Cybersecurity Tips for Black Friday

Source: RSM South Africa Communication

As we head towards the infamous Black Friday and Cyber Monday, cyber criminals will be looking to take full advantage of unsuspecting online shoppers.

When you consider that many of your staff may be accessing these sites from their work computers, one simple mis-click could put the IT infrastructure of the entire organisation at risk. Therefore ensuring that all staff have at least a basic understanding of cybersecurity is essential.

Below is some practical advice to identify phishing and other attacks, thereby reducing your chances of falling victim to online scams and fraud.

BE ALERT AND AWARE WHEN USING PUBLIC WI-FI

Do not conduct sensitive activities or provide personal information such as online shopping and credit card details using a public wireless network. Free Wi-Fi networks are often not proactively monitored and updated and are therefore hacker's paradise owing to lack of security.

ENSURE THE ONLINE SHOPPING WEBSITE HAS AN HTTPS CONNECTION WITH A VALID SECURITY CERTIFICATE

Data that is sent over a regular HTTP connection, between your browser and the online shopping site, is sent in plain text and therefore can be read by any hacker looking to exploit you. HTTPS uses a certificate and secure communication between your browser and the site is thus encrypted. An HTTPS certificate is a public “security certificate” that is issued by a “certificate authority” after several verification steps have been done to confirm the legitimacy of the organisation that is requesting the certificate.

PASSWORD SECURITY

Ensure that you use different passwords for different E-commerce websites and mobile apps. Make use of passwords that are complex and unique, containing a mixture of numbers, lowercase & uppercase letters and symbols. When using your social accounts (Google, Facebook etc.) to login into e-commerce sites, remember to first enable multi-factor or two-phase security authentication on your social accounts so that you are alerted when there is a login attempt to your account.

BE CAUTIOUS ABOUT ONLINE OFFERS

Deals that look too good to be true, probably are. Scammers will often post up an offer that is too good to pass up in the hope that it will lure victims into handing over their credit card details or personal information. If an item usually sells for R10 000 but is on special for R1000, it’s more than likely a scam.

THINK BEFORE YOU CLICK

Use caution when clicking on any unknown links. Delete emails that seem suspicious or are from unknown sources. Links will sometimes lure you onto a website that looks exactly like the original but is hosted at a different URL. Check the domain names and URL’s when performing online shopping and avoid following links from an email. Rather open your browser and navigate to the online shopping site yourself to see if the item is available.

LIMIT THE AMOUNT OF INFORMATION YOU POST ONLINE

When you create a new account on any online shopping website or app, ensure that you only provide the basic information required to create your account. There is no need for you to answer security or privacy questions while making a purchase or checking out on the E-commerce app or website. Hackers often use this information in order to learn more about you in order to hack you more effectively.

GRAMMAR CHECK

As many cyber thieves are located in developing countries, they often fall under the language barrier. They often make use of translation software which is regularly found to misinterpret words. Therefore, if you want to protect yourself from scams, stay away from discount-driven emails filled with spelling errors as they are sure signs of fraud.

ONLINE BANKING TRANSACTIONS

Be cautious when paying for something online. Online shopping sites should make use of secure payment gateways and usually redirect any payment to a secure site or portal hosted by a bank or payment gateway. Verify that this is secure and legitimate before providing your credit card details and OTP. Online retailers have no reason to store your banking details and should not do so. The payment information should only be exchanged with a secure banking portal. Where possible, use a virtual credit/debit card as this is more secure due to the temporary nature of the card's CVV number.

We hope that this information aids in protecting you, your employees and your business from cyber scammers.