Phone scams impersonating government and businesses

13 August 2020

Dear ACSC Alert Service subscriber

What's happened?

The Australian Cyber Security Centre and Australian Competition and Consumer Commission's Scamwatch have received an increased number of reports in the last five days of remote access scams.

Members of the public have reported receiving calls from cybercriminals pretending to be from telecommunication companies, government agencies including the Department of Home Affairs and parcel delivery companies.

A majority of the calls have been reported by people living in areas that have been locked down due to the COVID-19 pandemic, suggesting cybercriminals may be preying on people who are more vulnerable, housebound and easy to contact.

Where victims have handed over personal details, the cybercriminals are then using legitimate remote access applications like Team Viewer or Zoho Assist, to gain access to people's devices. They then log into your bank account and online accounts, and steal your details for financial gain.

Does it affect me?

Cybercriminals are cold calling people, so anyone can receive one of these calls, regardless of whether you have any usual dealings with the legitimate business being impersonated.

How do I stay safe?

If you receive one of these calls, NEVER provide your personal and financial details or give a stranger remote access to your device or computer – simply hang up.

- If you've received one of these calls but have not engaged with the scammer, you can report it to Scamwatch.
- If the cybercriminal has accessed your device via Team Viewer or Zoho assist, you should report it to ReportCyber and **immediately** notify your bank, as they may be able to put a temporary freeze on your financial accounts.
- To prevent further compromise, you should also change passwords on all your important online accounts including banking, email and social media, and turn on two-factor authentication for extra security.

If you're in doubt about a call claiming to be from a government agency or Australian business, and want to verify its legitimacy, contact the organisation by sourcing their details directly from their website, NOT by using the phone number or other details from the incoming call.

More information

Many organisations have dedicated scam pages on their websites alerting the public to the latest scams.

To help you spot a scam, NBN is running webinars next week to support Scamwatch's Scams Awareness Week. You can register via their Facebook page at www.facebook.com/nbnaustralia.

The ACSC also recently launched an interactive quiz, to help Australians spot the warning signs of phishing (scam) messages. Make sure you share the quiz with your colleagues, family and friends, available at www.cyber.gov.au/scam-messages.

Read more about remote access and threat-based impersonation scams – including what to do if you have given personal information to a scammer.

CONTACT US

Facebook: www.facebook.com/staysmartonline
Email: staysmart.online@defence.gov.au
Web: www.cyber.gov.au