Beware of online fraud and phishing scams

Businesses and consumers must continue to be on the lookout for online fraud and phishing scams as fraudsters try to take advantage of Covid-19.

Source: pixabay.com

“Given the speed at which organisations are being forced to respond to the pandemic, the rise of work from home policies as we social distance, increased online transactions, as well as financial relief schemes and support becoming available, we expect to see a rise in fraudulent activity in attempt to get victims to disclose personal or financial information,” says Kevin Hogan, fraud risk manager at Investec.

Over the past few weeks security vendors, researchers and even Interpol have reported an increasing number of malicious activities tied to Covid-19 and predictably, a lot of the activity has involved phishing and social-engineering campaigns using Covid-19 themes to get people to click on malicious attachments and links in emails or to download malware on their devices.

“In many cases, fraudsters impersonate legitimate companies, using similar names, websites and email addresses in their attempt to trick unsuspecting businesses and consumers, even reaching out proactively via emails and messages with surprisingly accurate and personal information,” adds Hogan.

“Some offer banking or relief scheme advice, others offer sites to purchase medical supplies and equipment while others attempt to intercept emails to get important information, especially given the rise of online transactions, shopping and business communication on digital platforms.”

Across the banking industry, the number of fraud cases where the account holder transferred funds to an unintended recipient grew 69% within the last year and given the new channels being used and unpatched home networks being used for corporate communication, this could grow.

This type of fraud, commonly known as Authorised Push Payment fraud, is due to third parties intercepting emails or invoices and altering banking details to divert funds into a fraudster’s account.

“While validating banking details has always been a central component to banking safety - when it comes to suppliers, constant changes and notifications of changing bank account details means, businesses, together with their financial partners should relook this process to ensure accuracy and security,” adds Hogan.

“Businesses and consumers should also be aware of the channels which they use to communicate with their financial institution and remain diligent. We follow strict rules and protocols, and these should be kept in mind during any financial engagement.”

Follow these tips

- Independently verify the company/individual offering the items before making any purchases
- Be aware of fake websites and email addresses – they often look almost identical to the legitimate ones, with subtle changes
- Do not click on unsolicited links or attachments from an unknown sender – or those that reroute you to login screens. Rather go to the URL login screen yourself
- Use unique username and passwords for all your online accounts – and change these every 6-months, especially for online banking
- Do not use your work email address for online shopping and social media accounts
- Never use devices you don’t own or control to log into work, banking and email accounts
- Ensure your devices have robust security installed and that they are running the latest software
- Do not allow remote access to your devices and stay clear of free public Wi-Fi
- Do not share your online banking or login credentials
- Authenticate account details and verify the banking details of suppliers before any payment is made or before asking your bank to make a payment on your behalf
- If you believe you have been the victim of fraud, alert your bank immediately

Fraud and cybercrime in today's money market is, unfortunately, on a sharp increase and so, the value of a relationship with your banking partner takes on a whole new dimension, especially during these times. Given they understand the role players, the business cycles and the authority matrix, they're usually able to pick up any fraudulent activity before it takes place.

"In these out of the ordinary times, extra vigilance is needed to safeguard your business and protect yourself from fraud," concludes Hogan.