CYBERSECURITY WEBINAR – 28 OCTOBER

TIPS AND RESOURCES

In this document

1 Q&As from the session

I have too many passwords to remember and need to change them often – any tips on how to store these digitally and securely?	Get a password manager – there are various options. • For one device, you can download 1Password (which is free). • If you want to install it on more than one device, you'll need to buy a licence. To view other password managers, click here.
Would you recommend additional third-party virus protection (eg Avast) if I use Office 365, or is the Microsoft built-in protection sufficient?	We recommend buying an antivirus solution, like McAfee, Kaspersky, Norton, and ESET, among others. They range between R300 and R600 per licence a year.
What is the best way to create and remember passwords?	• Create a passphrase or a pass-sentence, and then change some of the letters to special characters or numbers. For example: Travelingismyfavouritehobby! could be changed to Tr@vel1ng1smyf@vour1teHo66y! • If you want to use your pet or your kid's names in a password, use it as part of a sentence. • Using spaces between your words will strengthen your password. • Always use a combination of uppercase letters, lower case letters, numbers and special characters.
Is it safe to use the face recognition function for my banking app?	Yes, definitely.
Is it necessary to have an antivirus solution for my phone?	It is highly recommended.
IOS versus Windows security – which is safer?	https://www.forbes.com/sites/daveywinder/2020/02/11/platform-wars-2020-apple-security-threats-outpace-microsoft-windows-for-first-time/
How can I set up my online presence to protect myself from hacking and to keep my home business network secure?	• Work on secure, password-protected internet connections. • Change the default username and password on your WiFi routers and ensure it is strong and unique – '#Corona2020' is not going to cut it! • Don't use the same password across all devices and accounts. Every device and account need a strong and unique password, or even better, a passphrase. • You could get a VPN (virtual private network) so that all your internet connections are secure and encrypted.
Advice on hacking of bank accounts – how easy is it for someone to hack and steal money and what makes a person a target for this? If I get scam calls, does the fact that I am speaking to them give them access to my online banking profile and habits?	• Hackers can steal money and defraud you only if they have your account credentials, ie your username or profile number and your password. They can get these details only if you give it them, either by entering it into a fraudulent site through a phishing email or over the phone through a vishing call. • Rule of thumb: Never enter your credentials via a link in an email or give your details to anyone who asks for it over the phone – your bank will never ask you to do this. If you get a call from your bank with an offer that sounds too good to be true or from someone from the Fraud Department reporting a fraudulent transaction and they need you to verify your details, offer to call them back and then log in to your account to verify the call. • To enhance security, enable two-factor authentication when logging in to your account and if possible, use facial recognition.

NEDBANK PRIVATE WEALTH, AN AUTHORISED FINANCIAL SERVICES PROVIDER THROUGH NEDGROUP PRIVATE WEALTH PTY LTD REG NO 1997/009637/07 (FSP828), REGISTERED CREDIT PROVIDER THROUGH NEDBANK LTD REG NO 1951/000009/06 (NCRCP16), AND MEMBER OF JSE LTD THROUGH NEDGROUP PRIVATE WEALTH STOCKBROKERS PTY LTD REG NO 1996/015589/07, AN AUTHORISED FINANCIAL SERVICES PROVIDER (FSP50399) AND A REGISTERED CREDIT PROVIDER (NCRCP59).

PAGE 1 OF 4

2 How to protect yourself from fraud

Cybercriminals find it much easier to hack a human than to break through sophisticated security technology. This human hacking technique is called social engineering and is the art of manipulating or deceiving you into taking action or disclosing sensitive information using flattery, urgency, pressure, or greed.

Watch out for these common tactics and understand your role in preventing these attacks:

2.1 Phishing attacks

Phishing (hacking via email) is the most frequently used form of social engineering and everyone is a target.

Important tips

Check the sender's email address	Always **check the sender's details** carefully and ensure it's from the right domain, eg @nedbank.co.za or @nedbankprivatewealth.co.za.
Check spelling	Look out for **spelling errors**.
Approach links and attachments with caution	• **STOP, LOOK**, and **THINK** before clicking on a link or opening an attachment – always **hover your mouse** over links in an email to see where they will take you. • **Don't open attachments** if you don't recognise the sender or if you aren't expecting the email – these could contain malware or a virus. • **Never** enter and submit your credentials via a link.
Beware of urgent requests	• Be aware of emails or phone calls with a tremendous sense of **urgency** that demand your immediate action before something bad happens, for example threatening to close an account or send you to jail. The attacker wants to rush you into making a mistake. • Regard urgent security alerts, offers or deals as warning signs of a hacking attempt.
Trust your gut	If an email makes you feel anxious, fearful, curious or sounds too good to be true, rather **follow your gut, stop and verify** before clicking on anything.

2.2 Vishing attacks

Vishing is also known as **voice phishing** or **over-the-phone phishing**.

- Example 1: You get a call from someone pretending to be a representative from your bank claiming that your account has been locked due to fraudulent activity. They then ask you to 'Please verify your account number and PIN'.
- Example 2: You get a call from someone in IT who says they have picked up a virus or malware on your computer and they need you to 'Please verify your login details and password'.

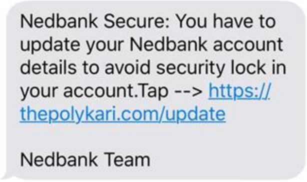
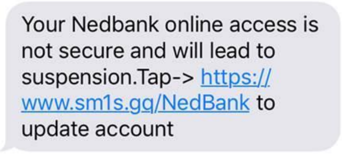
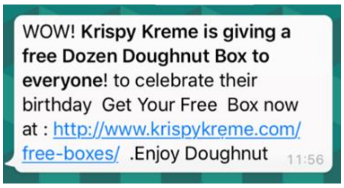
Important tips

Be aware of your emotions	Has the phone call made you feel panicked, fearful, worried, curious or flattered?
Never disclose sensitive information over the phone	If you get a phone call from someone asking for your banking, confidential or personal information, **do not respond** and end the call immediately.
Verify the caller	• Be very **suspicious** of anyone who asks you to share login information. • Always **verify** who you are speaking to. Don't assume someone is who they claim to be.

2.2 Smishing attacks

Smishing (short for SMS phishing) is **phishing via a text message** on your cellphone. Cybercriminals trick you into handing over personal information via a link in an SMS.

Important tips

Beware of an unknown source or number	**Never act** on any incoming texts messages that come from an unknown source or phone number.
Beware of urgent requests	Regard urgent security alerts and you-must-act-now offers or deals as **warning signs** of a hacking attempt.
Don’t click on links asking for your login credentials, PIN etc.	No financial institution or merchant will send you a text message asking you to update your account information or confirm your ATM card PIN, as shown below:  Nedbank Secure: You have to update your Nedbank account details to avoid security lock in your account.Tap --> https://thepolykari.com/update Nedbank Team  Your Nedbank online access is not secure and will lead to suspension.Tap-> https://www.sm1s.gq/NedBank to update account  WOW! **Krispy Kreme is giving a free Dozen Doughnut Box to everyone!** to celebrate their birthday Get Your Free Box now at : http://www.krispykreme.com/free-boxes/ .Enjoy Doughnut 11:56
Trust your gut	If a text message makes you **feel anxious** or **threatened** or **sounds too good to be true**, STOP, LOOK and THINK before clicking on any links.

The next time you feel anxious, worried, flattered or rushed by an email, a phone call, a text message or an interaction with a stranger, imagine a big red **STOP** sign and ask yourself: could this be a trick to hijack me and steal my personal or company information?

3 Tips for identifying fake news

Presume everything you receive is fake until you can prove that it is true

Interrogate content before you share it:

- What is the source? If there is no source, don’t share it. If it is a voice note, does the person identify themselves? Have you Googled the person?
- Is the source credible? Have you visited the social media pages of the alleged source?
- Does the link look legit? (For example, ‘CCN’ instead of ‘CNN’.)
- Does this content make you very happy, scared or angry? Red flag! Think about why the information might have been created and shared. Might it be political forces at work?
- Compare the information against that from trusted and official sources – are the main news sites covering the story?

4 How to protect yourself from fraud

4.1 General tips for parents

Communication	• Have an open discussion with your child about social media and other online platforms – the benefits and risks, what their friends are doing online, why they want to be online, and what they would do online. • Have regular check-ins and follow-up conversations**.**
General house rules	• No electronic devices in the bedroom after a set time every night. • No social media until high school. • Agree on a time budget with your child – how many hours a day on their device is reasonable. Set those time limits on the device. • Model good phone behaviour. • Establish media-free times and locations in your home.
Specific actions	• Help your child set up their social media accounts. Make sure that they have activated all privacy settings and do not include their date of birth. • Turn off location services on social media apps. • Set up some ground rules for sharing personal information. • Consider your child's privacy when posting photos of them. • Children must beware of anyone they don't know trying to join their network of friends – it's best to presume everyone they meet online is dodgy until proven otherwise. • Install filtering software on your WiFi connection at home. Turn off the WiFi at night. • Install tracking software. (Life 360 is free on most smartphones). • Remember the Billboard test (you shouldn't do or say anything that you wouldn't want printed on a billboard the next day).

4.2 Helpful resources for parents

General questions and research	https://www.commonsensemedia.org/
Parent guides Learn more about the websites, games and apps that your children are using.	• https://www.commonsensemedia.org/parents-ultimate-guides • https://www.bark.us/blog/streaming-sites-safety-kids/
How to set up a smartphone contract with your child	https://www.thedigitallawco.com/parents/smartphone-contract-teenagers/
How to install parental control software	For high-risk children: Bark, Qustodio or Our Pact Otherwise, the following are free and comprehensive: • **Google Family Link on Android:** https://www.thedigitallawco.com/smartphones/googles-family-link-app-everything-parents-need-to-know/ • **Screentime on Apple:** https://www.thedigitallawco.com/parents/apples-screen-time-app-everything-parents-need-to-know/
How to activate parental controls on YouTube Kids	• Log in to your child's profile. • Turn off **Allow searching**. This prevents your child from searching for content in the app. • Turn on **Approved content only**. • Click **Start** and then click the small **+** at the top right of each show to add channels or shows to the approved list. Preview the shows before adding them. Then click **Done**. • Turn on **Pause watch history** to prevent suggested videos showing. • Exit back to the login screen and then double-check the profile to ensure it is saved and set. See more at Common Sense Media's Ultimate Parent Guide to YouTube Kids: https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-youtube-kids
Documentary on the dangers of social media	Childhood 2.0: https://youtu.be/He3IJJhFy-I