African Bank Ltd press release

April 2021

Don’t be caught out by these common scams

While many of us are staying safe during the Lockdown, scammers are using people's real fears about the impact that the Coronavirus is having on their finances, to steal their money. It is important that consumers are aware of these scams and stay protected, particularly since so much of our work and business transactions are being conducted almost exclusively online these days.

Piet Swanepoel, Chief Risk Officer at African Banks, says unfortunately it never takes long for scammers to take notice. “These cyber criminals have updated their fraudulent online tactics to cash-in on the pandemic. The scams can take various forms, each designed to target unsuspecting online users,” he says.

Swanepoel cites five of the most common tactics which are used to catch unsuspecting people out:

1. **Fake calls and texts:** Scammers create fake emails or texts, which mimic the look and feel of legitimate institutions, to trick one into sharing valuable personal information like bank account details, ID numbers, passwords etc.
2. **Online scams:** Email scams that trick one into opening malicious attachments or clicking on links that allow scammers to steal your passwords, ID numbers, and bank details.
3. **Donation scams:** There have been reports of thieves taking money from consumers by claiming they are collecting money for charities or NGOs.
4. **Fraudulent online loan sharks:** Illegal money lenders are preying on people’s financial hardships, charging exorbitant interest rates for loans.
5. **Fake vouchers and refunds:** Scammers are offering fake vouchers for groceries or refunds on bank transactions, just to get unsuspecting South Africans to share their personal information.

He says these are just a few of the examples of how scammers are taking advantage of the difficult time the world is going through but are the most common to look out for. It is very important to learn how to protect yourself from being a victim of these scams. Being aware of any suspicious emails or any other unusual electronic activity that may come across your screens, phones and emails is the first step in protecting yourself. “You should never click on any unfamiliar or suspicious links, or comply with requests for sensitive/private information, unless you are 100% sure you can trust the source,” he says. Being aware

of disinformation campaigns and hoaxes, particularly on social media is also important so you can spot the hoaxes when they cross your desk.

Swanepoel says the next absolutely key requirement is having a strong and unique password for each critical site. “We recommend you use multi-factor authentication wherever possible. This means combining your username and password with something that you own, such as a One Time Password app on your phone.”

Then of course one must continue to apply all basic security features such as keeping your operating system, plug-ins and anti-virus software up to date and applying security patches when necessary.

If you are working from home you need to ensure you have secured your home Wi-Fi network. Swanepoel recommends you consider using a virtual private network (VPN) which provides a secure tunnel for all your internet traffic, preventing criminals from intercepting your data.

Finally, since many people may be wanting to get away during the April holidays it is worth noting that the final scam is advertising fake holiday accommodation and air tickets on public reseller sites such as Facebook and Gumtree. Many even have their very own fake website. The advert/website looks legitimate and the price appears to be cheap but as soon as the victim makes a purchase, thinking they are buying from a genuine person/company, the victim will find out they have been scammed and never receive the goods and can no longer contact the seller.

The golden rule is do not trust websites you do not know and if an offer look too good to be true, it is probably fake. Swanepoel recommends before you buy based on an ad or post, check out the company/person by typing the name in a search engine with words like or “scam” or “complaint.”. “Always be cautious if you are purchasing from someone you have not met or if you haven’t verified the product. Should you suspect that you are being targeted by a scammer, stop all communications immediately and report it to your bank immediately,” he concludes.

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 0717648233 WITH ANY CONSUMER PR QUERIES.