U.S. Department of State
Overseas Security Advisory Council

Social Engineering: Threats & Best Practices

October 2015

QUICK GUIDE: SOCIAL ENGINEERING

Social engineering exploits weakness in people, rather than those found in technology. Malicious actors prey on human relationships, commonly manipulating personal or professional information relating to the victim to disguise their intent. This method tricks victims into believing the communication is legitimate, and often into providing more information and access. It has been a longstanding tool of con artists, identity thieves and spammers.

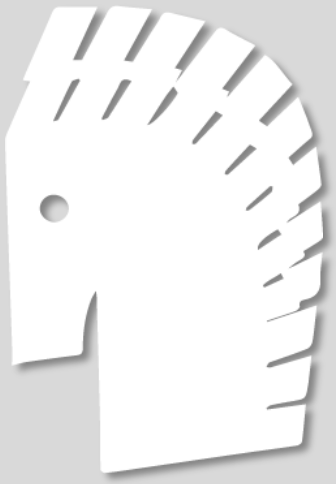
Information-Gathering Tactics:

- Shoulder Surfing
- Dumpster Diving
- Lobby Loitering
- Vishing
- Social media profiles
- Web searches

The Trojan Horse: Then & Now

The Trojan Horse is a classic example of social engineering. Following a decade of failed attempts to conquer Troy, the Greek army appeared to give up and go home. As a concession gift, they left the Trojans with an oversized wooden statue of a horse. A small battalion of Greek soldiers stowed away inside the horse and waited for the Trojans to celebrate their assumed victory. Then, the Greeks attacked and destroyed Troy from within the city walls.

A Trojan Horse in the cyber realm operates by similar principals. Malicious programs are disguised as routine system updates or new games to entice users into downloading and opening them. Trojans deviously carry out their malicious tasks in the background as users carry on with business as usual.



SOCIAL ENGINEERING ONLINE

Much like the traditional forms, social engineering online looks to exploit a user's interests, curiosity, and/or fear. But the online platform enables criminals and other threat actors to access personal and sensitive information much easier and cheaper than before – all they need is access to a computer. Malicious online actors are looking to gain unauthorized access to information systems to commit fraud, network intrusions, commercial espionage, identity theft, or to disrupt and destroy system functions. Social engineering is the entry-point to execute any number of these tasks.

Socially engineered e-mails may appear to come from:

- Colleagues
- Business contacts
- Event coordinators
- Official organizations
- Banks
- News Sources

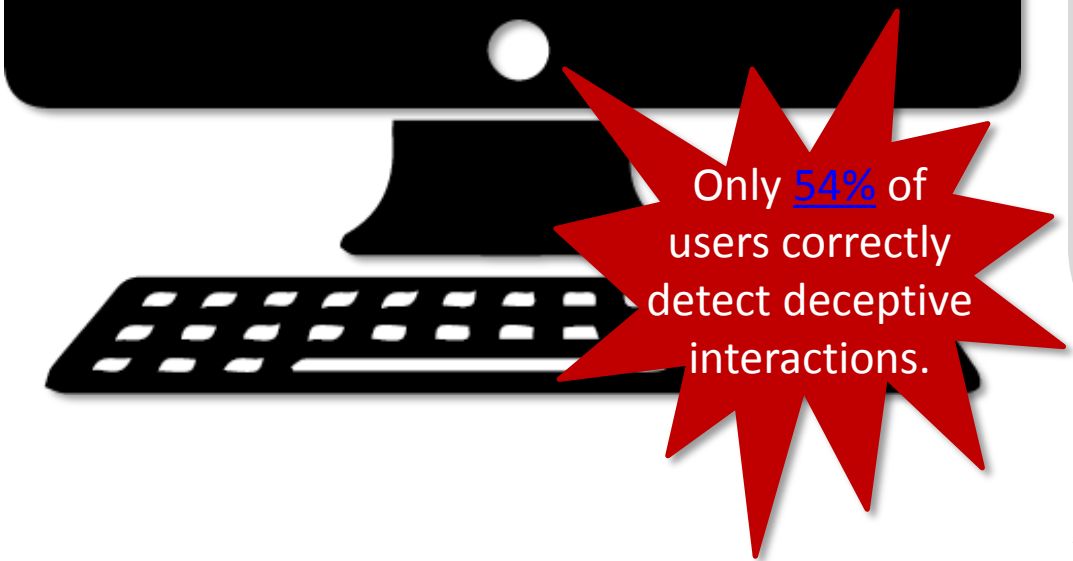
Socially engineered e-mails may reference:

- Work projects
- Conferences
- News headlines
- Major events
- Political elections
- Natural disasters

SOCIAL ENGINEERING ONLINE

Common Online Social Engineering Tricks:

- Fake antivirus & software upgrades
- Spoofed legitimate webpages
- Impersonated email contacts
- Fake social media personas
- Shortened URLs posted to social media forums
- Decoy file-sharing sites



Case Study: The Newscaster Campaign

For three years, Iranian hackers created and maintained an elaborate muse of false media personas. These personas were substantiated with social media profiles and a fake news website. The objective was to connect with targets in the defense, diplomatic, and nonproliferation fields and collect strategic intelligence. The hackers took their time making connections and feigning legitimacy, making the social engineering aspect resourceful and effective. The operation consisted of:

- The false "NewsOnAir.org" website with military and diplomatic content
- 14 associated LinkedIn, Twitter, & Facebook accounts with over 2000 professional connections
- Targeting of connections with spear phishing

"Newscaster" highlighted the ability of malicious actors to leverage social networks and create a convincing backstory for targets.

CHECK YOUR PRIVACY SETTINGS

Experts say serious hackers use the masses of personal information people share about themselves online to their benefit, primarily relying on social media forums. This trove of information allows threat actors to create persistent social threat – an ongoing relationship with their target that carries beyond initial interaction and can be repeatedly used in the future.

How unsecure social media profiles facilitate tailored targeting:

- Shows personal and professional interests
- Access to contacts for impersonation and/or additional exploitation
- Displays personal and work emails for targeting
- Physical location tracking

SOCIAL ENGINEERING ONLINE

CUSTOM MADE: FOR VICTIMS

Verify the identities of contacts

In a study of malware targeting Syrian oppositionists, private cybersecurity firm FireEye found threat actors exploited the power of lust. The actors created female avatars on Skype to establish relationships with male oppositionists and conversations were shaped to gather intelligence on the men. The victims were also asked if they used the Skype chat function on their computers or mobile devices, and their answer enabled the threat actors to tailor malware specifically to the victim's device. The remote access tool that gave the threat actors full control of the victim's device was delivered via photos of the fictitious women.

Separately, FireEye also reported on the revamped Nigerian scam. With evolved methodology, Nigerian hackers began preying on employees who were not native English speakers to decrease the likelihood that their fraudulent English-language emails would be detected. The hackers were able to intercept communications, provide false payment details, evade detection and steal millions of dollars.

CHECKLIST: SOCIAL ENGINEERING DETECTION

- ❑ **Scrutinize** email sender addresses.
- ❑ **Verify** the identities of contacts.
- ❑ **Never** share passwords.
- ❑ **Don't** click suspicious links.
- ❑ **Don't** open suspicious attachments.
- ❑ Be **wary** of "urgent" requests.
- ❑ Know **why** information is being requested of you.
- ❑ **Flag** suspicious emails for IT inspection.
- ❑ Pay **attention** to website URLs – look for the lock symbol and "https" to indicate a secure connection.
- ❑ **Never** enter your password on unverified websites.
- ❑ **Secure** social media profiles with strict privacy settings.
- ❑ **Maintain** employee awareness programs.
- ❑ **Always** keep anti-virus and other system defenses updated.