REVERSE THE THREAT

STAYSMARTONLINE WEEK 8–14 OCTOBER 2018

Know How to Spot Phishing or Fake Messages

Phishing is one of the most common forms of cybercrime. Think before you click to reverse the threat of cybercrime.

What is phishing?

Phishing is a way that cybercriminals try to steal your information — such as online banking logins, credit card details, business login details or account passwords — by sending fake messages.

These fake messages often pretend to be from a large organisation you trust and can be sent via email, SMS, instant messaging or social media platforms. They often contain a link to a fake website where you are encouraged to enter your personal details.

Because of phishing, many companies now have a policy that they will not call or email to ask you to update or verify your personal details, such as passwords, PINs, credit card information or account details. They will not call you out of the blue to request payment over the phone (for example, for a fine, bank transfer or undeliverable mail item).

$50 MILLION
lost to online-based **scams in 2017***

* Australian Competition and Consumer Commission, Targeting scams: report of the ACCC on scam activity (2017)

How to protect yourself from phishing

- Be wary — don't click on links in unexpected emails or in messages from people or organisations you don't know
- Be especially cautious if messages seem too good to be true or threaten you to make you take a suggested action
- If a message seems suspicious, contact the person or business to check if they are likely to have sent the message. Make sure you use contact details you find through a legitimate source and not those contained in the suspicious message
- Before you click a link, hover the mouse over that link to see the actual web address it will take you to
- Be particularly cautious of links shortened using URL shortening services — like **bit.ly** or **tinyurl.com** — that can hide the real destination of a link
- Use a spam filter to block deceptive messages from even reaching you.

What to do if you've revealed your personal information

- If you think you've entered your credit card or account details into a phishing site, contact your financial institution immediately
- Report scams to Scamwatch, which is run by the Australian Competition and Consumer Commission, to **scamwatch.gov.au/report-a-scam**
- If you think you've been the victim of identity theft, act quickly. For advice contact iDcare on **1300 432 273** or use their free Cyber First Aid Kit on their website **idcare.org** to help you work out what to do.

For more information on how to reverse the threat of cybercrime and Stay Smart Online, please visit:
staysmartonline.gov.au/reversethethreat

Follow us on Facebook
fb.com/staysmartonline

Sign up to our free alerts
staysmartonline.gov.au/alert-service