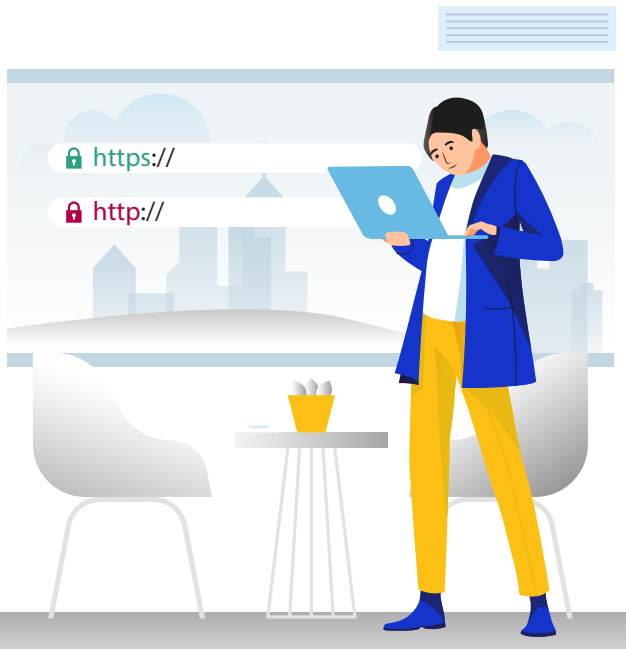
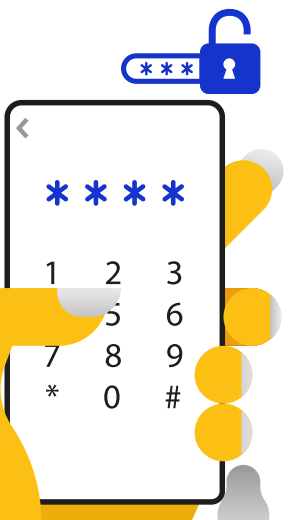
Shop at well-known eCommerce sites. Look out for the ‘s’ after ‘http’ in website addresses to confirm that a site offers SSL (Secure Sockets Layer) protection



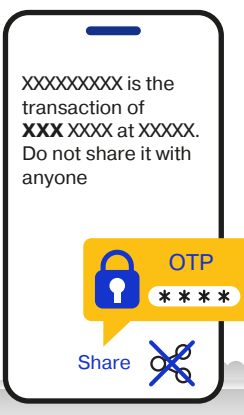
Don’t access your personal bank account or sensitive personal data on unsecured WiFi networks or public computers.

Update your passwords with a strong password unique to each account or switch to fingerprint or facial recognition where possible

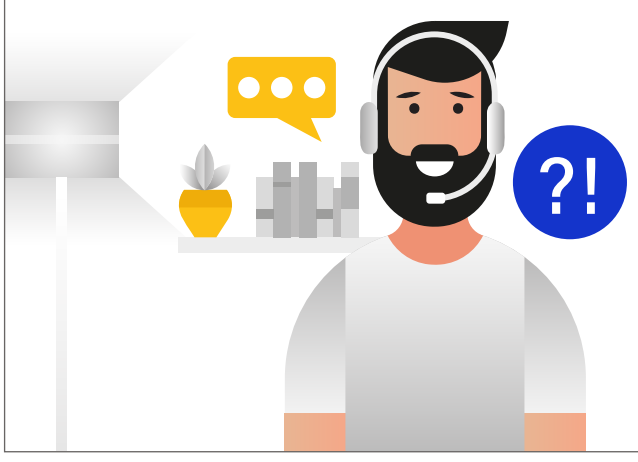
Never reuse passwords. Using a password manager will help you come up with unique passwords that will be hard to guess.
Never save passwords in your computer folder or on other devices



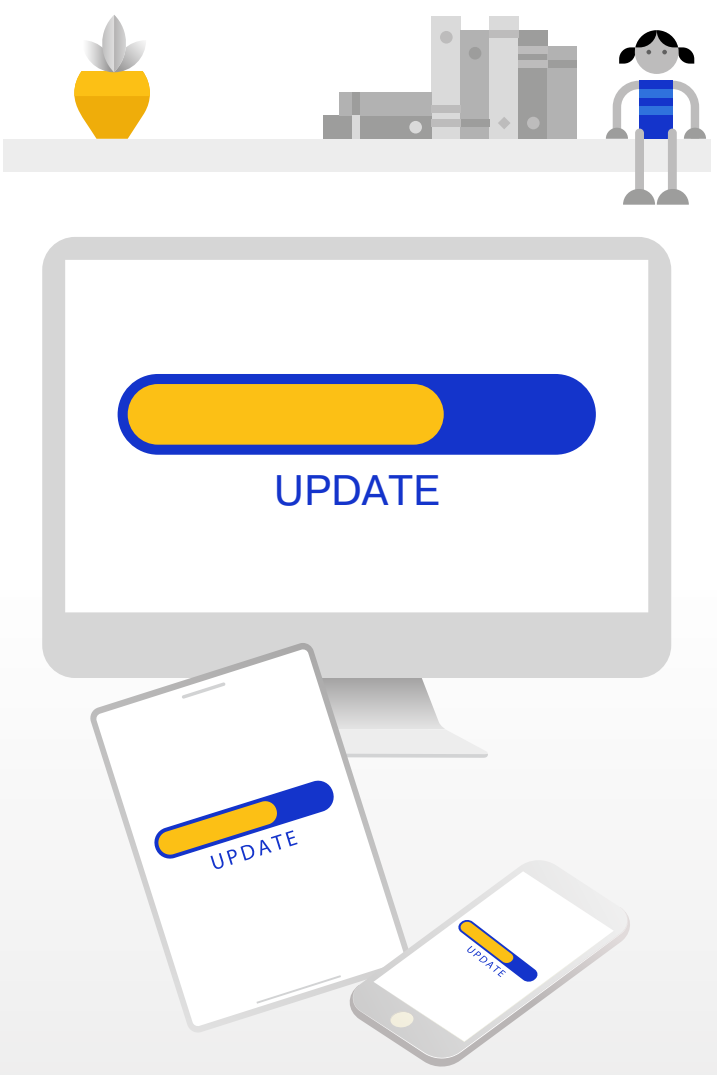
Do not share one-time passwords (OTPs) with anyone else – banks will never contact you to ask for an OTP that has been sent to your device



Never share personal account information on social media, over email, phone or chat.



Be wary of unsolicited and suspicious emails, SMS/text messages or phone calls. If in doubt, do not click on links or download files.



Make sure your phones and computers are updated with the latest software updates as they will help keep your data protected against cybercriminals.

Use a single credit card for all online transactions – this will make it easier to manage online transactions.

Sign up for transaction alerts – this will help you manage your online activity and see when your account has been used for a transaction.