momentum insure

Ensuring you protect yourself and your ***business' financial and corporate data***

As a result of more people accessing corporate data and systems from their remote working locations that may not have the same security specifications at their office sites, the risk of cyber threats to corporate and customer data is growing. Consequently, social engineering tactics from cyber criminals including phishing emails, have also grown in popularity as a tactic to steal consumer data such as usernames, passwords or credit card details by masquerading as a trustworthy organisation.

In fact, by 2020 already Mimecast's Threat Centre detected a whopping 64% growth in email threats. Moreover, a recent poll from consumer credit reporting agency, TransUnion, also revealed that 40% of consumers reported being alerted to digital fraud attempts that had been targeted at them over the course of the last three months, with 5% actually falling victim to these kinds of cyber threats.

In order to diffuse these threats, customers need to familiarise themselves with the tactics employed by cyber criminals, like phishing, and protect themselves as well as their businesses through avenues like insurance cover.

A phishing scam is an act of fraud where scamsters send emails or messages (via SMS or an app) that appear to come from a reputable organisation like a bank or even your insurer. The email or message usually asks you to click on a link or download an attachment. Once you click on the link or attachment, you are taken to a fake site, which resembles the real site, where you will be required to submit your log in details and once you log in, the fraudsters have your personal credentials and can access your accounts.

How you may be targeted:

You may be contacted by someone using the name of your service consultant but from a different email address, with an invoice attached to make payment on your premium. The invoice looks like it's from Momentum Insure but the banking details on the invoice are however not that of Momentum Insure and the mail is not being sent from within Momentum Insure.

The email chain between you and your consultant may have been intercepted and monitored by the scamster and therefore the banking details on the invoice belong to the fraudster and not Momentum Insure. Please make sure that you double check the email address and verify banking details, with your service consultant, prior to making any transactions toward your premium.

The following tactics have been identified as recurring by our claims and investigations teams.

- **Promise of wealth:** Scamsters are baiting people with the promise of them having won a prize (frequently linked to topical news events such as tickets, flights and accommodation to the Africa Cup of Nations knockout matches) or some other unexpected event of financial gain, eg an overseas relative passing away and mentioning you in their will.
- **Lottery scams:** Other popular forms of cyber threats include lottery scams that involve an email or social media message stating that you have won the lottery or a prize draw for a luxury item. The recipient of this is then expected to make a "small deposit" in order to have the prize couriered to them.
- **Counterfeit goods:** Cyber criminals and fraudsters are also using legitimate platforms such as Facebook Marketplace or Gumtree to create false advertisements to sell counterfeit products in an attempt to scam people.
- **Proof of payment:** Be very suspicious of offers that are too good to be true and sellers who request for a PoP (proof of payment) before you have viewed the product in real life. Never handover items to anyone until you have verified that the money is actually in your account. Don't rely on PoP because it can be falsified. Also avoid concluding a private sale over the weekend as you may not have access to verify the validity of the PoP.
- **Unscrupulous car dealers:** Unscrupulous car dealers usually sell written-off vehicles with prior accident damage at retail value without informing the buyer. The vehicle could have many underlying defects and there's usually no restitution against these dealers so it's wise to always purchase from reputable dealerships.
- **Scare tactics:** Cyber criminals and scamsters may also opt for the stick instead of the carrot, by employing scare tactics such as stating that you have an overdue invoice that will be handed over soon. Things to look out for here are unusual email attachments or emails from banks or other financial institutions requesting your personal information.
- **Sharing login details:** Remember that no financial institution will ask for your login details, so never share these details with anyone over email or the phone. If you have the option to activate a double or multi-factor authentication, please do so, as this will make logging into your web portals or confidential applications, such as banking applications, even more secure.
- **Suspicious branding:** If the logo or branding of the business on the email you receive appears suspicious or the address that you usually receive emails from appears strange, move it to your spam folder rather than responding to it.

Ultimately, while hybrid working has become the new norm and has enabled a lot of opportunities, it has also allowed for cyber threats to become more prominent. Following these tips should help ensure that you are protected against such crimes.

For more information or advice, please contact us on 0860 784 767.

For more information follow our official social media pages:

Facebook: @MomentumZA
Twitter: @Momentum_za
Instagram: @momentumza