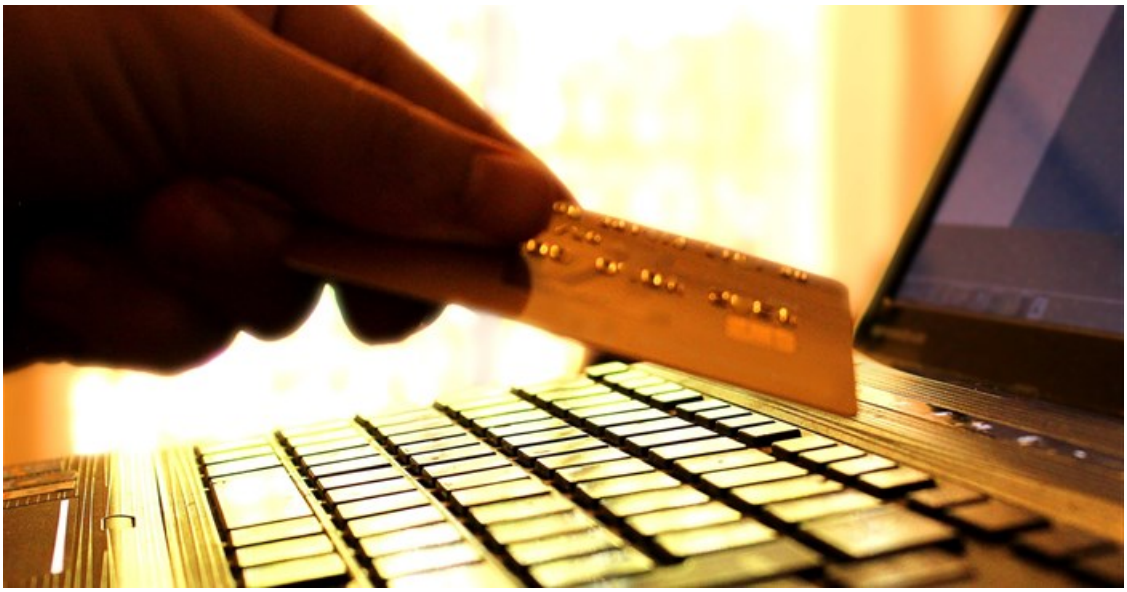
How to avoid festive phishing

Long queues, parking shortages and screaming children - festive season shopping is enough to drive anyone online online. According to research group We Are Social, almost a quarter of South Africans made online purchases over December, 2014.



Jack Mbreh via Stockvault

There's just one problem with skipping the malls: choosing to do your shopping online could expose you to credit card fraud. From fake discounts to spoofed banking emails, cyber-criminals are especially active during the festive season. Mimecast's customer success manager Heino Gevers knows all about the different types of email cyber-crime out there. He offers his top tips to having a phishing-free festive season.

Rein in your social media

Spear phishing - an email scam that targets individuals by using their personal information to lend credibility to a malicious email - has been on the increase over the last few years. While it might be tempting to share the details of your upcoming holiday, this is exactly the kind of information scammers use to pretend to be someone close to you.

Get wise

A huge amount of online crime takes advantage of people's ignorance about security. The best defence against cyber scamming is to educate yourself on internet fraud and phishing techniques. Keep up-to-date on the latest scams going around through the banking platform of your choice so you always know what to look for.

Top up your tech

Are you still running the expired antivirus software that came with your laptop? Outdated cybersecurity software leaves you vulnerable to malware. Employ technology - both personally and professionally - that interrogate unsafe links and websites in real time and non-intrusively. That way, you'll be able to avoid those nasty places on the net where unsafe code lurks.

Look twice

We all love a good bargain, especially during the gift-giving season. Cyber-criminals are well aware of that fact and often

send spoofed emails from retailers full of enticing discounts. If a special looks too good to be true, it probably is. Instead of accessing specials through emails, rather go to the retailer's site in question and search for it for yourself.

Doubt the design

How familiar are you with your bank's corporate identity? Today's email scams are increasingly sophisticated and look disturbingly legitimate. Familiarise yourself with the corporate identity of the businesses you deal with on a regular basis, particularly financial institutions, so you can catch out those small inconsistencies. If something feels off, avoid clicking on anything and notify the businesses.

The devil's in the details

Unfortunately, some emails just look too much like the real thing, right down to the logos, language and terms and conditions. The best way to check if an email is legitimate is to look closely at the URLs within - what looks at first glance as a link to "fnb.co.za" might, on more careful inspection, reveal itself to lead to "fbn.co.za". And always check for the padlock in the URL to make sure you're dealing with a secure link.

Use online tools

If you're unsure of a URL, you can use online scanning sites to check if it's malicious or not. Simply go to a site like "scanurl.net" and copy and paste the URL. If it's compromised, you'll find out immediately. Google is also your best friend when it comes to cyber safety. If you've never heard of an online retailer, research them thoroughly to see how long they've been doing business and what their user reviews are like.

Keep your details close to your chest

One golden rule to keep in mind is a bank or reputable retailer will never solicit personal information such as passwords or credit card numbers directly through an email. This is a red flag that the sender you're dealing with is not who it seems to be. If a business is soliciting sensitive data through a channel like email, stop doing business with them immediately.

Skip the credit card

With cyber scammers more active during the festive season, it's the perfect time to use up all of those loyalty points you've likely amassed through your bank or medical aid. These points are earned and there is a cap on how many you have at any given time, making them much safer to use in online shopping than your credit card. If you get compromised, the damage will be minimal.

There's nothing that will put a damper on a fabulous festive season faster than falling prey to a scammer. Thankfully, by following the above advice, you can shop online with confidence.