CyberCX

Security advice for individuals following Optus data breach

TLP: GREEN

Threat actors target Australians through mobile phones to access information and gain access to other systems, including victims' organisations. Threat actors are highly likely to be in possession of personal information from telecommunications provider Optus. This data is likely to increase threat actors' capability to conduct more targeted and sophisticated attacks, via phone, SMS, email or identity theft increasing the risk to individuals and Australian organisations. CyberCX Intelligence is providing the following advice for avoiding phone-based attacks based on known threat actor capabilities and behaviours:

- **Do not trust the caller or sender ID displayed by your phone.**
  - Threat actors can spoof the originating phone number for text messages. This may include threat actors being falsely displayed as an organisation, including government agencies, employers and carriers.
- **Do not trust someone because they have some of your personal information.**
  - Threat actors will commonly seek to obtain some personal information on targets before engaging with them and provide that information to gain trust. Details like name, date of birth and address may be exposed through data breaches and are much less reliable than details like recent account activity, including payments.
- **Never give two-factor authentication (2FA) permissions to a third party.**
  - Threat actors are highly likely to target individuals through their phone in order to overcome 2FA such as SMS verification codes. Threat actors commonly engage in social engineering to trick targets into providing a one-time passcode or authorising a push notification. You should never be asked to provide 2FA to a third party over the phone to authorise actions on your behalf such as banking, or IT support. Seeking alternative to SMS based 2FA is a further precaution to investigate with high-importance providers such as banks.
- **If in doubt, terminate and re-establish the correspondence through a different means.**
  - Terminating suspicious phone calls from an organisation and then calling back through a publicly listed number is a good way of avoiding scams. Actual representatives of organisations will understand this approach and should encourage you to confirm their identity.
- **Investigate account change notifications as a priority.**
  - Threat actors sometimes seek to gain control of victims' phone numbers and accounts using compromised personal information. Notifications about changes to accounts, such as social media, email, and banking, may be a sign of threat actors gaining access to accounts. These should be investigated as a priority by contacting service providers and taking steps to secure accounts.