Canada Free Press
...Because without America there is no Free World

Online attitudes should mirror real life behaviour

Online By By James Galpin, McAfee Canada
Wednesday, March 9, 2011

Most Canadians make a concerted effort to protect themselves so they avoid threats such as thefts, car accidents and physical attacks. They take fewer precautions, however, when it comes to steering clear of the many dangers that exist online.

Perhaps they believe there isn't much cause for alarm. This notion can be quickly dispelled with a look at some of the latest data. A recent survey from NetLingo.com indicates that 44 per cent of teens with online profiles on social networking sites report having been contacted online by a stranger. Adults clearly have their own threats to worry about as well; according to Javelin Strategy & Research's 2010 Identity Fraud Survey Report, the number of identity fraud victims last year totaled more than 11 million in the United States alone.

One of the reasons such troubling trends exist today is user behaviour. Every day, people are taking risks online that they would never take in real life. To prevent these lapses in judgment, users require more education around security. They must become, and remain, far more vigilant, and better at identifying the types of behaviour that are putting them at risk. Here are some examples of behaviours Canadians should learn to follow in order to stay safe online:

Don't let your children open the door to strangers: According to a Harris Interactive and McAfee study, 52 per cent of teens have given out personal information online to someone they don't know in real life.

Just as we would not ask a young child to open the door to a stranger, we shouldn't give them free, unsupervised access to an online world of strangers, some of whom with ulterior motives. To stay safe, parents should be discussing proper online behaviours with their children and spending time with them at the computer. They should also be installing software that helps manage how much time children spend online, blocks inappropriate websites such as school cheating sites, adult content, and hate/discrimination sites, and prevents children them from sharing personal information on social networks or other sites.

Be a defensive driver: Navigating the Internet can be similar to driving on a snow-covered highway. It can be treacherous, you can't always tell when the conditions are safe, and you need to put the proper equipment in place before starting your journey. Online, cybercriminals are stealthy: they'll hide malware in ads, online video and e-mails and this means users must be vigilant. Driving with poor brakes and bald tires greatly increases your chance of an accident; just as navigating the Internet without comprehensive security software greatly increases your chances of becoming a victim of cybercrime. Such software must include cloud technology to protect against emerging threats, anti-virus, anti-spyware, an inbound and an outbound firewall, anti-phishing protection and a website safety adviser to identify risky websites. The numbers are staggering: McAfee Labs says the first six months of 2010 were the most active ever for total malware production, with 10 million new pieces found and catalogued.

One disturbing trend that is on the rise is malicious advertising or “malvertising,” where an ad is used to distribute malware or exploit a user’s browser, resulting in an infection. The malware can also be delivered via e-mail spam or during a user download.

Another way cybercriminals fool consumers is through “scareware,” in which pop-ups can be used to message users that their PC has been infected by a virus and it must be cleaned immediately by using their scanning tool – which they must pay for. In reality, the user did not have malware at all; this tactic is only meant to get access to their credit card and charge it for useless software.

It’s important not only to protect yourself before you go online, but also to install security software from a company you trust.

Protect your home: Though there is a widely held world belief that Canadians are a law-abiding, unassuming people, we do not implicitly trust those we haven’t met. Most Canadians don’t leave their doors unlocked to strangers.

Rather, we keep our valuables safely behind locked doors to protect them from thieves. This principle needs to be applied to our computer data. Cybercriminals can access the personal information on our computers through unprotected connections such as wireless networks. Protecting these networks is essential to keeping ourselves safe, and can be done by simply installing network security software.

Free isn’t always better: We all love free stuff, but is free always better? While we may trust the free samples handed out in branded packaging in a grocery store, we are far less likely to trust a free sample without proper packaging, handed to us on the street. But while we recognize the inherent dangers of accepting free products whose source we can’t confirm, we continue to download digital content and software from unknown sources. The fact is that the more popular a topic, movie or artist, the more likely cybercriminals are using the popular search terms about these topics or people to guide you to infected content. Using website safety adviser software, your browser can notify you before you enter a website whose contents are questionable. Site rating icons are added to your search results as well as a browser button and optional search box. Together, these alert you to potentially risky sites and help you find safer alternatives.

And always purchase comprehensive security suite from a reputable company that can protect you from viruses, malware and spam.

Protect your personal devices: We all ensure our purses and wallets are secure when we leave our homes and offices, but today we need to take the same precautions with our smartphones. The evidence is hard to ignore: the number of employees using company-provided mobile devices reached 40 per cent in 2010 and the cost of identity fraud in the U.S. is now pegged at more than $54 billion annually. Our smartphones carry access to company data, personal contacts and our bank accounts – even our credit cards. To prevent data theft, make sure that if you are using your device on a Wi-Fi network, it is a secure network. For personal protection, ensure your device is equipped with an application that can track, wipe, lock and back up a lost phone. And for business devices, use an application that allows your corporate security policies to be pushed onto employee devices and enforced company-wide. Although users have been hearing about potential mobile threats for some time, McAfee Labs predicts that 2011 will be a turning point, when more mobile platforms will become targets.

Clearly Canadians need to take a page from the way they act in real life to dictate how they’ll act online. If we want to protect ourselves and our data, we need to use reliable security products that make securing our digital world a reality. If Canadians keep these five principles in mind when evaluating their online behaviours, they will minimize their exposure to risks such as identity theft, as well as the numerous problems that can come along with them.

http://canadafreepress.com/index.php/article/34234