Secure Tomorrow

Minet

AON | Global Network Correspondent

## MINET THOUGHT LEADERSHIP

Minet is a trusted pan-African advisor that meets the uncertainties of tomorrow by delivering risk and human capital solutions today. As the largest Aon Global Network Correspondent, Minet has access to a network of over 50,000 colleagues in 120 countries as well as to proprietary data, research and analytics which enable us to manage and secure the risks of tomorrow and provide clients with an unrivaled advantage. For more information, please visit www.minet.com

**Risk. Reinsurance. People.**

# HOW TO RECOGNIZE AND AVOID PHISHING SCAMS

July 15, 2019

You receive an email from a trusted entity or your bank with a link to verify information. It looks real except it is not. You assume it is your bank's website, so you log in with your details. At this point, the scam is done, and you have handed over your banking password to crooks who can use it to steal from you. This is phishing!

There are many types to it, as much as it is just another one of many cyber crimes. Scammers impersonate legit institutes such as bank websites to fool businesses into giving them important information, which they in turn use to take their money and to cause deceitful disruptions in companies' operations. It is important to note that phishing emails can be sophisticated and very convincing, therefore one should pay particular attention to every detail of every email address that you release any kind of information to.

Attackers use many different tricks to make you believe an email is legitimate. Some of those tricks include the following:

- Faking the email address to make it look like it is from someone you know and trust. One should not use the reply button to respond to suspicious emails, instead, open a new window and type in the official website of the institute in question to verify their contact details
- The emails will often threaten you, by for instance stating that the security of your account has been compromised. One should not click on any links that promise to fix your account or computer malfunctions from suspicious emails
- Malicious emails often contain misspellings, grammar mistakes and often start with an unfamiliar greeting or salutation as they do not know your name.
- Phishing emails may use the same logos and phone numbers that appear on your statements and bills, without exceptions, you should always be suspicious of emails that ask you for your (personal) information

Meanwhile, Mimecast's report on The State of Email Security for 2019 records that email attacks are on the rise. The report shows that 88% of organizations have seen email-based spoofing of

business partners and vendors while 67% has reported increases in impersonation fraud and ransomware is on a 26% hike.

It also states that phishing attacks themselves appear to be more a matter of when rather than if organizations will face them. The results show that 94% of respondents experienced a phishing attack in the previous 12 months, while 54% also saw this type of attack increase. Specifically, 45% of organizations saw an increase in targeted spear-phishing attacks with malicious links.

There is no harm in receiving phishing emails if you delete them. However, the risks of attacks are increasing in complexity and basic awareness alone is not sufficient in ensuring your company's cyber security. It is vital to have technologies, processes and controls designed to protect systems, networks, programs and devices from cyber-attacks.

## IS THERE A RISK TRANSFER MECHANISM FOR CYBER RISKS?

Keeping your company secure should not cripple you with stress and fear, rather transfer the risks of cyber crime to your insurer and continue business as usual. As part of a risk management plan, organizations routinely must decide which risks to avoid, accept, control or transfer. Cyber Risks Insurance cannot protect your organization from cyber crime, but it can keep your business on stable financing footing should a significant cyber breach occur. A Cyber security insurance policy will cover losses and liabilities for a business that uses the internet and systems for its operations. Your trusted insurer should be aware of the cyber threats that your business could be facing, and as such aid in implementing strategies that will improve your cyber resilience while assuring you of covers for your financial losses in case of attacks.

We cannot overemphasize the importance of raising awareness and understanding of email security policies and best practices across your organization as the first step toward building cyber resilience. These advances in cyber threats call for cultural shifts to ensure that everyone, regardless of their title and position, understands that they play a vital role in ensuring that your organization's cyber security is stable. At Minet we believe the future of cyber risk management must be proactive, oriented around sharing threat intelligence and collaborating within (and across) enterprises and industries. IT staff must constantly hunt for bad actors and raise the bar on preparedness for the inevitable day when a strike does come. Minet's Cyber Solutions can assist to explore the cyber risks that organizations may face no matter where they are on their digital journey.

**Liteboho Semoko** | Accountant Finance & Admin | Minet Lesotho