certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0076

Preventing Social Engineering Attacks

Original Issue Date: December 13, 2016

Description

Social engineering is defined as the art of influencing people to disclose information and getting them to act inappropriately. Some perpetrators consider it much easier to abuse a person's trust than to use technical means to hack into a secured computer system: they have learned how to trick their targets into giving them information by exploiting certain qualities in human nature. They use variety of communication, such as email, the internet, and the telephone, to perpetrate their scheme of defrauding and infiltrating companies to access sensitive information.

Security experts recognize that most scams follow a four-stage method:
(a) information gathering
(b) relationship development
(c) exploitation and
(d) execution

This methodology, along with the tendency for humans to be the weakest link in the security chain, creates a vulnerability that can have a serious operational impact. The social engineering strategies used by social engineers fall into the following basic categories:

Phishing/spamming/spear-phishing:

Phishing can take the form of an email from someone claiming to be in a position of authority who asks for confidential information, such as a password. Phishing can also include sending emails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.

IVR/Phone phishing (aka Vishing):

This technical tactic involves using an interactive voice response (IVR) system to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to "verify" confidential information. They have a number of techniques at their disposal. The perpetrators already have your name, address, phone number, bank details - essentially the kind of information you would expect a genuine caller to have and you are made to believe your money is in danger and have to act quickly.

Impersonation/pretexting:

This common form of deception may involve an attacker using a believable reason to impersonate a person in authority, a colleague, or vendor in order to gather confidential or other sensitive information. Unlike phishing emails, pretexting attacks rely on building a false sense of trust with the victim. The attacker first has to build a credible story that leaves little room for doubt on the part of their target.

Trash cover/forensic recovery:

Attackers collect information from discarded materials such as old computer equipment (e.g., hard drives, pen drives, DVD, CD) and corporate documents that were not disposed off securely.

Baiting:

A common method of baiting involves offering something enticing to an end user, in exchange for login information or private data. The "bait" comes in many forms, both digital, such as a movie download on a peer-to-peer site, and physical, such as a pen drive that is left out on a desk for an end user to find. The user, then out of curiosity will plug/load the infected device into his or her computer.

Quid pro quo ("give and take"):

An attacker makes random calls and offers his or her targets a gift or benefit in exchange for a specific action or piece of information with the goal of rendering some form of assistance so that the target will feel obligated in some way.

Tailgating (Piggybacking):

Attackers gain unauthorized access to company premises by following closely behind an employee entering a facility or by presenting themselves as someone who has business with the company. The attacker may state that he or she left security credentials inside the facility or at home if challenged by an employee while entering the facility.

Best practices for users & organizations

There are a number of steps users and organizations can take to protect themselves from this increasingly popular form of threat.

- Do not ever give personal information like banking or credit cards over the phone. Do not post any personal information in social media. Although some of these information may seem harmless, they actually may provide rich pickings for attackers.
- Lock down privacy settings on social media accounts. Make sure you're making information available only to those you wish to have it.
- Use the right software and hardware systems. Every piece of software you put on your computer has potential vulnerabilities, the more you have, the greater your surface of attack is on a particular machine.
- Equip yourself with antivirus, anti-malware, and anti-exploit security programs. No antivirus solution can defend against every threat that seeks to jeopardize users' information, but they can help protect against some.
- Lock your laptop whenever you are away from your workstation.
- Never provide confidential information or, even non-confidential data and credentials via email, phone or in-person to unknown or suspicious sources.
- Conduct a data classification assessment, identifying which employees have access to what types and levels of sensitive company information. Know who the primary targets of a social engineering scheme are likely to be.
- Never release confidential or sensitive information to strangers or anyone who doesn't have a valid reason for having it, even if the person identifies himself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out over the phone or by email.
- Reduce the reliance on email for all financial transactions. If email must be used, establish call-back procedures to clients and vendors for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.
- Avoid using unauthenticated pen/flash drives or software on a computer or network.
- Be suspicious of unsolicited emails and only open ones from trusted sources. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.
- If you receive an email with a link to an unknown site, avoid the instinct to click it immediately even if it seems to have been sent from one of your contacts. Take a look at the URL to see if it looks suspicious. Often the email might seem to have arrived from one of your contacts but if you check the email address you will see that it is not legitimate.
- Physical documents and other tangible material, such as computer hardware and software, should be shredded and/or destroyed prior to disposal in any onsite receptacles, such as dumpsters.
- Proactively combat information security complacency in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis. This includes developing an incident reporting and tracking program to catalog incidents of social engineering and implementing an incident-response strategy.
- Guard against unauthorized physical access by maintaining strict policies on displaying security badges and other credentials and making sure all guests are escorted. Politely refuse entry to anyone "tailgating." Keep sensitive areas such as server rooms, phone closets, mailrooms and executive offices secured at all times.
- Monitor the use of social media outlets, open sources and online commercial information to prevent sensitive information from being posted on the Internet.
- Website administrators should check their website regularly to look for private and confidential information that could have been uploaded mistakenly.

References

https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972
http://www.securitymagazine.com/articles/87523-ways-to-thwart-social-engineering-attacks

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India