Phriendly Phishing

Top tips to protect yourself with multi-factor authentication (MFA)

Keep your authentication devices safe

Use a password, PIN, fingerprint or face ID (biometrics) to access mobile authenticator apps to prevent unauthorised access.

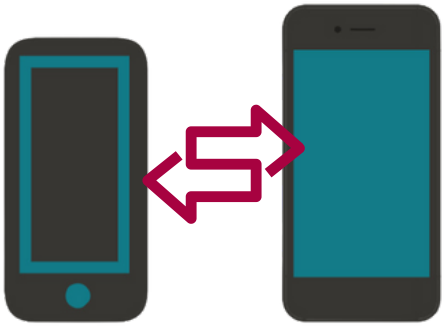
Safely store any security keys, access cards or tokens you use.

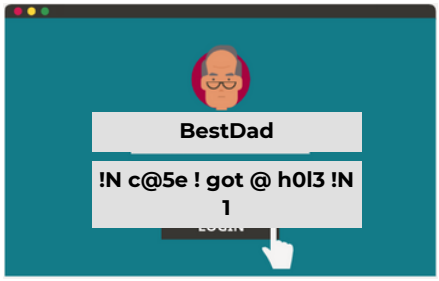
Don't share MFA codes

Never approve unknown sign-in attempts. Sign-in requests are the system's way of checking that you are the approved person for that account.

Transfer authentication apps

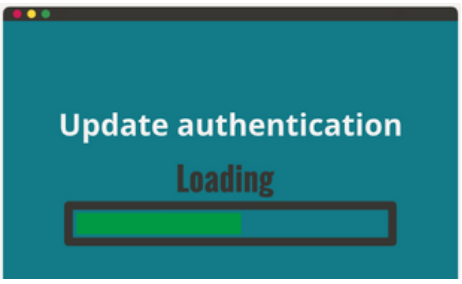
Remember to transfer any authentication apps when you change devices to maintain account access.





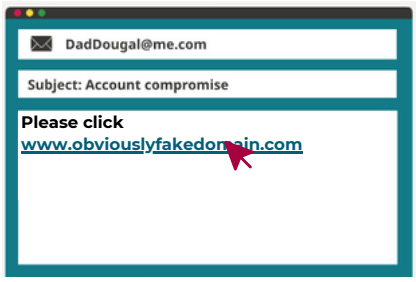
Create strong passwords and passphrases

A passphrase is more like a sentence and uses a mix of upper and lower case letters, numbers, special characters and spaces. Use a different password or passphrase for every account you have.



Secure your recovery accounts

In the case that you get locked out of your accounts, make sure that your recovery account is accessible and the most secure account that you have.



Be alert to sign-in links received via SMS or email

Always be suspicious of links in SMS and email. Scammers will try to trick you by sending you a fake sign-in link.

Keep your accounts safe by applying the tips to your cyber routine.