Protecting your organization against social engineering

CANADIAN CENTRE FOR CYBER SECURITY
October 2023 | ITSAP.00.166

Social engineering attacks occur when a threat actor uses social connection and manipulation to pressure or trick users into doing something that is against the best interest of your organization (like providing sensitive details, passwords, or financial information). Threat actors often impersonate a known person, a reputable organization or vendor, or even a government employee. They may try to influence users into doing something which gives them access to your environment, such as changing an account password. With this information , threat actors can steal your organization's business and financial information, access user accounts, and potentially deploy malware. Anyone can be a target of a social engineering attack, from an individual employee to the CEO of your organization. Knowing how to identify and safeguard your employees from social engineering attacks is crucial in protecting your organization's network, systems, and data.

How does social engineering work?

Social engineering attacks are also referred to as "human hacking" since threat actors leverage information they've found on the Internet and social media platforms to target individuals and organizations. Threat actors use this information as bait to lure or trick users into disclosing information about their accounts, passwords, and even system access within your organization. Threat actors use psychological techniques to evoke an emotional response to pressure users into completing a task or use attention grabbing titles to get users to click on malicious links.

Examples of social engineering attacks

- **Phishing** is a tactic threat actors use where a message that appears to be from a trusted source is sent to a large number of recipients. The message may ask recipients to provide sensitive information, complete an action (like change a personal or network password) or click on a link which looks legitimate but is actually malicious. For more information, consult Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101).
- **Spear phishing** is a phishing attack sent to a select group of individuals or a single person which includes details that are tailored to be more convincing and make the source appear more legitimate.
- **Whaling** is a phishing attack that targets a high-level employee such as a CEO or CFO.
- **Smishing** is a phishing attack sent through short message system (SMS) or text message.
- **Quishing** occurs when a phishing attack includes a quick response (QR) code that takes you to a malicious website when scanned. For more information, consult Security considerations for QR codes (ITSAP.00.141).
- **Vishing** is a phishing attack through voicemail or voice call on a landline, cell phone, or voice over Internet protocol (VoIP). Threat actors may use a spoofed phone number or alter their voice to disguise their identity. Threat actors may also utilize artificial intelligence (AI) to disguise themselves or imitate someone you know. For more information, consult What is voice phishing? (ITSAP.00.102).
- **Baiting** is a social engineering attack that occurs when a threat actor convinces you to take an action (like clicking on a malicious link) by promising you something appealing like a prize.
- **Quid pro quo** is a social engineering attack where a threat actor convinces you to give up sensitive information about you or your organization or preform a task (like clicking on a malicious link) in exchange for the promise of a service in return.
- **Honey traps** occur in social engineering attacks where a threat actor engages you in a fake romantic relationship online in order to get money or sensitive information from you.
- **Scareware** is a type of social engineering attack where a threat actor convinces you that your computer or network is at risk in hopes that you will take certain actions (like clicking on a malicious link).

Watch out for unsolicited communications with:

- attachments
- hidden links
- spoofed websites
- malicious QR codes
- login pages
- urgent requests
- threatening or urgent language
- prompts for personal or sensitive information
- callers who claim to be government officials or bank representatives

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Social engineering lifecycle

Threat actors typically follow a similar pattern when executing social engineering attacks. Knowing and understanding the actions a threat actor takes within this pattern can help you educate your employees and protect your organization.

The diagram below demonstrates the phases of a social engineering attack and the main actions a threat actor might take within each phase.

1.The bait

Threat actors research your organization and employees, then target them with an attack that appears to come from a trusted source. Information posted on social media sites, like Facebook, TikTok, LinkedIn, or Instagram, can be leveraged by threat actors to enhance the rouse that they know their target. The knowledge they have makes them seem more trustworthy and authentic.

2.The hook

Using social connection, sympathy, imposed urgency, threats, or a disarming tone a threat actor hooks the victim into their scheme. Users believe the scenario or request presented is real and that the threat actor is authentic.

3.The attack

Users are tricked into giving up sensitive information about themselves or your organization by clicking on a malicious link, changing passwords that give a threat actor access to accounts and networks, or opening a malicious attachment. This provides the threat actor with the key to unlock and steal your information.

4.The escape

Once a threat actor has convinced the user to complete a task, or has the information they want, they will disappear. They may also use scare tactics to silence their victim.

What can you do to protect your organization?

Social engineering attacks can be harmful to your organization. It can also disrupt your operations if your IT environment is compromised. The following list of action items can help you protect your organization:

- Use multi-factor authentication (MFA) on all systems and accounts. For more information, consult Steps for effectively deploying multi-factor authentication (ITSAP.00.105).
- Train your employees so they know what to do if they encounter a suspected social engineering attack. For more information, consult Offer tailored cyber security training to your employees (ITSAP.10.093).
- Contact the sender directly to verify the legitimacy of unsolicited messages. Generally financial institutions and government agencies will not call, text or email to ask a client to change or disclose sensitive information.
- Verify links before clicking on them by hovering over the link to see the sender or website details.
- Report suspected attacks to your IT team or management immediately.
- Limit the information posted to personal and professional social media accounts. For more information, consult Use of personal social media in the workplace (ITSAP.00.066).
- Filter spam emails and remove embedded macros. For more information, consult Spotting malicious email messages (ITSAP.00.100) and How to protect your organization from malicious macros (ITSAP.00.200).
- Implement allow lists or block IP addresses, domain names, and file types that you know to be malicious. For more information, consult Application allow list (ITSAP.10.095) and Protective Domain Name Systems (ITSAP.40.019).
- Install security tools like antivirus, antimalware, and anti phishing software, as well as firewalls, from trusted vendors. For more information, consult Preventative security tools (ITSAP.00.058).
- Activate automatic updates and patches for security tools and operating systems on your devices. For more information, consult How updates secure your device (ITSAP.10.096).
- Develop and implement an incident response plan that covers cyber incidents, including social engineering attacks. For more information, consult Developing your incident response plan (ITSAP.40.003).
- Back up information offline to ensure your backup is disconnected from your systems and network. For more information, consult Tips for backing up your information (ITSAP.40.002).

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada