Windows Server عنصراً أساسياً في بنية البيئات التجارية والمؤسسات, يقدم Windows Server العديد من الخصائص المتقدمة مثل إدارة الهويات، والأمان، والتخزين، والتحكم في الشبكات، مما يجعله الخيار المفضل للشركات التي تبحث عن حلاً موثوقًا وقويًا لتشغيل خوادمها.

بإصداراته المختلفة، يمكن للمستخدمين اختيار الإصدار الذي يلبي احتياجاتهم، سواء كان ذلك في مجال الحوسبة الظاهرية، أمن البيانات، إدارة الهويات، أو توفير الخدمات عبر الشبكة, من خلال ميزاته المتعددة وأدوات إدارته القوية، يسهم Windows Server في تبسيط إدارة البيئات وتحسين أداء الخوادم

باختصار، نظام Windows Server يمثل أحد أهم الأدوات التقنية في عالم الأعمال والمؤسسات. إنه يوفر القدرة على تشغيل وإدارة بيئات الخوادم بشكل فعّال ويوفر أمانًا واستقرارًا للبيانات والخدمات, يُعتبر Windows Server حلاً شاملاً يلبي احتياجات الشركات الكبيرة والصغيرة على حد سواء، مما يجعله أحد الركائز الأساسية لنجاح الأعمال وتطورها في عالم التكنولوجيا الحديث .

الاسرة والأمن السيبراني

68% من الاباء يراقبون استخدام التقنية لاطفالهم بعمر 6 إلى 9 سنوات, 41% من الاباء يراقبون استخدام التقنية لاطفالهم بعمر أكبر من 10 سنوات ,60 %من الاباء قلقين من أن يقوم شخص بسرقة هوية أبنائهم باستخدام المعلومات المنشورة على الانترنت, في دراسة أجريت عام 2012 في الولايات المتحدة الامريكية وجدت أن الاطفال بعمر أقل من 19 سنة يمثلون 6 من جرائم سرقة الهوية ,في دراسة أخرى اعترف 30 % من المراهقين أنهم قد تعرفوا على أشخاص في الانترنت يستخدمون صور وهويات مزيفة.

توعية الأسرة بالمخاطر السيبرانية

- ليس كل مايرونه في الانترنت صحيح
- ليس كل الاشخاص في الانترنت يستخدمون شخصياتهم الحقيقة
- ابدأ بوضع مجموعة من القواعد والقوانين التى يجب على جميع العائلة والابناء اتباعها في الفضاء السيبراني
- التأكد من أن جميع الاجهزة المنزلية المرتبطة بالانترنت محمية بطريقة مناسبة
- استخدم إعدادات الخصوصية والأمن المناسبة لاعمار أبنائك عند دخولهم المواقع الإلكترونية أو شبكات الألعاب الإلكترونية أو التطبيقات الذكية. (1)

إضاءة

تعتبر بيانات الموظفين
هدفا رئيسيا للمهاجمين
فلا تغفل عن حماية
بياناتك وأجهزتك داخل
وخارج العمل !

الأمن السيبراني في المملكة العربية السعودية

بات الأمن السيبراني في السعودية من أهم المجالات خلال الفترة الأخيرة، في ظل امتلاك المملكة أكبر سوق لتكنولوجيا المعلومات والاتصالات في الشرق الأوسط، وحرصها على تطويره بصورة مستمرة، وبعد تعرض المملكة للملايين من الهجمات الإلكترونية.

زاد الاهتمام بمجال الأمن السيبراني في السعودية، الذي يضمن توفير الحماية ضد تلك الهجمات شهدت المملكة العربية السعودية مؤخراً تطورات عدة بشأن تنظيم الأمن السيبراني، إذ جرى إصدار مرسومًا ملكيًا رقم 6801 لعام 11/2/1439 (31 أكتوبر 2017)، للموافقة على لائحة الهيئة الوطنية للأمن السيبراني، المُحددة لأدوار ومسؤوليات الهيئة، والتي تعزز قانون استخدام تكنولوجيا المعلومات والاتصالات في الوكالات الحكومية.

والجدير بالذكر أن الشركات في المملكة العربية السعودية، عانت وقت بداية جائحة كورونا ولجوئها إلى العمل عن بُعد، من الملايين من الهجمات الإلكترونية والتي بلغ عددها 22.5 مليون هجوم إلكتروني، كلف الدولة خسائر قُدرت بـ 6.5 مليون دولار.

ولموقع المملكة العربية السعودية الاستراتيجي في المنطقة، تعرضت البنية التحتية لتكنولوجيا المعلومات والاتصالات في كل من القطاعين العام والخاص لتهديدات مستمرة بسبب الحوادث الإلكترونية، تلك الحوادث التي أثرت بالسلب على الاقتصاد من حيث المستوى المالي والتشغيلي والتكتيكي مستقبل الأمن السيبراني في السعودية

بات الأمن السيبراني أمرًا حيويًا للغاية لنجاح رؤية 2030 بالمملكة العربية السعودية، لدرجة أنه ينعكس من خلال استراتيجية وطنية متطورة للأمن السيبراني، ولذلك أصبحت البيانات والذكاء الاصطناعي والابتكارات التكنولوجية جزءًا أساسيًا من هذه الرؤية، وتعد السعودية الدولة الثانية في مؤشر الأمن السيبراني العالمي.[3]

جهود المملكة العربية السعودية في الأمن السيبراني

- تُعد المملكة العربية السعودية من أهم الدول المُطبقة لسياسات الأمن السيبراني، ولذلك حصلت السعودية على المركز الثاني في مؤشر الأمن السيبراني العالمي في الكتاب السنوي العالمي للتنافسية (WCY) لعام 2023 من قِبل المعهد الدولي للتنمية الإدارية (IMD) الواقع في سويسرا,
- كما أصدر سوق الأمن السيبراني في المملكة العربية السعودية، تقريراً في عام 2022، أفاد بوصول القيمة السوقية لقطاع الأمن السيبراني المحلي في عام 2020 إلى 3.6 مليار دولار.
- اهتمت الدولة السعودية بتطوير مهارات الطلبة الملتحقين بالجامعات المتخصصة في مجال الأمن السيبراني، ولذلك جرى توقيع اتفاقية بين وزارة التعليم العالي والهيئة الوطنية للأمن السيبراني، وذلك في عام 2021
- وتنص الاتفاقية الموقعة على توفير العديد من البرامج التدريبية لتعزيز مهارات طلبة تخصصات الأمن السيبراني في السعودية، إلى جانب منحهم ما يقرب من 231 منحة دراسية في هذا التخصص
- ولم تقتصر البرامج التدريبية على طلبة تخصصات الأمن السيبراني فقط؛ بل شملت أيضًا المؤسسات والأشخاص في الأمن السيبراني، إضافة إلى المواطنين السعوديين.(3)

إنجازات المملكة العربية السعودية في الأمن السيبراني

- إنشاء كلية متخصصة بالأمن السيبراني والبرمجة والذكاء الاصطناعي تسعى إلى بناء وتأهيل قدرات وطنية شابة محترفة للمساهمة في تحقيق اهداف المملكة في رؤية ٢٠٣٠.

- وزارة التعليم والهيئة الوطنية للأمن السيبراني قامت بتخصيص 1000 مقعد للمستفيدين و المستفيدات من برنامج خادم الحرمين الشريفين للإبتعاث الخارجي في مجال الأمن السيبراني.

- العديد من الجامعات السعودية تضمن مجالي الذكاء الاصطناعي والأمن السيبراني في خططها.

- وضع الاستراتيجية الوطنية للأمن السيبراني الجديدة من قبل الهيئة الوطنية للأمن السيبراني.(3)

إنجازات المملكة العربية السعودية في الأمن السيبراني

تم تشكيل الهيئة الوطنية للأمن السيبراني في October 31 , 2017 لرفع مستوى الحماية للشبكات C والاجهزة والأنظمة المعلوماتية وما تحويه من بيانات.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تم إنشاء الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز .

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

تم إنشاء مركز الأمن الإلكتروني لمواجهة التهديدات الالكترونية الموجهة على المملكة العربية السعودية.(3)

NCSC
مركز الأمن الإلكتروني
المملكة العربية السعودية

لمحة تاريخية عن الهجمات السيبرانية التى استهدفت المملكة

2016

هجمة الانظمة الصناعية Triton
(2016-2017)
تهدف إلى التحكم والتلاعب بأنظمة السلامة الصناعية

2017

هجمة شمعون 2(2016-2017)
العمليات التدميرية تم تنفيذها بشكل متزامن ومتناسق بحيث واجهت المملكة ثلاث موجات رئيسية (1)

2018

هجمات تدميرية (2018)
استهداف ست هجمات حيوية خلال أقل من شهرين ببرامج الفدية والمسح والتدمير أثرت على خدماتها

ختام

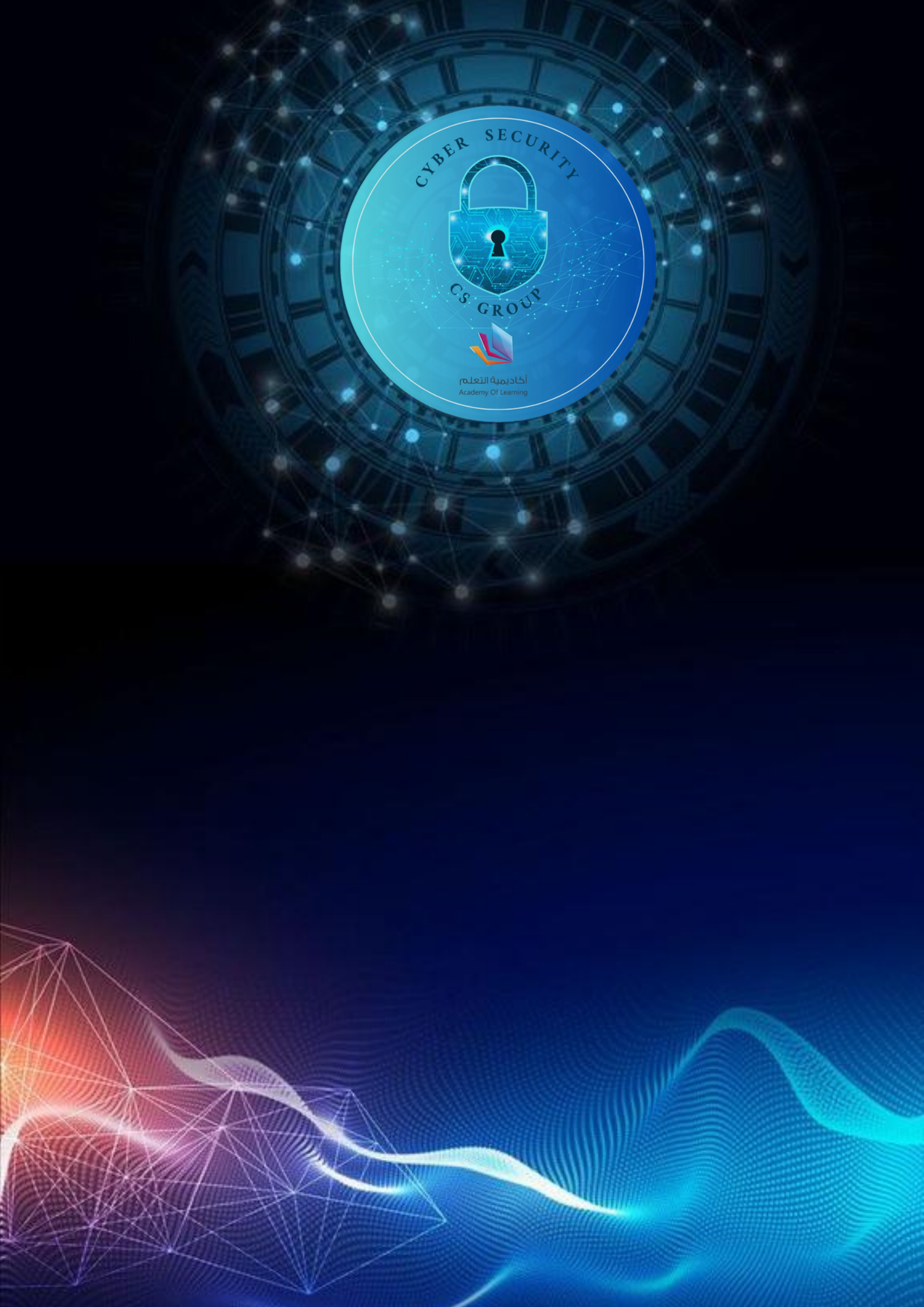
في ختام حديثا عن الامن السيبراني يجب القول ان الأمن السيبراني ذات أهمية بالغة في عالم تكنولوجيا المعلومات الحالي، فقد تطورت أساليب الهجمات السيبرانية بشكل كبير، مما يشكل تهديدًا جديًا على الأفراد والشركات والمؤسسات.

ومن خلال تحقيق الأمن السيبراني، يتم حماية البيانات والشبكات والأنظمة من الاختراق والاستغلال غير القانوني، وتعتبر اتخاذ سياسات أمنية قوية وتوظيف التكنولوجيا المتقدمة مثل تحليل الضوابط وانترنت الأشياء والتعرف على السياق واسعة النطاق، ضرورةً ملحّة لمكافحة التهديدات السيبرانية.

كما تُعزز الوعي والتدريب في مجال الأمان السيبراني قدرة الأفراد والمؤسسات على التعامل مع التحديات الأمنية الرقمية بفعالية.

المراجع

(1) الهيئة الوطنية لأمن السيبراني- برنامج التوعية بالآمن السيبراني
Piper, Fred, and Sean Murphy. (2) Cryptography: A very short introduction. Vol. 68. Oxford Paperbacks, 2002.
(3) مقدمة في الامن السيبراني أيمن الحربي.
(4) الضوابط الاساسية للآمن السيبراني _الهيئة الوطنية للأمن السيبراني.


CYBER SECURITY
CS GROUP
أكاديمية التعلم
Academy Of Learning