Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Detecting Socially Engineered Messages

JANUARY 2019

Introduction

Socially engineered messages present a significant threat to individuals and organisations due to their ability to assist an adversary with compromising accounts, devices, systems or sensitive information. This document offers guidance on identifying socially engineered messages delivered by email, SMS, instant messaging or other direct messaging services offered by social media applications.

What are socially engineered messages?

Socially engineered messages are messages sent by an adversary in an attempt to direct users into performing specific actions such as opening an attachment, visiting a website, revealing account credentials, providing sensitive information or transferring money. To increase the likelihood of users performing an adversary's desired actions, the adversary will go to lengths to make their messages appear as if they are legitimate and from a trustworthy source. As a result, socially engineered messages are likely to be work-related, infer a sense of urgency or target a specific interest of users. They may also appear to come from someone known to users such as a colleague, senior manager or authoritative part of their organisation (e.g. the information technology, human resources or finance areas).

Who do socially engineered messages target?

While socially engineered messages can be received by anyone, an adversary often prioritises the targeting of certain users due to either their profile, access to sensitive information, ability to make changes to systems, authority to undertake risky business activities (such as transferring large sums of money) or their job's requirement to routinely interact with unfamiliar people. Broadly, this can include:

- high profile individuals[1]
- senior managers and their staff
- system administrators
- staff members from human resources, sales, marketing, finance and legal areas[2].

It should be emphasised that other users should not consider themselves immune to receiving socially engineered messages. An adversary may message as many users as possible hoping that at least one message will be successful.

[1] https://securingtomorrow.mcafee.com/mcafee-labs/twitter-accounts-of-us-media-under-attack-by-large-campaign/
[2] https://www.csoonline.com/article/3225469/security/office-365-phishing-attacks-create-a-sustained-insider-nightmare-for-it.html

How can socially engineered messages be identified?

While socially engineered messages can be very convincing, there are things to look for to assist in differentiating them from legitimate messages. Users should consider the following questions.

Is the sender asking you to open an attachment or access a website?

When messages contain links to websites, users should browse to the website themselves rather than clicking on the link in the message or directly copying or typing the link into a web browser. An adversary can use a number of techniques (such as single letter substitutions) to either obfuscate or trick users into accessing a malicious website that they think is legitimate. Never enter credentials into websites if directed there by a link in a message[3].

When opening attachments from messages, users should be cautious and exercise judgment. If unsure, use a known out-of-band contact method for the sender (e.g. a phone number) to confirm their intent to attach files to the message.

Is the sender asking you to perform a specific activity for them?

Often an adversary will be unable to achieve their goals without interacting with users. This may be due to existing security controls or the complex nature in which an adversary is attempting to compromise a system. For example, if Microsoft Office macros are disabled an adversary may provide users with step-by-step instructions on how to enable them in order for their malicious code to execute when the user opens a Microsoft Word document. Users should treat any requests to change the configuration of systems or perform specific actions as highly suspicious.

Alternatively, a form of social engineering known as CEO fraud involves an adversary masquerading as an organisation's CEO and requesting large transfers of money, often when they know the actual CEO will be uncontactable and unable to refute the request[4].

Is the sending asking for information they wouldn't necessarily have a need to know?

One of the easiest ways of performing social engineering is for an adversary to simply ask users for the information they want by exploiting user's natural desire to be helpful. Often an adversary will masquerade as someone users might expect to have a legitimate requirement to access the information being asked for. For example, a colleague asking for copies of documents that they accidentally deleted. Alternatively, an adversary may choose to masquerade as someone that users may not necessarily know but could be reasonably expected to have a requirement to access the information they are requesting, such as a new starter with the information technology help desk or a staff member working on the same project but from a different office.

Users should never disclose credentials such as passwords to other people. Furthermore, users should be suspicious of any requests for sensitive information from people that they do not interact with on a regular basis. Even if users know the person requesting sensitive information, they should still consider whether that person has a legitimate need to know that information, as malicious insiders often leverage their contacts in order to gather information or privileges they shouldn't have access to[5].

[3] https://www.express.co.uk/life-style/science-technology/755409/gmail-phishing-scam-fake-email-login-hack
[4] https://www.cso.com.au/article/600535/ceo-fired-after-fake-ceo-email-scam-cost-firm-47m/
[5] https://www.reuters.com/article/net-us-usa-security-snowden/exclusive-snowden-persuaded-other-nsa-workers-to-give-up-passwords-sources-idUSBRE9A703020131108

Is the message suspiciously written?

While an adversary may go to lengths to make their messages appear as if they were legitimate and from a relevant and trustworthy source, another adversary may lack the skills or motivation to do so. Incorrect spelling and capitalisation, abnormal tone and language, or the absence of a specific addressee can indicate that a message is likely to be a socially engineered message.

How should socially engineered messages be handled?

If you suspect that you've received a socially engineered message, do not delete or forward it. Contact your organisation's information technology help desk or security team and seek advice on how to proceed.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).