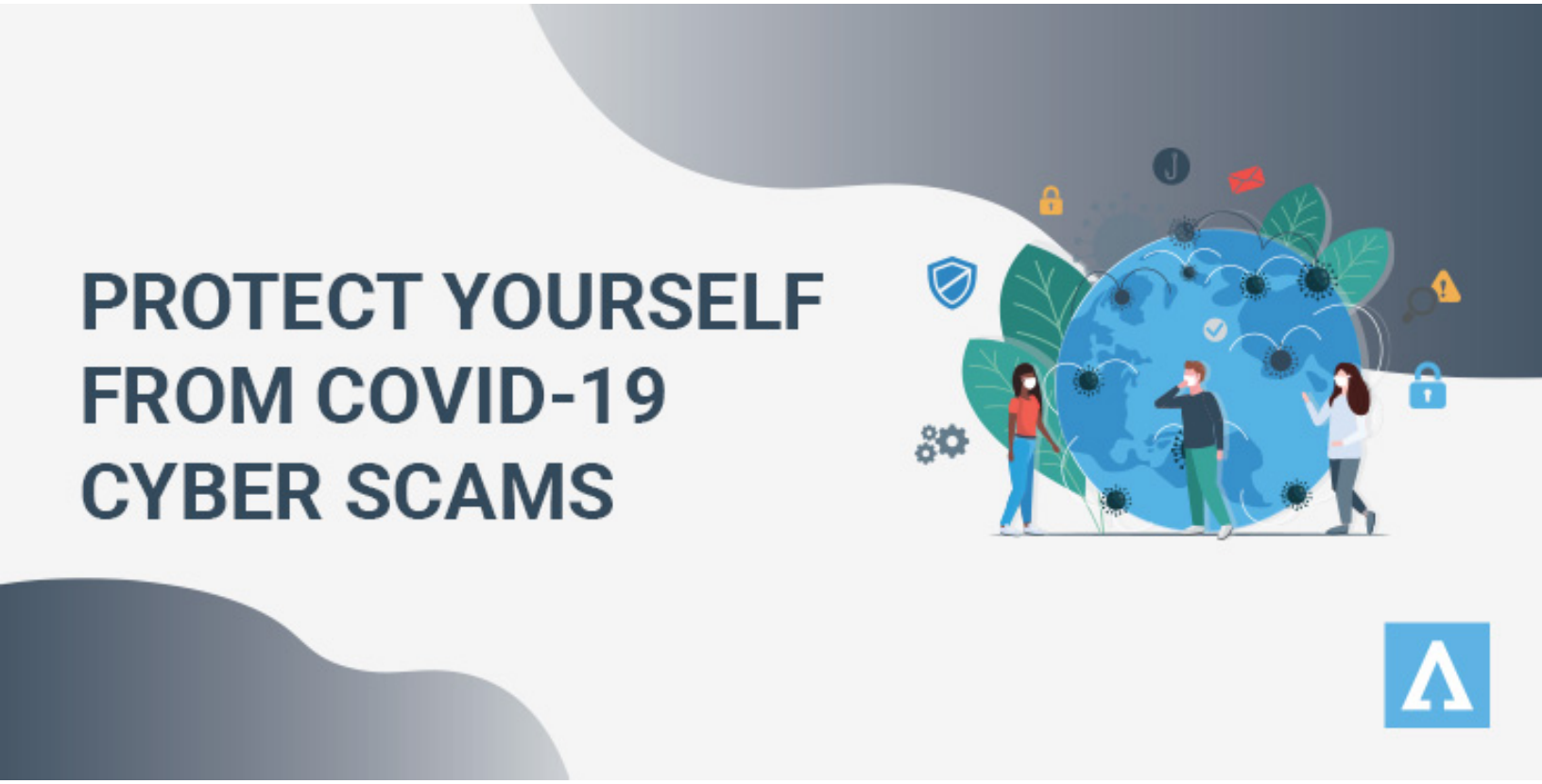

Protect Yourself From COVID-19 Cyber Scams

A New Wave of Cyber Attacks is Happening Worldwide

Cybercriminals know that many people are adjusting to a new normal, making it easy to trick them with savvy COVID-19 phishing emails and text messages. Cyber attackers are leveraging the fear and uncertainty created by this event to trick unwary users. This is why it's so important to maintain cyber security awareness training campaigns and phishing simulations.

Worldwide COVID-19 has closed offices, schools, and companies. People are living in lock down, quarantine, self-isolation, and implementing social distancing. Employees are working from home under the new COVID-19 protection measures.

The new realities of COVID-19 have changed every aspect of our lives. However, one thing has not changed – cybercriminals continue to actively target victims with phishing attacks.

COVID-19 phishing emails, BEC scams, smishing, and vishing attacks are happening worldwide.

> “Unfortunately, scammers are taking advantage of the spread of coronavirus to exploit and play on the fears of consumers across Australia.
>
> Scammers are doing things such as falsely selling coronavirus-related products online, and using fake emails or text messages to try and obtain personal data.
>
> Other scams include phishing emails and phone calls impersonating the World Health Organisation, government authorities, and legitimate businesses – including travel agents and telecommunications companies.” (COVID-19/coronavirus Scams, Scamwatch Australia)

Individuals who are directly affected by this pandemic are the prime target of COVID-19 cyber-attacks, whether working from home or using the Internet for personal email and social media.

The Economic Costs of Phishing

A successful phishing attack can have devastating impacts on businesses, regardless of size, location, and industry. Consider these statistics on the economic costs of phishing so far in 2020:

$17,700 is lost every minute due to phishing attacks
Data breaches cost enterprises an average of $3.92 million
Phishing attacks account for more than 80% of reported security incidents
94% of malware is delivered by email
The economic fall-out of COVID-19 is massive and it will be long-lasting. The last thing any company can afford is the economic cost of a phishing attack.

Your employees’ personal life can also be impacted as many of these scams are used to commit financial fraud or identity theft.

Keep your employees and your business protected – download our free Working From Home Cyber Safety Kit. This special kit gives you actionable tips and best practices to keep you and your employees cyber secure when working from home.

Dealing with the Phishing Threat when Working from Home

Employers had very short notice on how to prepare employees to work from home. This rush to get employees working from home has opened many security flaws and doors that hackers are waiting to exploit.

Cybercriminals know that employers did not have the opportunity to train employees on how to work from home securely or to ensure that all laptops have the latest software, security patches, and operating systems installed.

Couple with this the uncertainty each of us is facing around COVID-19 – and it is really easy to believe an email about COVID-19 vaccines, a sale on masks or gloves, or an email purporting to be from an official government health agency.

To protect employees and your business, share these keys to working from home securely and safely:

- If you don't recognize the email sender, don't open the email.
- If the email or text message sounds too good to be true – it is.

Be aware of cyber scams about COVID-19 treatments, testing, vaccines, quarantine measures, and information from government officials.

- Pay attention to the spelling of email addresses, subject lines, and email content.
- Be wary of emails using urgent language or that ask you to share your confidential information.

No health agency or government department will email you asking for your health details or sell you a COVID-19 vaccine or test.

- Do not click on links in unsolicited emails or text messages.
- Never send confidential information in an email.

The Red Cross, World Health Organization, and your government health department will never ask for your confidential information in an email.

- Do not accept social media followers or friends from accounts you do not recognize. If an account that you do not trust follows or friends you, block the account.
- Do not trust social media posts promising COVID-19 cures, tests, vaccines, or selling masks and gloves.
- When in doubt, do not click. This includes downloading attachments, clicking links, and filling out web forms. Contact your IT department whenever you have doubts about an email.

If you receive a message or call from someone pretending to be a health official, colleague, or government employee about COVID-19 – do not interact with the caller – hang up immediately and if possible, block the sender or caller.

How Cybercriminals are Using COVID-19 To Phish and Hack

The COVID-19 phishing emails, vishing, smishing, and social media scams are not isolated to one location or demographic. Everyone (even us) has received a COVID-19 related cyber attack message.

Consider these news headlines from around the world about COVID-19 and cyber attacks:

- Cybermenaces : l'autre risque épidémique du Covid-19 (France)
- COVID-19 Scams Are Everywhere Right Now. Here's How to Protect Yourself (United States)
- Des fraudeurs imitent l'Agence de la santé publique du Canada (Quebec, Canada)
- Beware of criminals pretending to be WHO (World Health Organization)
- Attackers using COVID-19 themed scams (New Zealand)
- Here's what you need to know about the COVID-19 scams popping up in Canada (Canada)

- COVID-19 Complication: Ransomware Keeps Hitting Healthcare (Worldwide)

The cyber threats around COVID-19 are real and they will only increase. COVID-19 is a great opportunity for cybercriminals to exploit the natural human behaviors of fear, trust and wanting to help.

> "The stereotype of a cybercriminal is that of a bored teenager who is computer literate and socially maladjusted. This is far from the truth and every time there is a crisis we can see that cybercriminals are in reality ruthless and heartless individuals looking to inflict suffering on their victims in whatever way they can, and if a global crisis, such as COVID-19, plays to their advantage they will do so," says Brian Honan, head of Dublin-based consultancy BH Consulting." (COVID-19 Complications: Ransomware Keeps Hitting Healthcare)

This is why we put together the Working From Home Cyber Safety Kit. We want to make it easy for you to maintain your security awareness training campaigns and phishing simulations during this pandemic.

Share These Working From Home Cyber Aware Strategies With Your Employees

Cyber security must remain a priority when you're working from home. We understand that this is a challenging time and it's easy to forget cyber security best practices and lessons.

To stay cyber aware and secure, make sure you:

- Use the secure connection we provided to connect to the company network. If you have questions about configuring the company VPN, contact the IT department.
- Do not connect to the company network with an unsecured public Wi-Fi network.
- Do not share work data and information to your home computer or personal devices. It's important that you only work on computers and devices that have the latest security updates installed for operating systems and browsers.
- Make sure your computer has the latest applications, operating systems, network tools, and internal software installed. Talk to the IT/support team about installing malware protection and anti-spam software on your work computer.
- As soon as you're set up to work from home, create new and strong passwords for your laptop, corporate mobile device, and email.
- Use only approved cloud applications for sharing and storing data.
- Do not store or print paper documents with sensitive information at home. If you have to print a document, please shred the document immediately after using it. Do not put these documents in your recycling bin.
- Use only company approved call and video conferencing applications for your meetings and beware of unexpected requested to join a conference call.

Remember to continue with your cyber security best practices. Do not click suspicious emails or respond to text or phone messages. No one from the office will email you or call you asking you for confidential information.

Please remember that cybercriminals are sending COVID-19 phishing emails, text messages, and phone calls. Your health department, city officials, and government officials will never contact you with news about a COVID-19 vaccine or test or ask you for your confidential information.

TERRANOVA
SECURITY