Media Release

Working from home? Here's how to protect yourself from COVID-19 themed cyber scams

An overload of COVID-19 communication sets the perfect scene for malicious actors, says a UNSW cybersecurity expert.

With a full lockdown looming, working remotely is expected to be the new norm for many professionals. But for many organisations, working outside a secure office environment could lead to vulnerabilities in the maintenance of IT systems that cyber criminals can exploit.

"While the world is grinding to a halt, cyber-attacks are on the rise, preying on public fear and anxiety," says Yenni Tim, researcher of Cybersecurity at the UNSW Business School.

As the number of COVID-19 victims increased throughout the month of March, so did the number of phishing email attacks. Between 10 and 26 March, the Australian Cyber Security Centre (ACSC) received more than 45 cybercrime and cyber security incident reports from individuals and businesses. All 45 cases were linked to COVID-19 themed scams and phishing activity.

The ACSC reported that many of those phishing emails were sophisticated and contained malicious links to fake websites that automatically installed viruses on the user's devices once opened. In doing so, cyber criminals have the ability to steal the user's financial and personal information.

Anxiety and fear fuelling the rise in phishing attacks

In times of crisis, opportunistic malicious actors aim to exploit our vulnerabilities, Dr Tim says.

"Being able to quickly identify common patterns in phishing emails is very important because the health crisis has triggered anxiety and fear in our nation – emotions that malicious actors are always taking advantage of," she says.

Cyber criminals feed off the fear of individuals, especially during current uncertain times where people are more likely to act irrationally and will do anything to get more information about the pandemic.

KPMG's report on COVID-19 stated that malicious cyber actors use the tactics of impersonating well-known organisations such as Australia Post or the World Health Organisation (WHO) to lure people to provide their confidential data.

"Being isolated from the workplace community has increased the risks of phishing attacks as people can no longer easily turn to a colleague to confirm the legitimacy of an email," Dr Tim says.

Many people can also be more vulnerable and have less capacity to be vigilant as they are overwhelmed by a new way of working, while simultaneously having to look after their family and ensuring their own health and safety.

A lack of concentration is a key factor in scam success. “Due to an increase in the volume of communication relating to COVID-19 – such as official company updates, check-ins from insurance and healthcare providers and the government – people have become overloaded with information. This sets the perfect scene for malicious actors looking to throw a phishing email in the mix,” Dr Tim says.

The reported surge in traffic on video conferencing apps such as Zoom is also a cause for concern for many businesses that are carrying out meetings through virtual conferencing and collaborative tools.

“As more people start using online communication platforms, such as Zoom or Teams, opportunistic and malicious actors will be very quick in setting up phishing attacks. They send Zoom look-alike emails embedded with malware, or bring people to malicious websites with the word ‘Zoom’ in them to trick them into providing data or download malicious files,” Dr Tim says.

What are common patterns of phishing attacks?

Phishing emails and SMS phishing (also called smishing) typically take the form of the following three patterns. Dr. Tim cites a few real COVID-19 themed phishing emails as examples:

- **Demanding urgent action**

E.g. Dear colleagues, we have been hit by COVID-19. One of our team members has tested positive for the virus. Please study the attached document and follow the next steps.

- **Too good to be true**

E.g. Hi, I have tried to call you twice today. Because of the coronavirus situation, we are reaching out to transfer some support fund to your account in the next few hours. Please confirm here that your details are correct.

- **Impersonation of well-known organisations**

E.g. The WHO is sending you important safety information, click this link or open this attachment.

E.g. This is an email from HR: Please take a minute to enrol in the following ‘working remotely’ online module. Note: this is a compulsory module and we expect all staff to complete them today.

E.g. Service companies such as telecommunications and travel companies are sending you their renewed refund policies in response to the health crisis. Click here to learn about your eligibility.

“We have seen malicious actors tailor their social engineering attacks based on the latest trends at the time, such as Bitcoin back in 2018, and now we are facing COVID-19 themed social media, text messages and email campaigns,” Dr Tim says.

The malicious activations in such phishing emails and texts commonly include:

- Attachments which can trigger the download of malware (e.g., a macro-enabled Microsoft document triggers the download of Emotet malware)
- Links to fake versions of authority websites (such as WHO) that solicit the user to provide their username and password
- Links to websites with service advisories prompting people to download malware-infected files and executables

How to protect yourself from social engineering attacks

Dr Tim has four recommendations to protect yourself from cyber scams.

First, be very vigilant when an email or text asks you to do one or more of the following actions:

- Open or download an attachment or mobile application
- Click on a link, and/or
- Provide your data (by going to an impersonated website or replying to the email)

These are the most common giveaways that an email or text message is malicious. Dr Tim also recommends that you:

- **Avoid acting on emails using mobile devices**

Research carried out by Dr Tim shows that people are more susceptible to phishing attacks when reading emails on their mobile devices. This is because it's more difficult to verify the legitimacy of an email when viewed on a mobile device. Mobile users also tend to be always 'switched on' and malicious actors can easily take advantage of this – especially with phishing emails that demand immediate action. People also tend to be more distracted when reading emails on their mobile phones, which means they are less likely to apply the proper scrutiny.

- **Verify the sender and look for the official announcements**

Hover over or tap the sender's email address to make sure the person is who they claimed to be. It is common for malicious actors to disguise their email addresses with lookalike letters, or domain names that closely resemble legitimate domain names. When in doubt, do a quick search instead of replying to the email or do anything they are asking you to do.

"For example, if you receive an email that appears to be from the government, informing you of a new mandatory registration process that you would need to comply with due to the COVID-19 outbreak – do not action directly through the email," Dr Tim says. "Instead, search for the official government website and look for the official announcement."

- **Be wary of emails and texts that directly solicit your username and password**

Just remember, authorities such as WHO or the government will never ask for your username and password to unlock an email attachment or access health and safety information. They will also not request your bank account information through emails or texts to process a donation or to access any funds.

What are the key security challenges that organisations are facing?

As the workforce rapidly shifts to working from home, there are a couple of key security issues that many businesses face.

The first issue is that many organisations didn't plan to have their entire workforce working from home and had to move quickly to provision for remote working capabilities, says Bianca Wirth, Director of Cybersecurity at KPMG Australia.

"In such situations, if these businesses didn't have the right infrastructure in place, security may not be at the forefront of rapid deployments and compromises would have to be made."

"It is also important for organisations to ensure they are not just looking at security from a phishing perspective, but on their mobile devices. Having the right device management solutions and policies for accessing emails on non-work devices is critical to ensure your data stays safe while people are working remotely," Ms Wirth says.

There is also the physical security aspect of people working from home and the risks involved with discarding confidential documents in residential garbage bins instead of secure destruction bins.

In its recent COVID-19 report, KPMG advised employers to protect themselves by taking additional steps such as:

- Ensuring all communications go through an official single channel in your company and providing regular communications on the approach your organisation is taking on COVID-19.
- Making sure your finance processes go to the finance team for approvals, especially any requests for large payments. This safeguard can protect the business against the risk of business email compromise and CEO frauds. Ideally, use a different channel such as calls or texts to confirm an email request.
- Re-assessing your approach to pushing critical security patches down to computers connected to your VPN, updating firewalls and anti-virus software across your IT network and encrypting data at rest on laptops used for remote working.

Although a number of SaaS-based phishing simulation services companies have published COVID-themed templates, Ms Wirth discourages organisations from running these phishing simulations as part of their security education and awareness program due to their insensitive nature and to avoid any confusion with official announcements made from the corporate communications team.

“In situations like COVID-19, it is important to have streamlined and coordinated communication throughout the organisation. You have to work closely with your internal communications and crisis management teams to vet security communications and integrate security messaging into the broader business communications,” Ms Wirth says.

The ACSC anticipates an increase in scams and phishing attacks over the coming weeks so it is essential for organisations and individuals to stay vigilant and be on high alert.