Tips for staying safe online, so you can bank with confidence.

Create strong passwords

- ☐ **Long:** avoid short and predictable passwords
- ☐ **Diverse:** combine a mixture of letters, words and symbols for added security
- ☐ **Unique:** re-using a password multiple times makes it less secure, as it only takes one breach to compromise all accounts and websites with the same password. Avoid using anything that can be easily guessed, such as pet or family member names, birthdays, your address, common words/phrases
- ☐ **Secret:** keep it private and safe. Never share with anyone, even family or friends. Note: CommBank staff will never ask you for your NetBank password or Personal Identification Number (PIN)
- ☐ **Memorable:** try creating a passphrase, which is similar to a password, but instead uses words that tell a story. It should be easy to remember, while making it difficult to guess e.g. MyPetGo@tHa$@PhD

Extra tip: For an added layer of defence, consider two-factor authentication. This is a way to confirm your identity by requiring something additional to a password and username e.g. a code sent to your mobile phone. At CommBank, this takes the form of a NetCode SMS (for NetBank registered customers).

Things to look out for when shopping online

Before making your purchase, there are a few things to look for before you input your card details:

- Avoid websites without a padlock symbol and 'https' at the start 

- When you search for the website online – check to see if there are any negative reviews on the legitimacy of the website
- If the site you are accessing has an app available, we recommend accessing via the app
- Try to shop online with brands you know and trust.

Avoid suspicious links and attachments in email or SMS

- Hoax emails and SMS will appear to come from CommBank and may say 'unusual activity', 'suspended account' or 'verification required'. At CommBank, we won't send you links that take you directly to the NetBank logon page or that ask you to update or disclose your personal information
- Hoax emails and SMS will create a sense of urgency to act quickly
- Avoid opening emails or attachments from unknown senders.

Protect your device

- Keep your operating system, security software, web browser and add-ons up-to-date, by ensuring automatic updates are enabled or installed as soon as they are available. This dramatically reduces your device's exposure to malware
- When you are downloading and installing apps onto your phone or tablet, only install apps from the official stores (Apple's App Store or Google Play)
- Check the number of times a particular app has been downloaded to help ensure its legitimacy.

Common types of scams and what to look out for.

Phishing scams

Phishing attacks can take the form of emails, SMS, phone calls, or social media notifications, where scammers use links to fake webpages to get people to enter their personal details or passwords.

If you're a CommBank customer and you've received a suspicious email, you can help other customers by forwarding this to **hoax@cba.com.au** so we can take action against any fake sites.

If you think you may have accidentally given details to a phishing scam, please call us straight away on **13 2221**.

Investment scams

Investment scams occur when someone contacts you out of the blue, via phone or email, with a chance to invest in a 'once-in-a-lifetime opportunity'.

Examples include a cold call from a scammer pretending to be a stock broker, or an email from a money making opportunity that requires you to act quickly. The scammer often sounds legitimate and knowledgeable and will throw facts, figures and projections at you to make their investment seem too good to miss out on.

Romance scams

Romance scammers usually create fake online identities designed to quickly capture your attention and lure you in. Once they've gained your trust, often over several months, they use your newfound relationship to request you send them money or gifts.

They may ask you for money to fix a non-existent health, travel or family problem or convince you to transfer assets into their name – using manipulative, psychologically controlling and deceitful tactics to succeed.

Be aware, and talk to your friends and family – seek their opinion if someone you don't know is asking for money (even if you think you know them virtually).

Remote access scams

Remote access scamming occurs when targets are contacted via phone, text or email by a scammer falsely claiming to be from a familiar company, such as a bank, telco, software company or government agency. They'll often give a fake but credible story, to trick you into giving them remote access to your computer or device. This gives the scammer full access to your computer – and personal information – from a remote location.

Top tips to protect yourself.

- ☐ If you see a suspicious message, never click on a link or open an attachment. If you receive a request to make a payment or change account details, call to confirm with the person via a trusted number, like one from their official website
- ☐ When presented with an investment opportunity that seems too good to be true, talk to an investment advisor.

  It's always important you understand the risks associated with any investment. For independent information about investment choices you should visit ASIC's Moneysmart website, which has useful information on products such as term deposits, as well as tips on how to choose a financial advisor
- ☐ If someone you've never met before asks for money, think twice and ask more questions to determine if it's a scam
- ☐ If you receive a call you don't feel comfortable with, avoid providing any personal information and hang up. But if you accidentally give the caller any sensitive information, please contact us on **13 2221** immediately
- ☐ Check your accounts regularly so you can quickly identify and report any unrecognised transactions. Please call us on **13 2221** immediately if you notice a transaction you didn't make.

For more information visit:
commbank.com.au/security | **scamwatch.gov.au** | **staysmartonline.gov.au** | **moneysmart.gov.au**

Commonwealth Bank of Australia ABN 48 123 123 124.

ADV14907 280420