

Forum:[Hack Forums](#)

Thread: [Social Engineering | Basics, attack techniques, examples](#)

Ph4n70M Phr34K - June 16, 2023, 8:28 am

Related threads:

<https://hackforums.net/showthread.php?tid=6243986>

<https://hackforums.net/showthread.php?tid=6243938>

<https://hackforums.net/showthread.php?tid=6233658>

<https://hackforums.net/showthread.php?tid=6244776>

Introduction

“There is no technology today that can’t be overcome through social engineering.” - Kevin Mitnick, former hacker and social engineering expert.

Despite the implementation of the most robust technological security measures, every organization faces a challenging and unpredictable vulnerability: its us, humans. For a hacker aiming to acquire vital data or system access, understanding human psychology is just as crucial as mastering computer systems. What is social engineering and how can you safeguard against it? We will address these crucial queries in the following discussion.

What is social engineering and where it is being used.

Social engineering is a non-technical strategy used by cyber-criminals that relies heavily on human interaction and often involves manipulating people into breaking standard security practices and procedures in order to gain unauthorized access to systems or information.

In other words social engineering is the art of manipulating, influencing, or deceiving people so they give up confidential information. Because social engineering exploits human weaknesses rather than technical or digital system vulnerabilities, it is sometimes called ‘human hacking. Offenders leverage social engineering strategies as it is typically simpler to manipulate your inherent tendency to trust than to find methods to breach your software. For instance, tricking someone into revealing their password is generally less complex than attempting to hack that password (unless the password is particularly weak).

Social engineering is not only used in hacking or cyber-security contexts. Its principles have been applied in a variety of scenarios outside the digital world. Social engineering approaches are deeply rooted in understanding human behavior and motivation. They exploit victims' emotions and impulses in manners known to compel individuals into actions that may be detrimental to them. It is a fraudulent scheme that has been in play for several decades. Here are a few areas where social engineering is usually applied to:

- Cyber security and hacking: Social engineering is often the first tactic used by cyber-criminals and hackers in their attempts to gain unauthorized access to systems or information. It's usually the

starting point because it tends to be easier and less time-consuming to exploit human vulnerabilities than to find and exploit technical vulnerabilities. People are often the weakest link in the cyber-security chain. They can be manipulated into revealing sensitive information, such as passwords, or tricked into performing actions that compromise security, like clicking on a malicious link or opening an infected attachment. Moreover, most people are not fully aware of the types and extent of risks that they face, which makes them more likely to fall for these types of attacks. This is why education and awareness training about social engineering and other cyber security threats are vital in helping to prevent such attacks.

- Marketing and Sales: Social engineering techniques are often used in sales and marketing to persuade customers to buy products or services. This can include creating a sense of urgency, using authority figures or celebrities to endorse products, or offering 'exclusive' deals that make the customer feel special.

- Politics and Propaganda: Politicians and governments often use social engineering techniques to influence public opinion or voter behavior. This could include appealing to emotions, using fear tactics, or employing propaganda to shape perceptions and beliefs.

- Interrogation Techniques: Law enforcement agencies often use social engineering during interrogations. For example, they may build rapport with suspects to make them more likely to divulge information, or they might pretend to know more than they do to prompt a confession.

- Con Artists and Fraud: Social engineering is essentially the bread and butter of con artists. They may use tactics such as posing as a bank official, a lottery representative, or a needy individual to trick their victims into giving them money.

- Espionage: Social engineering has long been used in espionage to extract sensitive information. Spies may use techniques such as seduction, befriending targets, or blackmail to manipulate individuals into revealing secrets.

How does social engineering work.

Social engineering exploits human psychology and behaviors to deceive individuals into providing sensitive information or granting access to systems or resources. While the specifics of a social engineering attack can vary greatly based on the tactic used and the target involved, the general steps often include:

- Investigation or Research: The attacker identifies the target and gathers as much information as possible to understand their interests, habits, relationships, job role, etc. This information is often collected from social media profiles, company websites, or other public sources.

- Strategy Development: Based on the information collected, the attacker devises a plausible scenario or pretext. This could be posing as a colleague in need, a trusted vendor, a support person from a software company, or even a sweepstakes with an attractive prize, for example.

- Rapport Building: The attacker makes initial contact with the target and works to build trust. They may use the information gathered earlier to build a connection or establish credibility. Fraudsters commonly mimic or 'imitate' corporations that victims are familiar with, trust, and possibly frequently engage with—so often that they automatically comply with instructions from these brands, neglecting to take the necessary safety measures. Some con artists who employ social engineering tactics utilize easily accessible toolkits to create counterfeit websites that mirror those of well-known brands or businesses.

- **Exploitation:** Once trust has been established, the attacker manipulates the target into performing a certain action or revealing confidential information. This might involve clicking a malicious link, revealing a password, or transferring funds to a specific account. In this stage, the attackers are often Provoking panic or a sense of immediacy. Individuals often react impulsively when they are frightened or rushed. Social engineering schemes may employ a variety of tactics to incite panic or a feeling of haste in victims—for instance, informing the victim that a recent credit card transaction has been declined, that their computer has been infected by a virus, or that an image on their website infringes copyright laws, and so on. Social engineering can also tap into victims' fear of missing out (FOMO), generating a distinct form of urgency.

- **Execution:** The attacker uses the gained information or access for malicious purposes. This could involve stealing funds, accessing confidential data, or installing malware for further attacks.

- **Exit:** After achieving their goal, the attacker typically covers their tracks to avoid detection and to possibly use the same access route in the future.

Known social engineering tactics and techniques.

Almost every type of cyber-security attack contains some kind of social engineering. For example, the classic email and virus scams are laden with social overtones. Social engineering can impact you digitally through mobile attacks in addition to desktop devices. However, you can just as easily be faced with a threat in-person. These attacks can overlap and layer onto each other to create a scam. Understanding the different attack vectors for this type of crime is key when it comes to prevention. Here are some common methods used by social engineering attackers:

- **Phishing:** This is a method where an attacker sends a communication, usually an email, that appears to be from a reputable source and asks for sensitive information such as usernames, passwords, or credit card details. The recipient is tricked into believing that the message is something they want or need and then clicks a link or downloads an attachment.

- **Spear Phishing:** This is a more targeted form of phishing, where the attacker has researched their victim and personalizes their communications to appear more legitimate. This might involve using the victim's name, job title, or other personal information. Spear-phishing attacks are particularly effective because they're highly personalized and often appear to be coming from a trusted source.

- **Watering Hole Attack:** In this type of attack, the attacker observes which websites an organization or a specific group of people frequently visit, then attempts to infect those websites with malware - but the main goal is to infect a user's computer and gain access to the network. The perpetrator collects data about a specific group of people to identify their commonly visited websites, subsequently probing these sites for weak points. Gradually, some members of the targeted group will succumb to the infection, providing the attacker with an entry point into the secure system.

- **Honey Trap:** In this method, the attacker creates a fake profile on social media or dating sites to get the victim to divulge confidential information over time, often under the guise of a romantic or very close friendship relationship. A ploy that entices men to engage with a non-existent but appealing female persona online. This strategy has its roots in age-old espionage techniques where an actual woman was employed for similar purposes.

- **Baiting:** Baiting involves presenting a tantalizing offer to a target, prompting them to take a specific action. This could be executed via a peer-to-peer or social networking site, offering an enticing (potentially adult) movie download, or it could involve a USB drive marked "Q1 Layoff Plan" intentionally left in a public location for the victim to discover. Once the USB device is utilized or the harmful file is downloaded, the victim's computer becomes infected, enabling the perpetrator to

seize control of the system.

Examples of Social Engineering Attacks.

Here are examples of several significant incidents involving social engineering:

- Kevin Mitnick's Hacking Career: Kevin Mitnick is perhaps the most famous social engineer. In the 1980s and 1990s, Mitnick used social engineering, among other tactics, to hack into dozens of systems, including those of major corporations like IBM and Nokia. He often tricked people into revealing their passwords by posing as a system administrator. Mitnick was eventually caught and sentenced to prison. He now works as a security consultant and has written several books on the subject.
- Operation Aurora: In 2009, a series of cyber-attacks known as "Operation Aurora" was launched by hackers believed to be based in China. The attacks, which targeted dozens of major companies, including Google and Adobe, used spear-phishing emails to trick employees into clicking on a link that installed a hidden trojan horse on their computers.
- The AP Twitter Hack: In 2013, the Associated Press's Twitter account was hacked, and a false tweet was sent out claiming that there had been an explosion at the White House and President Obama was injured. The hackers had used spear-phishing emails to obtain the login information of AP staff. The tweet caused a brief panic and a significant temporary drop in the stock market.
- The Fappening or Celebgate: Took place in 2014. In this high-profile case, an individual (or possibly a group) used social engineering techniques, among others, to gain unauthorized access to the iCloud accounts of several celebrities, which led to the leak of many personal photos, some of them explicit. The attacker reportedly used a technique called "spear-phishing," sending targeted emails to the celebrities that appeared to be from Apple or Google, asking them to provide their usernames and passwords. Once the information was obtained, the attacker was able to access the accounts and download the content. The FBI investigated the breach and a man named Ryan Collins was ultimately apprehended. He pleaded guilty to a felony violation of the Computer Fraud and Abuse Act and in 2016 was sentenced to 18 months in federal prison. It's worth noting that this case underscores the importance of not only strong, unique passwords but also the use of two-factor authentication, which can add another layer of security to accounts.
- The 2016 US Election Interference: Russian hackers used social engineering techniques in their alleged interference in the 2016 US Presidential Election. They sent spear-phishing emails to over 1,000 people, including many linked to the Democratic National Committee (DNC). By posing as Google with a request for users to change their passwords, the hackers were able to gain access to many email accounts, including that of the chairman of Hillary Clinton's campaign.
- The 2020 Twitter Bitcoin Scam: In 2020, 130 high-profile Twitter accounts were hijacked, including those of Elon Musk, Bill Gates, and Barack Obama. The attackers posted tweets asking followers to send Bitcoin to a specific address with a promise of doubling their money. The attackers reportedly gained access to Twitter's internal systems by calling employees and posing as Twitter IT staff needing login credentials to access the system. The hack is one of the most high-profile examples of social engineering in recent years.

Here are some other high quality threads related to this topic:

<https://hackforums.net/showthread.php?tid=6239568>

<https://hackforums.net/showthread.php?tid=6239517>

Thank you for reading, please leave a QL or HQ post if you enjoyed it.
Stay tuned for more content.
Sincerely, LEGENDS

Ph4n70M Phr34K - June 26, 2023, 4:29 pm

Here are some other high quality threads related to this topic:

<https://hackforums.net/showthread.php?tid=6239568>

<https://hackforums.net/showthread.php?tid=6239517>

Monyito666 - June 27, 2023, 10:37 pm

Thank you for this very informative, I learned alot from you! Keep posting sir!

Ph4n70M Phr34K - June 29, 2023, 9:39 am

(Jun 27, 2023 10:37 PM)Monyito666 Wrote: [\[CITE\]](#) Thank you for this very informative, I learned alot from you! Keep posting sir!

Thanks.

Make sure to also read the threads that i linked, they hold much more value in this topic.

abbnd - June 29, 2023, 10:14 pm

I read this earlier, but didn't think to comment. Lots of work put in, and lots to help you rethink your strategy. Thanks!

highboy - July 1, 2023, 11:25 am

Hey, thanks for share your knowledge with all of us!

SIM-5382664 - July 2, 2023, 10:16 am

thanks this was very helpful indeed

Ph4n70M Phr34K - July 5, 2023, 9:35 am

(Jun 29, 2023 10:14 PM)abbnd Wrote: [\[CITE\]](#) I read this earlier, but didn't think to comment. Lots of work put in, and lots to help you rethink your strategy. Thanks!

(Jul 1, 2023 11:25 AM)highboy Wrote: [\[CITE\]](#) Hey, thanks for share your knowledge with all of us!

(Jul 2, 2023 10:16 AM)psychmike Wrote: [\[CITE\]](#) thanks this was very helpful indeed

Thanks, more to come shortly.

SVJ - July 10, 2023, 2:37 pm

Very informative and useful. Thank you so much man!

Ph4n70M Phr34K - July 13, 2023, 12:20 pm

(Jul 10, 2023 02:37 PM)Adjust Wrote: [\[CITE\]](#) Very informative and useful. Thank you so much man!

Thanks. Make sure to read the linked threads if you want to read more.

BiNBo - July 14, 2023, 11:10 am

An excellent piece, well written and very comprehensive. The weakest link in many security chains is the human element. This just goes to show exactly that!

cakerw - July 24, 2023, 7:16 am

Thank you very much for your advice, learned a lot

Ph4n70M Phr34K - July 25, 2023, 11:30 am

I was about to add few direct examples from the past but decided that it would be too easy and obvious to correlate them with my aliases.

spROUTrop - July 30, 2023, 3:02 am

Great thread, thanks for sharing this! Sadly Kevin Mitnick passed away a few days ago I believe.

nimda - August 24, 2023, 3:28 am

Thanks man, beginner here. Ashamed to admit but always been interested in pentesting.

niklaus8391 - September 16, 2023, 8:50 pm

Very informative and useful. Thank you so much man!

Philosopherglobe - September 18, 2023, 4:02 pm

Definitely the most fertile ground for making progress with hacking. Great return on time investment

virtualgod - October 6, 2023, 1:52 am

insane post, helped a lot sir

cyphalos - October 8, 2023, 11:25 am

This was really useful to learn from. Thank you for posting! I also really like that you put sources on everything too!

SIM-3205487 - October 11, 2023, 1:43 am

Aye thanks for sharing this bro!

source - November 25, 2023, 12:48 pm

The reason why every bug bounty program does not include SE is because they know how successful it is.

The human is the weakest link.

cute-as-ducks - January 24, 2024, 9:37 am

Thanks for this. Helped alot.

Dr34dm0nk3y - January 24, 2024, 3:48 pm

Lost of high quality info there. Highly appreciate the share!

L0Kae - January 30, 2024, 5:11 pm

I managed to pull off some social back in high school, well if you can even call it that? We where all meant to take home laptops and use them to do our homework right... I done mine and printed it off in class, i then wrote a script that would delay about 7 mins then del sys 32... i gave the computer to the teacher and watched as it bricked in front of her then watched as she tried to fix it and failing, i then told her i don't have a computer at home and need one really bad as my family is very poor and since that laptop was broken could i have another to do my homework and keep the broken one to try fix, she said if the "IT guy" can't fix it i can have it... he just said its "went dead" so i got it... it was running linux before i left school... is that social engineering?

luther - February 1, 2024, 9:06 pm

thaankks for tthis it was very helpfullll

hewhotracks - February 2, 2024, 10:52 pm

Thank you for this I learned alot from you! Keep posting sir!

iFaínez - February 6, 2024, 1:57 pm

Interesting information and also very pleasantly captured. People are so easy to partially understand certain situations.

Thanks for sharing this!

an0n_face - February 7, 2024, 7:25 pm

Amazing content, I learned a lot of stuffs with it :)

Cgelin - February 9, 2024, 6:01 pm

Thank you so much for this

nao3330333 - February 11, 2024, 7:41 pm

seems cool, thanks lmao

Dark Matter - February 13, 2024, 2:24 pm

Awesome post. ?

anihil - February 17, 2024, 10:13 pm

awesome , topic by topic and patience , poor advance

curced - February 25, 2024, 11:26 am

Thank you very nice information. you never stop learning

Gin Ichimaru - February 27, 2024, 2:51 am

thanks for the information contained in this thread

HaryJoab - March 17, 2024, 9:29 pm

thank you

Restinpeso24 - March 19, 2024, 5:13 pm

Another banger of a post mate! Good read as always..

niquitot4 - March 21, 2024, 12:30 am

This is one of the best posts on this site tbh, thanks a lot

Stanley - April 7, 2024, 4:34 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

t1gers - April 7, 2024, 5:27 am

very good material thanks for helping me learn

kippXYZ - September 29, 2024, 7:37 pm

thank you, good to know that.

SIM-5320087 - *October 9, 2024, 12:25 pm*

That's great, thanks for the share.

SIM-5614029 - *January 30, 2025, 11:37 am*

Thank you for sharing a clear summary with an excellent thread build.

Really appreciate the way of posting you participate in

MoonDouma - *March 17, 2025, 1:31 pm*

Thanks for sharing, it's interesting how many things can be done with social engineering.

PapalaLilek - *March 19, 2025, 11:58 am*

Thank you for information. I can learn a lot Fromm this.

bitter222 - *March 20, 2025, 10:29 am*

Thanks man needed something like this!