Social Engineering

What Is Social Engineering?

Social engineering, or the “con game,” is the art of manipulating end users into providing confidential or personal information. Below are the different types:

Phishing:
Hackers pretend to be trusted organizations such as banks, company suppliers, IT staff, or mobile carriers, in order to get your personal information, such as credit card details or confidential corporate information.

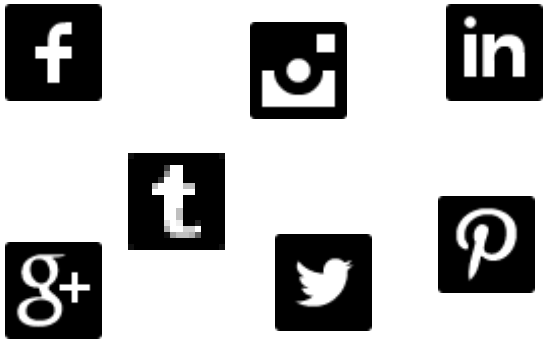
Piggybacking/Tailgating:
This is when an unauthorized hacker physically follows an authorized employee into a restricted area (e.g. pass through locked doors) or uses their computer to access locked IT systems.

What Is Social Engineering?

Pretexting:
Hackers impersonate other trusted figures within an organization to gain your trust and manipulate you into providing personal/confidential information.

Pharming:
Hackers re-create websites that look identical to the original but instead contain malware and/or key loggers to gain your personal information. The website URL will look very similar, although it may have a slight typo or a slightly different domain name.

Social Media:
An upcoming form of social engineering is through social media. Similar to phishing, hackers will act as a trusted organization or friend and try to obtain your personal information through messages, or get you to click malicious links through posts.



How Does It Affect You?

63% of data breaches come from internal sources.[1]

Social engineering can affect you in many ways:

1. If hackers are able to get your credentials, they can:
    a. Impersonate you when performing criminal acts (e.g. steal corporate information, spam others, perform DDOS attacks, share illegal files).
    b. Use your credentials to hack your company and network.
2. Hackers aim to get your personal information (name, social insurance number, credit card information, etc.), giving them the ability to steal your identity.

600,000 Facebook accounts are compromised every single day.[2]

1. Peterson, 2016. 2. Zaharia, 2016.

How Does It Affect Your Organization?

Successful social engineering attacks give hackers:

- Access to physically restricted areas and locked IT systems, allowing them to install malware and viruses.
- Ability to control devices and files within the organization's network. They can then send out confidential data or spam other organizations via email.
- Authority to manage, transfer, and steal your organization's assets, both physical and monetary.

90% of data breaches could have been prevented.[2] Understand how on the next slides.

1. Ponemon Institute, 2016. 2. Peterson, 2016.

A Hacker's Common Practices

Phishing	Pose as a trusted organization (bank, mobile carrier, insurance agency, supplier, government, etc.). They try to scare you and create panic, usually by claiming your account has been hacked, your account is locked, or your account is about to expire, etc. This is followed with an immediate action such as clicking a link or telling them your account details. Refer to the phishing training materials for more specific information on how to detect phishing.
Piggybacking	Tell you they forgot their key card/password and ask for your help. Dress up in official uniform such as a delivery man or electrician to pass through security. They may walk in with their hands full (usually coffee) and ask for help to gain access to the building. Tell you they have been locked out of their computer or forgot their laptop and ask if they can borrow yours. Wait near an entrance and simply follow someone into the office who holds the door for them.
Pretexting	Claim to be an authority figure like an auditor or your IT manager and ask for your information in order to complete a task. They can also be outside your organization and pose as a lawyer or other trusted occupation to gain your trust and ultimately your personal information. Hackers may even try to befriend you outside of work to get your personal information or they may claim to be an employee so you will trust them and let them in the building.
Pharming	Hackers will use identical URLs with a different suffix such as .net instead of .com. They will also create a website with a minor typo such as infotirch.com instead of infotech.com because the "e" and "r" are next to each other on the keyboard so it is easy to make that mistake. They will have the website functioning and looking legitimate. They can also replace certain links in emails or online to redirect you to their fake site without you knowing.
Social Media	Click bait is the most common way to get users to click on malicious links. Click bait are stories that are very interesting, trending topics, or controversial posts that entice you to click on the link to "read more" about the article. Posts can also be too good to be true to get people to click on them, such as "go to this website and get $1,000 today." Hackers can contact you through messages using social media and use phishing or pretexting methods.

Be Proactive

The best ways to avoid becoming a victim:

- ❑ Always ask for a person's credentials before letting them into a restricted area. If possible, swipe their credentials on the keypad for verification.
- ❑ Be suspicious of any email, text, or call asking for personal information. Most trusted organizations don't ask for personal information through those means. Look out for any communications that create a false sense of urgency and check links before opening them.
- ❑ Don't be afraid to ask questions or report suspicious behavior. It's better to be safe than sorry.
- ❑ Always pay attention to URLs; look for typos, the suffix (.com, .net, .co, etc.), and https (most trusted organizations use https).
- ❑ Don't let anyone use your login or credentials as their activity is associated with your name.
- ❑ Don't tell anyone your login or the answers to your security questions – even outside of work.
- ❑ Watch for click bait on social media. If it sounds too good to be true, it probably is.
- ❑ Research a website/company that asks for your personal information. Make sure they are legitimate and are taking steps to protect your data.

Reporting and Contact Information

If you have any general questions:

– Bruin Support Services at 1.800.756.7920

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.