MOBIUS
CONSULTING

Actualising change

WARNING! SPIKE IN CYBER ATTACKS

With the festive season on the horizon, studies show that we can expect an increase in cyber attacks. As you prepare to do your holiday shopping, cyber criminals are also preparing to take advantage of the **Black Friday** and **Christmas deals** in physical stores and online stores. Therefore, we strongly urge you to be alert (especially if you plan to do your shopping online).

TYPES OF ATTACKS

- **Phishing Scams** are when attackers disguise themselves as reputable brands and trick you into sharing your personal information (e.g. credentials, credit card information, etc.) with them. You may be tricked into clicking on a suspicious email disguised as a Black Friday or Christmas deal.
- **Ransomware Attacks** are a tactic scammers use to gain access to your systems and lock you out, demanding that you pay them a ransom fee before they relinquish control.
- **E- skimming/ Magecart** is increasing in frequency. Attackers use this technique to inject malware into websites that have e-commerce capabilities and steal customer details and banking information.

The rise of online shopping has increased the opportunities for hackers to exploit the situation and target innocent consumers.

WHAT TO DO IF COMPROMISED?

BE VIGILANT AND DON'T PANIC.

1. Contact your information security team to report any information security incident. They will instruct you on what to do.
2. Make sure all your devices have the latest software updates installed plus up-to-date antivirus and anti-malware software installed. Run security and antivirus updates once a day.
3. Ensure your email service protection features are enabled.
4. Enable multi-factor authentication (MFA) on all your accounts where this feature is available.

HOW TO STAY SAFE:

A few simple ways to recognise phishing attempts. These are some of the tell-tale signs:

Spelling and Grammar:
Cyber criminals aren't known for their great grammar and spelling.

Suspicious Links:
If you suspect that an email message is a scam, don't click on any links. Rather search for the article subject in Google and find a reputable source for the information. When in doubt, don't click!

Suspicious Attachments:
If you receive an email with an attachment from someone you don't know, or an email from someone you do know but with an attachment you weren't expecting – don't click and open the attachment. Rather call them first to confirm.

Threatening Tone:
Cyber criminals use fear and panic as a tactic to entice you to react in haste and often irrationally. Again, don't panic and contact your information security team.

Website Spoofing:
These emails appear to connect to legitimate websites or companies but take you to fake scam sites.

Altered Web Addresses:
A form of spoofing where the web address closely resembles the name of a well-known company, but is slightly altered; for example,"**www.mobuisconsulting.co.za**" or "**www.mobuisconsutling.co.za**".

Mismatches:
The link text and the URL are different from one another; or the sender's name, signature, and URL are different.

PLEASE SHARE WITH FRIENDS, COLLEAGUES AND FAMILY.

Contact Mobius Consulting: **CPT** +27 21 201 1120 | **JHB** +27 10 590 6111 | **UK** +44 84 5544 4656 | **MU** +230 5297 0903
SA: info@mobiusconsulting.co.za | **UK:** info@mobiusconsulting.co.uk | **MU:** info@mobiusconsulting.mu