African Bank Ltd press release

17 April 2020

10 tech safety tips when working from home

Amid all of the physical disruptions that have been caused by the global spread of COVID-19 and with so many people working from home, targeted phishing scams, disinformation campaigns and disruptive cyberattacks have been common during lockdown.

"These scams can steal information, create panic and worsen the economic and social impact of the virus. Individuals in particular should be cognisant of these threats. Remember even if travel and commercial activity are limited during this time, cyberspace remains relatively open for business," cautions Penny Futter, African Bank's Chief Information Officer.

She provides the following 10 tips for anyone working at home:

- Be aware of any suspicious emails or other electronic activity that may come across your screens, phones and emails. Do not click on or provide any information with suspicious links or which include requests for sensitive/private information, unless you are 100% sure you can trust the source. Phishing scams are rife and you need to be especially wary of phishing scams targeting remote workers with sensational or emotional messages. Without your colleagues around, you need to be extra vigilant of both email and phone scams. If you are working remotely for a company, ensure you report any suspicious messages to your IT Security team.

- Be aware of disinformation campaigns and hoaxes, particularly on social media. These campaigns can cause confusion, increase public panic, and lead people to overreact or underreact to the virus.

- Your passwords are the key to the kingdom so guard these closely. Without the company network to protect you, the power now lies squarely in your hands, or your passwords. Make sure your password for each critical site is strong and unique. Check the policy on password managers and use one if allowed.

- Use Multi-Factor Authentication wherever possible. Futter says this means combining your username and password with something that you own, such as a One Time Password app on your phone.

- Don't fall for "credential phishing" attacks, where scammers trick you to hand over your username and passwords. Best is to not ever click on links asking you to update details. Rather bookmark the sites you frequently visit or type them manually into the browser.

- Apply all basic security features. Keep your operating system, plug-ins and anti-virus software up to date and apply security patches when necessary.

- Secure your home WiFi Network. There are two basic must-dos to set this up securely: Change your default router password and change the password for your WiFi network. Whatever you do, do not run a WiFi network without a password.

- Keep your work environment private. Keep your home environment safe and ensure nobody is allowed to access your work computer, including your family and kids if you are working with sensitive information. Others could unintentionally download malicious software or access files they shouldn't see. Ensure that your work conversations remain private and check your policy on smart home devices like Alexa or Google Home. If possible also try and avoid printing at home, and if you must, make sure you lock sensitive documents away and shred them before discarding them.

- Use a VPN. Using a virtual private network (or VPN) provides a secure tunnel for all your internet traffic, preventing criminals from intercepting your data. Ask your security team to set one up for you.

- Last but not least ensure you read your policies. They are there to keep you, the company and its data safe. In turn, this allows you to work in the comfort of your PJs and slippers.

"Remember during this highly challenging time you are your company's strongest line of defence so remember to remain super vigilant," concludes Futter.

ENDS

Visit the African Bank website or like them on Facebook , Twitter and LinkedIn

PREPARED ON BEHALF OF AFRICAN BANK BY CATHY FINDLEY PR. CONTACT JACQUI MOLOI ON JACQUI@FINDLEYPR.CO.ZA OR (011) 463-6372 WITH ANY CONSUMER PR QUERIES.