

Forum:[Hack Forums](#)

Thread: [Social Engineering / Attack Types / Examples / Defense](#)

B3A - April 20, 2023, 9:40 am

Bellow you will find most common SE methods explained , examples and ways to protect yourself.

Phising :

Phishing is a type of social engineering attack where a scammer tries to trick you into providing sensitive information such as passwords, credit card numbers or other personal data. This is often done through email, text message, or a fake website that looks like a legitimate one.

Example :

Code Subject: Urgent

Dear Customer,

We have noticed some unusual activity on your account, and we need you to take urgent action to secure it. Please click on the link below and enter your login details to verify your identity.

[phisinglink]

If you do not take action within the next 24 hours, your account may be suspended, and you will not be able to access your funds or make transactions.

Thank you for your cooperation.

Sincerely,
The Security Team

Note that the message may look legitimate, but the link will lead to a fake website designed to steal your login credentials. It's important to always double-check the sender and the website before providing any sensitive information.

Whaling :

Whaling social engineering, also known as "CEO fraud," is a type of phishing attack that targets high-level executives or individuals in positions of power. The attacker sends a message that appears to be from a senior executive, such as the CEO, CFO, or COO, to an employee with access to sensitive information or funds. The message is often urgent, requesting the recipient to transfer a large sum of money to a specific account or provide sensitive information, such as login credentials or financial data. The message may also contain a sense of urgency or threat, such as the need to keep the transfer confidential.

Code An attacker impersonates a high-ranking executive within a company and sends an email to an employee in the HR department. The email appears to come from the executive's personal email address and is crafted to look legitimate by using the executive's name, signature, and company

logo.

The message requests that the employee send over a file containing sensitive information, such as W2 forms, for all employees within the company. The email also includes a sense of urgency, stating that the information is needed immediately for a confidential business deal.

The employee, believing the message to be legitimate, sends over the requested file. It is only later discovered that the executive's email account had been hacked and the message was fraudulent.

How to defend :

Be cautious of any unexpected or suspicious messages that ask you to provide personal information, click on links, or download attachments. Always double-check the sender's email address or website URL to see if it matches the correct source, as scammers can create fake websites that look same to the originals. Enabling multi-factor authentication on all your accounts provides an extra layer of security by requiring a second factor, such as a fingerprint or one-time code, to log in. Keeping your software and security systems up to date by installing the latest updates and patches can help to protect against known vulnerabilities and threats. It's also helpful to educate yourself and others on how to spot phishing messages

Extra for whaling :

Monitor accounts: Monitor accounts regularly for any unusual activity & Educate employees

Diversion Theft :

Diversion theft social engineering/ "false pickup," is a type of scam where an attacker poses as a somethinglegit to gain access to goods or information. The attacker will often convince victims to allow them access to the goods or information and then divert them to a different location, where the goods or information can be stolen. This type of attack can be used to steal goods such as shipments from a warehouse, or info such as logins or financial data.

Example :

Code Attacker will call the ware and pose as a delivery person for a shipment. Then will request that the shipment be diverted to a different location due to a change in the delivery address. Then provide a fake delivery confirmation number or pose as a representative of the company to gain the employee's trust. Once the goods are to the new location, steals them.

How to defend :

It is important to verify the identity of all service providers, delivery personnel, and contractors before providing access or information

Baiting :

Baiting is where someone offers something enticing like a free download or gift card in exchange for personal information or access to a device or network. Then use this information or access to carry out frauds such as installing malware, or accessing confidential data. The term "baiting" refers to the attacker using something tempting to lure the victim

Example :

Code Baiting social engineering is when an attacker offers something tempting, like a free download, in exchange for personal information or access to a device or network. For example, an attacker might create a fake website that offers free movie downloads in exchange for login credentials. Once the attacker has this information, they can use it to carry out fraud

Honey Trap:

Else, e-whoring. Will briefly explain because there is a whole section about it.

Can be used in a million ways in order to get money, info or any other assets. Victim is often asked to hand gift cards , cashapp , money for travels or taxis. Short term and long term tactics available to distract big numbers out of victims.

How to defend :

Never hand personal information , codes or money to strangers. Confirm their identity in person and avoid handing anything before hand.

Be curious and suspicious with anyone you dont know in person asking for personal information or money in any way/form

Pretexting:

Pretexting is when someone tricks you into giving them sensitive info or access to a system or network by creating a fake story or scenario. They may pretend to be someone you trust like a bank or an agent from a service you are related and use a convincing story to persuade you to give them the what they want. This type of scam usually involves a lot of research on the victim to make the story seem real. The word "pretexting" refers to the use of a false story to trick the victim. Most times "pre" means set before the start. Usually involves graphics and other media to confirm the sayings. (Tools to do this can be found in another thread named " Social Engineering Toolkit "

Example :

Code An attacker calls a victim and pretends to be a customer service representative from a popular online store. The attacker tells the victim that there has been a problem with their recent purchase and asks for the victim's credit card information to fix the issue.

The attacker creates a fake story to trick the victim into believing that their purchase has been compromised and that they need to provide their credit card information urgently. The victim, thinking they are speaking to a legitimate customer service representative, provides the requested information, not realizing that they have just given the attacker access to their credit card account. Pretexting in this case is used with graphics , emails and texts confirming the "legit" sayings

How to defend :

Pretexting refers to the use of a false story to trick someone. It's important to be careful when giving out sensitive information, and to always verify that the person you are talking to is who they say they are.

SMS Phising :

SMS phishing/smishing is whensomeone uses text messages to trick you into giving them your personal information. They might send you a text message that looks like it's from a legitimate source like your bank or a government agency and ask you to click on a link or provide your personal info

Example :

Code You receive a text message that appears to be from your bank. The message tells you that there has been suspicious activity on your account and that you need to click on a link to verify your identity. The link takes you to a website that looks like your bank's website, and it asks you to provide your login credentials and other personal information

Scareware :

Scareware is when scare tactics are used to trick you into buying fake or unnecessary software. They might show you pop-up messages or warning alerts that falsely claim your computer has a virus and offer to fix it for a fee after you pay for the software, you might end up downloading malware onto your computer, or simply wasting your money on useless software

Example :

Code You're browsing the internet and suddenly a pop-up message appears on your screen. The message claims that your computer is infected with a dangerous virus and your personal information is at risk. It urges you to click on a link to download anti-virus software that will protect your computer. You getting charged for something that wont work or even harmful.

How to defend :

To defend against scareware, use reputable anti-virus software, don't trust unsolicited pop-up messages, close the window, research and verify the software's authenticity, and keep your software up to date

Tailgating / Piggybacking :

Is when you gain access to a secure area by following closely behind someone who has the authorized access. This could be a physical space a building or room or a digital space such as a network

The attacker takes advantage of people's natural tendency to hold the door open for others or to avoid confrontation by questioning someone who appears to belong in the space.

How to defend :

Maintain a policy of not letting strangers follow you into secure areas

Watering Hole :

Is when a hacker targets a website or online platform that is frequented by a particular group of people, such as employees of a specific company or members of a certain industry. Then infects the computers with a virus and steals info or logins. These logins can be used to breach the original targeted website.

*Search

*Be Suspicious

*Avoid fast reactions

*Verify the most you can

Dread.Reaper - April 20, 2023, 9:47 am

Awesome Read, great information for people to know.

Lukasi - April 20, 2023, 10:30 am

Knowledge has increased again, thank you for sharing?

Jess234 - April 20, 2023, 10:44 am

Can you dm me because i can't dm you

B3A - April 20, 2023, 10:50 am

(Apr 20, 2023 10:44 AM)Jess234 Wrote: [\[CITE\]](#) Can you dm me because i can't dm you
Just reply here and I will kindly help

ALEDIO - April 20, 2023, 1:27 pm

My compliments, an interesting and quite complete thread. I'm happy to see that in the last few days you're dedicating yourself to making HQ threads and you're succeeding admirably, always try to improve your own threads as much as possible from all points of view so they will get more visibility.

B3A - April 26, 2023, 1:38 am

Thank you guys for the positivity.

LMK if there is anything new you'd like to see

qiiwudhu - May 15, 2023, 6:56 pm

(Apr 20, 2023 09:40 AM)Be?? Wrote: [\[CITE\]](#) Bellow you will find most common SE methods explained , examples and ways to protect yourself.

Phising :

Phishing is a type of social engineering attack where a scammer tries to trick you into providing sensitive information such as passwords, credit card numbers or other personal data. This is often done through email, text message, or a fake website that looks like a legitimate one.

Example :

Code Subject: Urgent

Dear Customer,

We have noticed some unusual activity on your account, and we need you to take urgent action to secure it. Please click on the link below and enter your login details to verify your identity.

[phisinglink]

If you do not take action within the next 24 hours, your account may be suspended, and you will not be able to access your funds or make transactions.

Thank you for your cooperation.

Sincerely,
The Security Team

Note that the message may look legitimate, but the link will lead to a fake website designed to steal

your login credentials. It's important to always double-check the sender and the website before providing any sensitive information.

Whaling :

Whaling social engineering, also known as "CEO fraud," is a type of phishing attack that targets high-level executives or individuals in positions of power. The attacker sends a message that appears to be from a senior executive, such as the CEO, CFO, or COO, to an employee with access to sensitive information or funds. The message is often urgent, requesting the recipient to transfer a large sum of money to a specific account or provide sensitive information, such as login credentials or financial data. The message may also contain a sense of urgency or threat, such as the need to keep the transfer confidential.

Code An attacker impersonates a high-ranking executive within a company and sends an email to an employee in the HR department. The email appears to come from the executive's personal email address and is crafted to look legitimate by using the executive's name, signature, and company logo.

The message requests that the employee send over a file containing sensitive information, such as W2 forms, for all employees within the company. The email also includes a sense of urgency, stating that the information is needed immediately for a confidential business deal.

The employee, believing the message to be legitimate, sends over the requested file. It is only later discovered that the executive's email account had been hacked and the message was fraudulent.

How to defend :

Be cautious of any unexpected or suspicious messages that ask you to provide personal information, click on links, or download attachments. Always double-check the sender's email address or website URL to see if it matches the correct source, as scammers can create fake websites that look same to the originals. Enabling multi-factor authentication on all your accounts provides an extra layer of security by requiring a second factor, such as a fingerprint or one-time code, to log in. Keeping your software and security systems up to date by installing the latest updates and patches can help to protect against known vulnerabilities and threats. It's also helpful to educate yourself and others on how to spot phishing messages

Extra for whaling :

Monitor accounts: Monitor accounts regularly for any unusual activity & Educate employees

Diversion Theft :

whensomeone uses text messages to trick you into giving them your personal information. They might send you a text message that looks like it's from a legitimate source like your ba
Great job