Phriendly Phishing

Protect Against a Data Breach

INVESTIGATE ACCOUNT CHANGES IMMEDIATELY

Threat actors sometimes seek to gain control of victims' phone numbers & accounts using compromised personal information. Notifications about changes to accounts, such as social media, email, & banking, may be a sign of threat actors gaining access to accounts.

These should be investigated as a priority by contacting service providers & taking steps to secure accounts.

BE HYPER VIGILANT ABOUT PHONE CALLS & SMS

Calls & SMS threats can be falsely displayed as an organisation, including government agencies, employers & carriers.

Read more on the CyberCX blog.

PRACTICE CYBER HYGIENE ONLINE

- Never respond to requests to provide personal & account information, or access to your device.
- Never click on any links that look suspicious or provide passwords, personal or financial information.
- Subscribe to www.scamwatch.gov.au for the latest information about scams impacting our community.

IF YOU EXPERIENCE ANY MISUSE OF YOUR CREDENTIALS, PLEASE CONTACT IDCARE FOR SUPPORT

Phriendly Phishing

Protect Against a Data Breach

REVIEW STOLEN INFO & CONSIDER GETTING NEW ID

Drivers license & Passport:

Scammers can gain access to your MyGov, ATO, financial accounts & social media. Download Passport Fact Sheet here. Check with your state for updates to your drivers license.

Medicare card:

Risks include unauthorised access to financial accounts & your Medicare account. View the change your card fact sheet.

Email address:

Beware of phishing emails, including those asking to update billing details or pay invoices.

MONITOR YOUR CREDIT REPORT TO IDENTIDY ANY SUSPICIOUS ACTIVITY

Apply for a free credit report once every 3 months or you can also pay to add a credit ban to your account.

IF YOU EXPERIENCE ANY MISUSE OF YOUR CREDENTIALS, PLEASE CONTACT IDCARE FOR SUPPORT