Cybersecurity Awareness Month: 5 Tips for consumers

With October being International Cyber Security Awareness Month people should be more responsible when it comes to what they do on the internet.

Source: pixabay.com

According to Mimecast, a global email and data security company, almost half of global organisations in a recent survey admitted their management and finance teams are not knowledgeable enough to identify and stop an impersonation attack. South African businesses alone saw a 36% increase in this type of fraud, with someone from the legal department the most attractive target for an impersonation attack.

Human error is involved in the majority of all security breaches, and these casual mistakes can cost organisations money, their reputation – and employees, potentially their job.

Organisations need to understand that employees are their last line of defence. To this end, Mimecast develops risk profiles of individual employees to better understand how at-risk they are to cyber attacks. If an employee's risk profile is too high, they receive further training to ensure the organisation - or government department - is as well-protected against cybercriminals as possible.

Here are five tips for consumers to protect themselves against cybercrime, especially as we head into peak shopping season with Black Friday, Cyber Monday and the Christmas shopping period coming up:

Tip 1: Think before you share

Cyber attacks are not just random anymore. They are well-researched and usually architected using the information you share online. Personal details like where you work, job title, who your friends are and what you are doing, are all over social media sites like LinkedIn and Facebook. Hackers use these sites to gather intel on unsuspecting victims – this is called Social Engineering.

Tip 2: Keep your eyes peeled for dodgy URLs

Cybercriminals are getting more advanced in their efforts to trick you into entering your financial details on unsecured websites or convincing you to click on an innocent-looking link that downloads malicious software onto your device. Even if you receive a branded email, from what looks like a legitimate retailer with their logos and fonts, it could be a scam.

Always type a retailer's address into your browser to avoid being redirected to a fake site. And be on the lookout for the all-important https:// (as opposed to http:///). The "s" stands for secure – so that one little letter is crucial to your online safety.

Tip 3: Make use of alternative (and safer) payment methods

Every time you enter your credit or debit card details into an online form is a chance for those details to be intercepted by cybercriminals. Set up a dedicated online shopping account with strict credit and overdraft limits, with only enough money to buy what you need. Alternatively, use the e-bucks, Discovery Rewards and Avios points you've been collecting all year.

Tip 4: If it seems suspicious, it probably is

Keep track of retailers you're expecting a shipment from. If you receive an email that contains tracking information from a courier service or retailer you haven't used, do not click on the tracking URL. This is a malicious link disguised as something familiar. The same goes for attachments – these could contain malicious code. Again, rather type the courier service website in manually to avoid being sent to a fake site.

Tip 5: If you think you've fallen victim to cybercrime – act fast!

- ### Report it to the police

  The statistics provided by the South African Police Service are just the tip of the iceberg – there are many cases that go unreported every year. These reports aid in investigations and can help shut down these cybercriminals and their syndicate organisations for good.

- ### Report it to your bank

  Get in touch with your bank as soon as you suspect something irregular is going on and have your card cancelled immediately. Depending on the circumstances, they may even be able to reverse the fraudulent charge and get your cash back.

- ### Report it to the business you thought you were buying from

  They have a vested interest in knowing they are being impersonated online, and are often better resourced in the hunt to track the perpetrators down. They are also familiar with the processes followed in getting suspicious sites blacklisted or shut down.

- ### Do not negotiate

  If you find yourself locked out of your PC due to ransomware, it's likely the attackers will ask you to pay a ransom to give you back control. And they often ask for payment in untraceable currencies like Bitcoin. But once you've been

identified as a soft target, they'll probably be back for more.