

Online Security

NZers flock online for shopping despite cybercrime fears - Symantec

New Zealanders plan to do nearly 40 percent of their Christmas shopping online this year despite fears of having their credit card or personal details stolen, according to new research from Norton by Symantec.

The Norton Online Shopping Survey reveals that 20 percent of Kiwis find online shopping stressful because of security worries yet 37 percent still do not check a **website's security** before shopping online and only 17 percent of those who bother to check are fully confident they know what to look for.

"New Zealand's love affair with online shopping has seen one in three Kiwis spend more than two hours per week shopping online," said Mark Gorrie, Director, Norton Business Unit, Pacific region, Symantec.

"However with the number of people affected by online crime continuing to rise[1], scammers are constantly refining their skills and targeting New Zealanders with malicious links and scams containing 'too good to be true' deals to steal their credit cards details and personal information.

"While the Norton Online Shopping Survey shows that New Zealanders are concerned about security when they shop online, some Kiwis are still choosing to not act on these concerns and putting themselves at risk of identity theft and credit card fraud," Gorrie added.

Online Shopping Security Concerns

Over two thirds of New Zealanders (68 percent) worry most about having their credit card details stolen, whilst half of respondents (51 percent) admitted they were fearful of purchasing goods from an untrustworthy or illegitimate site.

In addition, New Zealanders were concerned about falling victim to a data breach from an online retailer and having a username and password leaked from an online retailer - both at 35 percent. Surprisingly, 12 percent of those surveyed were not concerned by any of these risks at all.

Many of these security concerns are warranted with approximately 17 percent of New Zealanders experiencing credit card fraud as a result of online shopping. Indeed the

proportion might even be as high as 25 percent since eight percent said they have experienced credit card fraud but are not sure whether the fraudsters obtained their card details whilst they were shopping online or not.

Smartphone security also presents security challenges for New Zealanders shopping online. The majority of New Zealanders (80 percent) have used their smartphones to browse online shops and 62 percent have made online purchases using their smartphones. Interestingly one in three Kiwis (32 percent) have entered their credit card details on a mobile app yet more than half of all Kiwis (51 percent) are using unprotected smartphones. Only one third of New Zealanders who shop online use two factor authentication and nearly half (47 percent) do not even know what two factor authentication means.

Norton Online Shopping Safety Tips

- If it is too good to be true, it probably is. Be aware of the cheap price tag as free or discounted goods could end up being really costly. So if you have found the latest hot designer shoes, but for a tenth of the price, regardless of how nice they may be for your office Christmas party, they are probably not real. Cybercriminals are experts at creating websites and making them look identical to your favourite brand sites. Only shop at reputable online sites and avoid getting your credit card scammed.

- Beware of fake website links. Do not click on links in an email that appear to come from your favourite online store. Instead type the store's address into your browser to avoid going to a malicious website.

Be smart with your passwords. Protect your accounts with strong, unique passwords that use a combination of at least 10 upper and lowercase letters, symbols and numbers to help keep the bad guys at bay. Make it difficult for attackers to access your information by changing your passwords every three months and not reusing passwords for multiple accounts. That way, if a cybercriminal gets your password, they can't compromise all of your accounts. And if it is too overwhelming to keep up this practice, use a password manager to help.

Beware of phishing scams. Think twice before opening unsolicited messages or attachments, particularly from people you don't know, or clicking on random links. The message may be from a cybercriminal who has compromised your friend or family member's email or social media accounts.

Organise your online shopping. Set up an email account specifically to deal with online shopping. Provide as little information as possible to get the account set-up and don't use it for anything else such as online banking, business correspondence or family matters.

Protect your bank details. Always look out for the 'padlock' icon or the Norton Secured Seal when making a payment online. These symbols indicate that the website you are visiting uses encryption to protect you, so cybercriminals cannot capture your personal

information. Never let a website 'remember' your credit card details, always retype them if you want to shop there again.

Online payments. Even though it is the season of goodwill, avoid using public or shared computers, or even a wireless network to make a payment online. Hackers can easily capture your account information, log-in details and steal your money. Use a separate credit card with a small credit limit for online purchases.

Is your internet security software up-to-date? Update your security software regularly, especially during the festive season. Cybercriminals are more sophisticated than ever before and they will jump on any social trend to spread malware and steal your personal details.

Check your statements. Always check your credit card statements to look out for unexpected transactions.