RMIT UNIVERSITY

How to…
Avoid getting scammed

Top ten tips from the RMIT Chief Information Security Officer (CISO) to minimise your exposure to cyber scams

Australians lost more than $4.7m to reported threat-based impersonation scams in 2017. If you receive an unexpected request for money or personal information, double check the credibility of the request, even if it appears to be from a reputable source.

1. Always question unexpected messages from government agencies or trusted businesses. It could be a scam.
2. Don't be pressured by a threatening caller. Hang up and check the legitimacy of the call through an online search or directory assistance.
3. Never send money, share bank details or other personal information to people you don't know or trust.
4. Don't open suspicious texts, pop-up windows or emails and don't click on links or open attachments. When in doubt, take a screenshot as a record and delete them.
5. Never share your password or login, even if it's just temporary. Your personal and RMIT login provides others with access to valuable information and the RMIT network.
6. Never give anyone remote access to your computer if they have contacted you out of the blue, even if they claim to be from a trusted company
7. Help your friends and family by sharing attempted scams. Not everyone will recognize the same scams. As scammers are often based abroad, they can be difficult to stop.
8. Beware of messages that convey a sense of urgency or use scare tactics. Inducing panic and fear can be used to sway your rational thinking.
9. If it seems too good to be true, it probably is! Social media is full of fake competitions and giveaways hoping to collect your personal information. Liking or sharing these posts passes this risk onto your friends and family.
10. Your personal details are difficult to un-share and can be used to steal your identity. Review your social media privacy settings and think twice about what you share online.

If you have given your information to a suspected scammer visit IDCARE **www.idcare.org**, Australia's not-for-profit national identity and cyber support service.

Keep up to date with the latest scams. Subscribe to:
www.staysmartonline.gov.au/alert-service