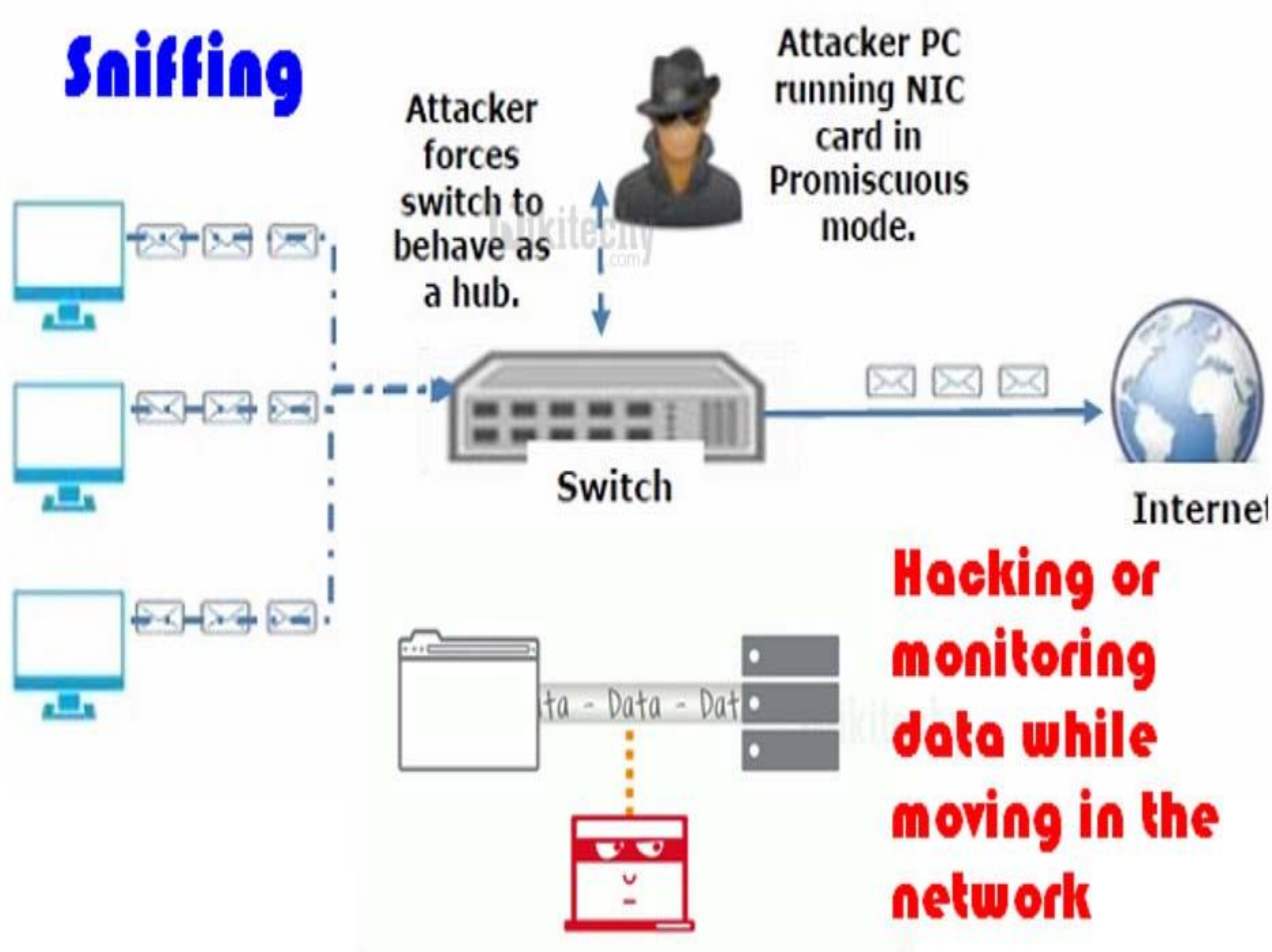
UNIT-4-Sniffing Packet Analysis & Session Hijacking

Sniffing : What Is Sniffing?

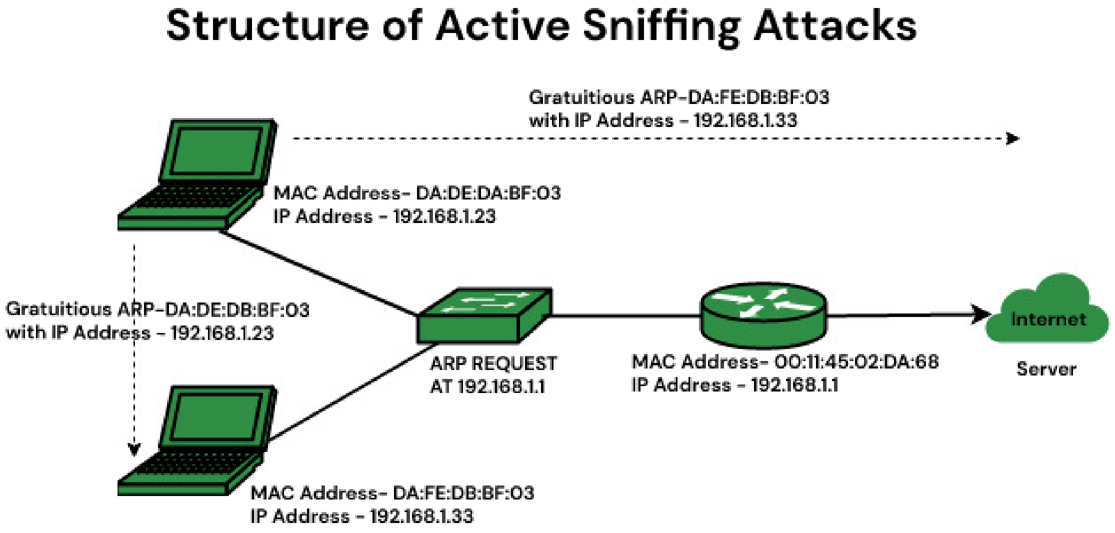
In its simplest form, sniffing is the act of intercepting and monitoring traffic on a network. This can be done using software that captures all data packets passing through a given network interface or by using hardware devices explicitly designed for this purpose.


Sniffing
Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet
ta - Data - Dat
Hacking or monitoring data while moving in the network

What Are Sniffing Attacks

A sniffing attack occurs when an attacker uses a packet sniffer to intercept and read sensitive data passing through a network (Biasco, 2021). Common targets for these attacks include unencrypted email messages, login credentials, and financial information.

In some cases, attackers may also use sniffing attack tools and packet sniffers to inject malicious code into otherwise innocuous data packets in an attempt to hijack a target’s computer or other devices.


Structure of Active Sniffing Attacks
Gratuitious ARP-DA:FE:DB:BF:03
with IP Address - 192.168.1.33
MAC Address- DA:DE:DA:BF:03
IP Address - 192.168.1.23
Gratuitious ARP-DA:DE:DB:BF:03
with IP Address - 192.168.1.23
ARP REQUEST
AT 192.168.1.1
MAC Address- 00:11:45:02:DA:68
IP Address - 192.168.1.1
Internet
Server
MAC Address- DA:FE:DB:BF:03
IP Address - 192.168.1.33

Credit Card
Bank Account
Passwords
etc.
KeySniffer
USB Dongle
All your keystrokes
transmitted in clear text
and readable to anyone
All your keystrokes!
Credit Card
Bank Account
Passwords
etc.
Low Cost
Crazyradio
Dongle
KEYBOARD TRANSMISSIONS CAN BE DETECTED FOR SEVERAL HUNDRED FEET

Types of Sniffing Attacks: There are 2 primary sniffing attack types: passive and active.

Passive Sniffing: In a passive sniffing attack, the hacker monitors traffic passing through a network without interfering in any way. This type of attack can be beneficial for gathering information about targets on a network and the types of data (e.g., login credentials, email messages) they are transmitting. Because it does not involve any interference with the target systems, it is also less likely to raise suspicion than other types of attacks.

Active Sniffing

Active sniffing is a type of attack that involves sending crafted packets to one or more targets on a network to extract sensitive data. By using specially crafted packets, attackers can often bypass security measures that would otherwise protect data from being intercepted. Active sniffing can also involve injecting malicious code into target systems that allows attackers to take control of them or steal sensitive information.

Consequences of a Sniffing Attack

A successful sniffing attack can have several severe consequences for the targets. These can include:

- Loss of sensitive data, such as login credentials, financial information, and email messages
- Injection of malicious code into target systems, allowing attackers to control devices or access sensitive information
- Interruption of network traffic, which can cause communication problems and slow down network performance
- Exposure of confidential information, such as trade secrets and proprietary data
- Damage to the reputation of the organization whose network has been compromised

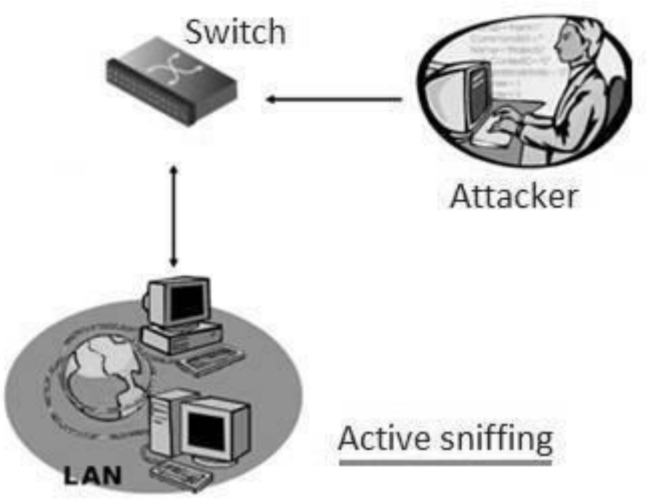
How Can Sniffing Attacks Be Prevented? There are many ways to protect your network against sniffing attacks. Some key measures include:

- Using encryption to protect sensitive data from being intercepted
- Never sending sensitive information over an unencrypted connection
- Ensuring that all computers on a network are adequately protected with antivirus and firewall software
- Making sure the wireless network is secured using WPA or WEP encryption
- Regularly updating all software and devices with the latest security patches
- Staying aware of what type of traffic passes through the network and taking steps to protect sensitive information
- Using a VPN when connecting to public Wi-Fi networks
- Continuously monitoring the network for unusual activity.

SniffingTechniques

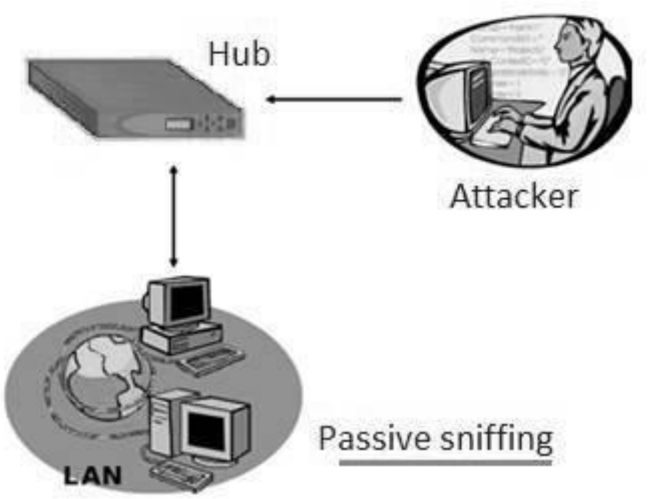
Active sniffing & Passive sniffing Techniques

Active sniffing



• In this sniffing type, attacker directly interacts with target machine by sending packets and receiving responses.
• This sniffing is carried out through Switch. In this type, attacker tries to poison the switch by sending bogus MAC address.
• Examples of active sniffing : ARP spoofing, MAC flooding, HTTPS and SSH spoofing, DNS spoofing etc.

Passive sniffing



- In this sniffing type, attacker does not interact with the target. He/she simply hook on to the network and captures packets transmitted and received by the network or exchanged between two machines.
- This sniffing is carried out through hub. An attacker connects to the hub from his/her machine. Attacker needs account on the LAN.
- Examples of passive sniffing: Hub based networks or wireless networks

Packet Analysis

Packet analysis is the process of examining the contents of the data packets the network sniffer captures. Packet analysis can reveal useful information about the network, such as the source and destination IP addresses, protocols, ports, payload, and errors. It can also help identify anomalies, vulnerabilities, and malicious activities on the network. Some examples of network sniffing and packet analysis tools for reconnaissance are Nmap, Wireshark, and Tcpdump.

Packet analysis for troubleshooting :Troubleshooting is the process of identifying and resolving problems on a network, including performance issues, configuration errors, or security breaches. Network sniffing and packet analysis can help you troubleshoot network problems by providing visibility into the network traffic and its behavior. Network sniffing and packet analysis tools monitor network traffic, filter and search for specific packets, measure network latency and throughput, and detect any errors or anomalies on the network.

2.Data extraction involves extracting sensitive or valuable information from network traffic, such as usernames, passwords, credit card numbers, or files. Network sniffing and packet analysis can help you simulate data extraction by capturing and analyzing the packets that contain the information you are looking for. These tools help decode and decrypt the packets, extract the payload, and reconstruct the data. Some examples of data extraction techniques hackers use you should be aware of are session hijacking, ARP spoofing, and DNS spoofing.

3.Network attacks happen when a hacker exploits the vulnerabilities of a network or its devices, services, or users. Network sniffing and packet analysis can help you simulate network attacks by manipulating the network traffic and its behavior. Hackers use network sniffing and packet analysis tools to inject, modify, or drop packets, spoof or redirect the packets, or launch denial-of-service attacks.Capture Telnet, FTP, TFTP, HTTP passwords.

-1.Replay VoIP conversations.

- 2.Capture routing protocol (OSPF) authentication passwords.

- 3.Troubleshoot network issues.

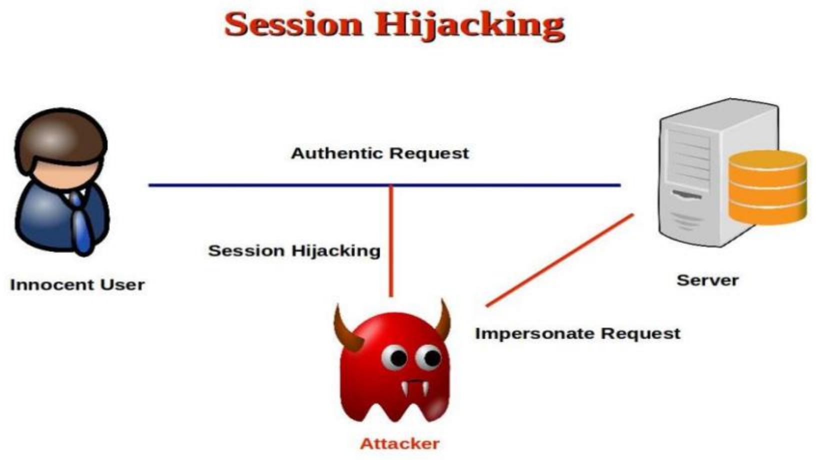
- 4.Use Kali Linux to hack networks and capture user data

Session Hijacking

Session hijacking is a technique used by hackers to gain access to a target's computer or online accounts. In a session hijacking attack, a hacker takes control of a user's browsing session to gain access to their personal information and passwords. This article will explain what session hijacking is, how it works, and how to prevent it from happening.

A session hijacker can take control of a user's session in several ways. One common method is to use a packet sniffer to intercept the communication between the user and the server, which allows the hacker to see what information is being sent and received. They can then use this information to log in to the account or access sensitive data.

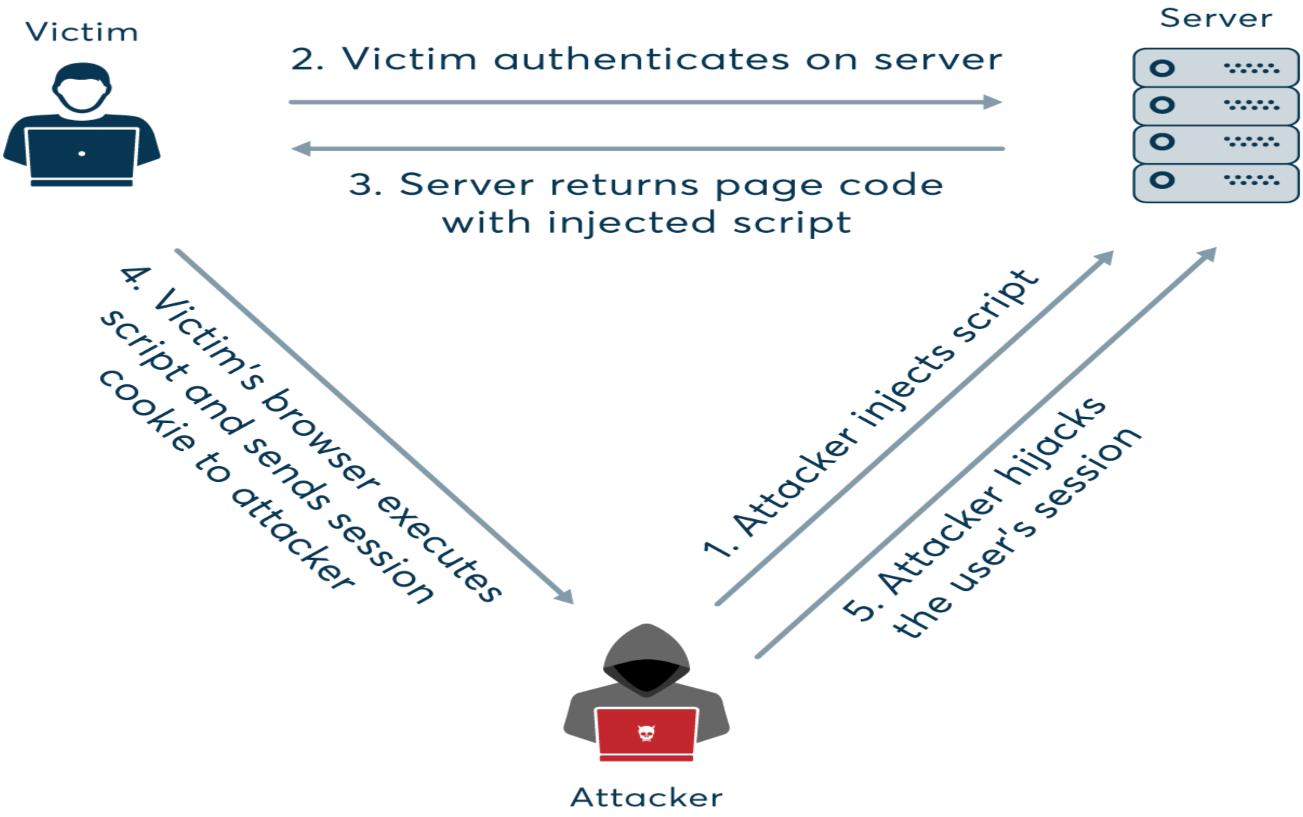
Session hijacking can also be performed by deploying malware to infect the user's computer. This gives the hacker direct access to the machine, enabling them to then hijack any active sessions.



The Different Types of Session Hijacking?

Session hijacking are 2 types 1)active & 2)passive.

Active session hijacking: the attacker takes control of the target's session while it is still active. The attacker does this by sending a spoofed request to the server that includes the target's session ID. This type of attack is more challenging to execute because it requires the attacker to have an OnPath (also known as "man-in-the-middle") position between the target and the server.


Victim
Server
2. Victim authenticates on server
3. Server returns page code with injected script
4. Victim's browser executes script and sends session cookie to attacker
1. Attacker injects script
5. Attacker hijacks the user's session
Attacker

Passive session hijacking: occurs when the attacker eavesdrops on network traffic to steal the target's session ID. This type of attack is easier to execute because all an attacker needs is access to network traffic, which can be easily accomplished if they are on the same network as the target.

Prevent Session Hijacking

There are several ways to prevent session hijacking from happening:

- **Use strong passwords and multifactor authentication.** These techniques protect accounts from being accessed by hackers if they manage to steal a user's session ID (Alkove, 2021).
- **Only share session IDs with trusted sources.** Be careful when sharing links or sending requests to websites, as these may include session IDs.
- **Use a VPN.** A VPN helps prevent attackers from intercepting traffic, making it more difficult for them to steal session IDs (McCann & Hardy, 2022).
- **Keep software up to date.** Make sure to keep operating systems and software up to date with the latest security patches to prevent attackers from exploiting vulnerabilities to access users' sessions.
- **Take cybersecurity training.** Cybersecurity threats are constantly evolving, so it's essential to stay informed on the latest attack techniques and how to prevent them. Consider getting certified in various cybersecurity domains, including ethical hacking, incident handling, and penetration testing.

The Dangers of Session Hijacking Attacks

There are many risks associated with not taking steps to prevent session hijacking. Some of these dangers include:

- **Theft of personal information.** Session hijacking can give hackers access to confidential information, including passwords and credit card numbers, leading to identity theft or financial fraud.
- **Malware infection.** If a hacker can steal a user's session ID, they may also be able to infect the user's computer with malware (Marino, 2021). This can allow them to gain control of the target's computer and steal their data.
- **Denial-of-Service (DoS) attacks.** A hacker who gains control of a user's session could launch a DoS attack against the website or server to which they're connected, disrupting service or causing the site to crash.

SOCIAL ENGINEERING:

Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks or physical locations or for financial gain.

Social engineering Process Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

If the attack is successful, the attacker gains access to confidential information, such as Social Security numbers and credit card or bank account information; makes money off the targets; or gains access to protected systems or networks.

Process of social engineering attacks

Popular types of social engineering attacks include the following techniques:

- **Baiting.** An attacker leaves a malware-infected physical device, such as a Universal Serial Bus flash drive, in a place it is sure to be found. The target then picks up the device and inserts it into their computer, unintentionally installing the malware.
- **Phishing.** When a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing financial or personal information or clicking on a link that installs malware.
- **Spear phishing.** This is like phishing, but the attack is tailored for a specific individual or organization.
- **Vishing.** Also known as *voice phishing*, vishing involves the use of social engineering over the phone to gather financial or personal information from the target.

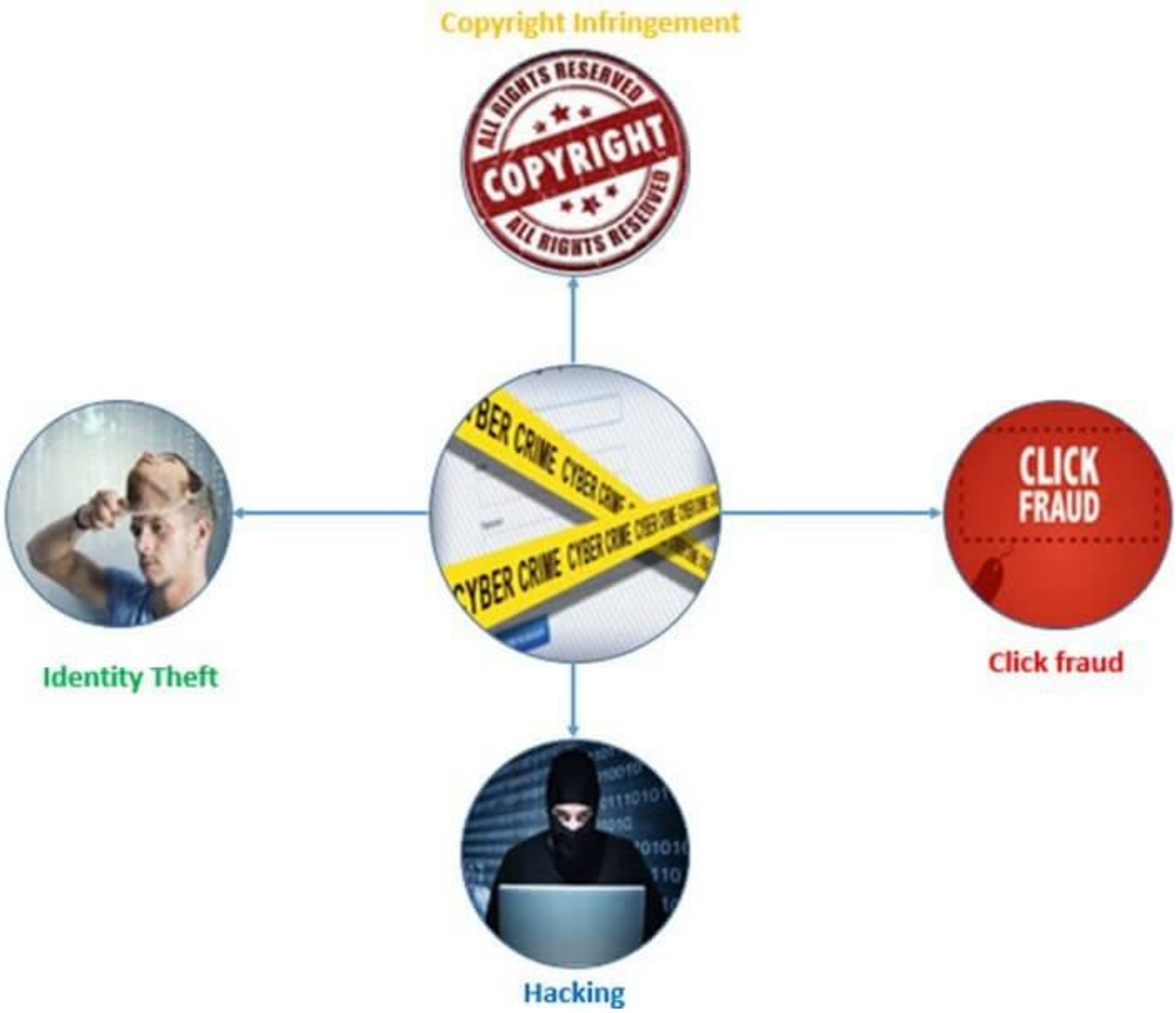
- **Whaling.** A specific type of phishing attack, a whaling attack targets high-profile employees, such as the chief financial officer or chief executive officer, to trick the targeted employee into disclosing sensitive information.

IDENTITY THEFT?

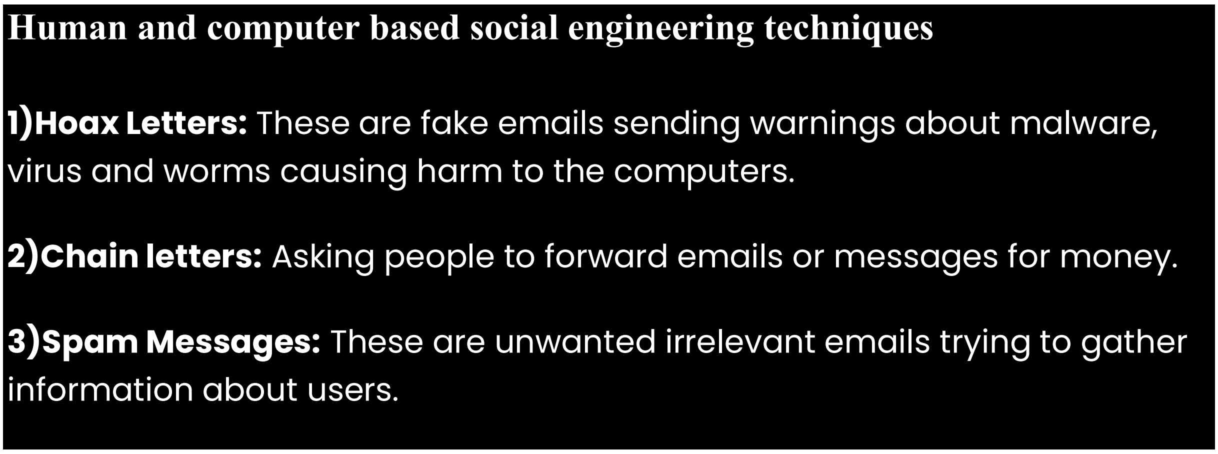
Identity theft occurs when criminals steal a victim's personal information to commit criminal acts. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name.

Cyber criminals commit identity theft by using sophisticated cyber attack tactics, including social engineering, phishing, and malware. Identity theft can also result from rudimentary tactics with criminals stealing mail, digging through dumpsters, and listening in on phone conversations in public places.

The ultimate goal of many cyber attacks is to steal enough information about a victim to assume their identity to commit fraudulent activity. Unfortunately, most people only discover they're victims of identity theft when they apply for a loan, attempt to open a bank account, apply for a job, receive a call from a collection agency, or request a new credit card.



Human and computer based social engineering techniques



Human and computer based social engineering techniques

1)Hoax Letters: These are fake emails sending warnings about malware, virus and worms causing harm to the computers.

2)Chain letters: Asking people to forward emails or messages for money.

3)Spam Messages: These are unwanted irrelevant emails trying to gather information about users.

4)Instant Chat messengers: Gathering personal information from a single user by chatting with them.

5)Phishing: Creating a cloned fake website trying to gather sensitive information about users. It can be done by sending a fake email as though coming from an original website and then trying to collect confidential information.

Phishing can also be executed through fake mobile applications.

Mobile based Attacks:

1)SMS based: Sending a fake SMS saying that the user has won a bounty, urging him/her to register with confidential information or try and collect other important details.

2)Through Malicious Apps: Applications downloaded from third party sources may be malicious; they can access authentication information and other sensitive details.

3)Through Email and messengers: Attackers can send spam emails or malicious links through messenger applications. When the victim clicks on it- he may be redirected to a malicious site, or a malware could be downloaded or it may lead to some other malicious activity.

Phishing

Phishing is a type of online fraud that involves tricking people into providing sensitive information, such as passwords or credit card numbers, by masquerading as a trustworthy source. Phishing can be done through email, social media or malicious websites.

Process of phishing?

Phishing works by sending messages that look like they are from a legitimate company or website. Phishing messages will usually contain a link that takes the user to a fake website that looks like the real thing. The user is then asked to enter personal information, such as their credit card number. This information is then used to steal the person's identity or to make fraudulent charges on their credit card.

Types of Phishing Attack

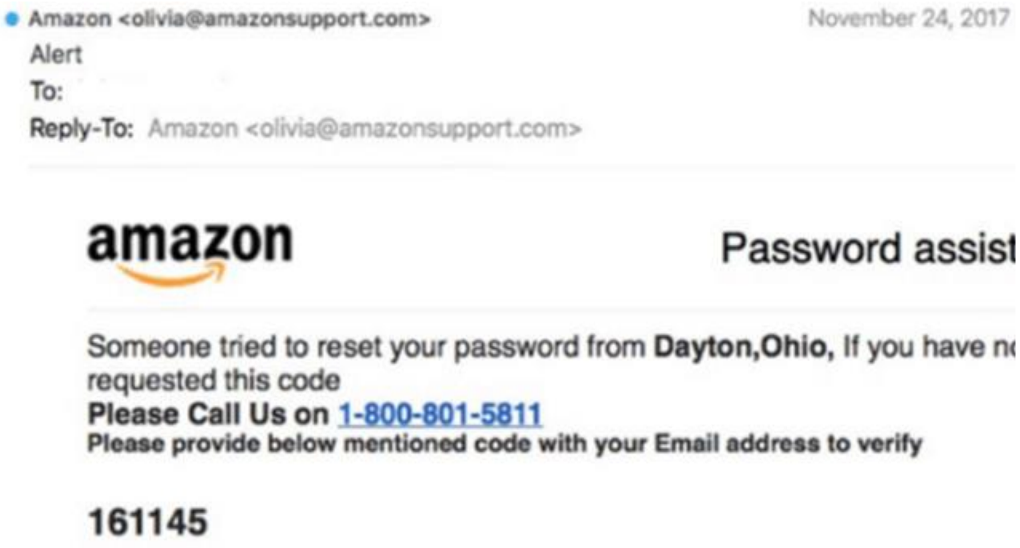
The 5 Most Common Types of Phishing Attack

1. Email phishing

Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organisation and sends thousands of generic requests.

The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.

In other cases, the fraudsters create a unique domain that includes the legitimate organisation's name in the URL. The example below is sent from 'olivia@amazonsupport.com'.



Amazon <olivia@amazonsupport.com> November 24, 2017
Alert
To:
Reply-To: Amazon <olivia@amazonsupport.com>

amazon

Password assist

Someone tried to reset your password from **Dayton,Ohio,** If you have n
requested this code
Please Call Us on 1-800-801-5811
Please provide below mentioned code with your Email address to verify

161145

The recipient might see the word 'Amazon' in the sender's address and assume that it was a genuine email.

There are many ways to spot a phishing email, but as a general rule, you should always check the email address of a message that asks you to click a link or download an attachment.

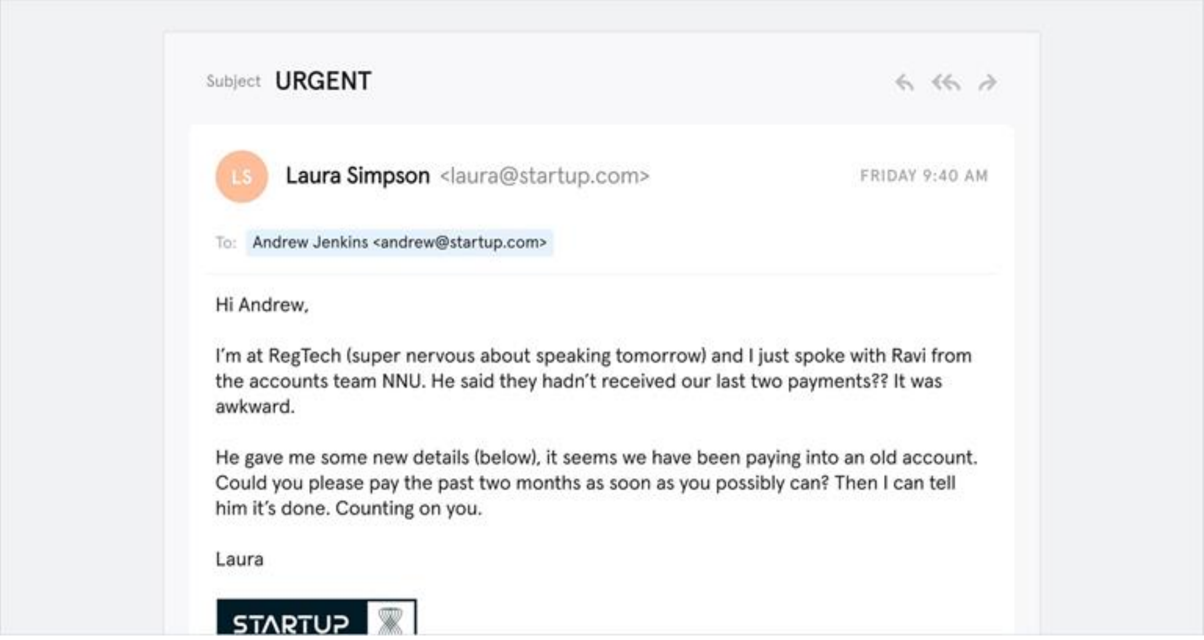
2. Spear phishing

There are two other, more sophisticated, types of phishing involving email.

The first, spear phishing, describes malicious emails sent to a specific person. Criminals who do this will already have some or all of the following information about the victim:

- Their name.
- Place of employment.
- Job title.
- Email address; and
- Specific information about their job role.

You can see in the example below how much more convincing spear phishing emails are compared to standard scams.



Subject URGENT

Laura Simpson <laura@startup.com> FRIDAY 9:40 AM

To: Andrew Jenkins <andrew@startup.com>

Hi Andrew,

I'm at RegTech (super nervous about speaking tomorrow) and I just spoke with Ravi from the accounts team NNU. He said they hadn't received our last two payments?? It was awkward.

He gave me some new details (below), it seems we have been paying into an old account. Could you please pay the past two months as soon as you possibly can? Then I can tell him it's done. Counting on you.

Laura

The fraudster has the wherewithal to address the individual by name and (presumably) knows that their job role involves making bank transfers on behalf of the company.

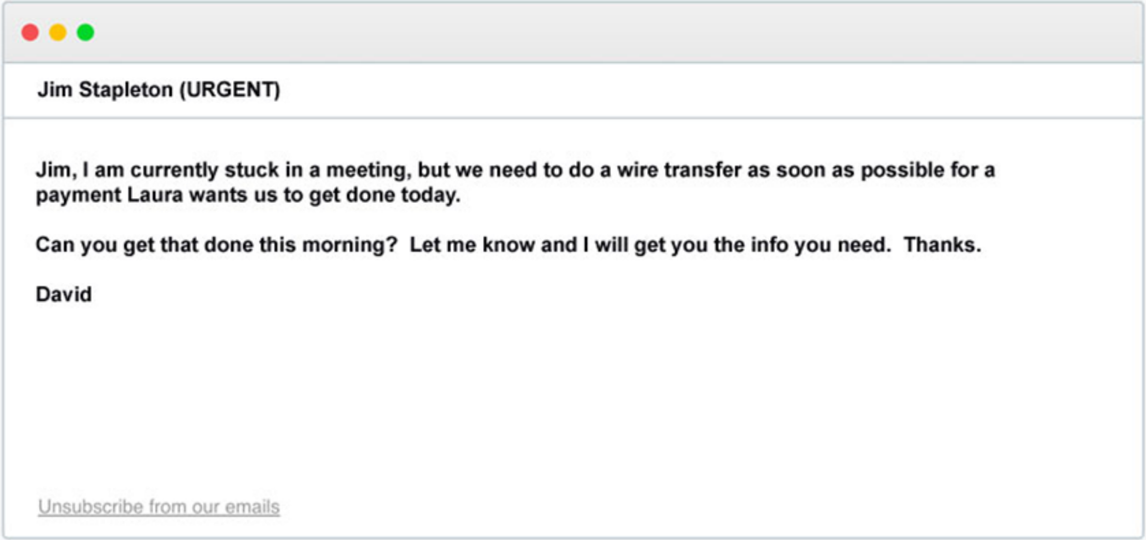
The informality of the email also suggests that the sender is a native English speaker and creates the sense that this is a real message rather than a template.

3. Whaling

Whaling attacks are even more targeted, taking aim at senior executives. Although the end goal of whaling is the same as any other kind of phishing attack, the technique tends to be a lot subtler.

Tricks such as fake links and malicious URLs aren't helpful in this instance, as criminals are attempting to imitate senior staff.

Whaling emails also commonly use the pretext of a busy CEO who wants an employee to do them a favour.



Jim Stapleton (URGENT)

Jim, I am currently stuck in a meeting, but we need to do a wire transfer as soon as possible for a payment Laura wants us to get done today.

Can you get that done this morning? Let me know and I will get you the info you need. Thanks.

David

Unsubscribe from our emails

Emails such as the above might not be as sophisticated as spear phishing emails, but they play on employees' willingness to follow instructions from their boss.

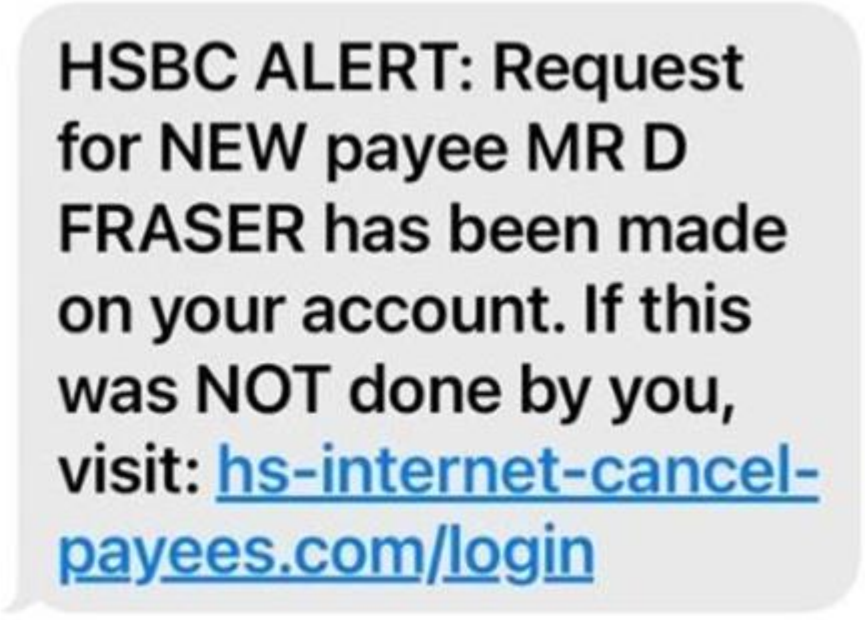
Recipients might suspect that something is amiss but are too afraid to confront the sender to suggest that they are being unprofessional.

4. Smishing and vishing

With both smishing and vishing, telephones replace emails as the method of communication.

Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.

One of the most common smishing pretexts are messages supposedly from your bank alerting you to suspicious activity.



HSBC ALERT: Request for NEW payee MR D FRASER has been made on your account. If this was NOT done by you, visit: hs-internet-cancel-payees.com/login

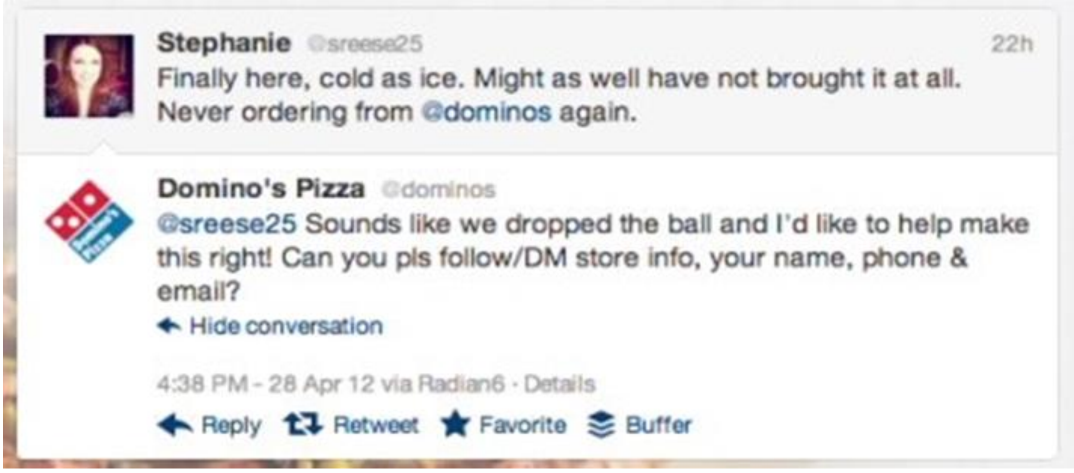
In this example, the message suggests that you have been the victim of fraud and tells you to follow a link to prevent further damage. However, the link directs the recipient to a website controlled by the fraudster and designed to capture your banking details.

5. Angler phishing

A relatively new attack vector, social media offers several ways for criminals to trick people. Fake URLs; cloned websites, posts, and tweets; and instant messaging (which is essentially the same as smishing) can all be used to persuade people to divulge sensitive information or download malware.

Alternatively, criminals can use the data that people willingly post on social media to create highly targeted attacks.

As this example demonstrates, angler phishing is often made possible due to the number of people containing organisations directly on social media with complaints.



Stephanie @sreese25 22h

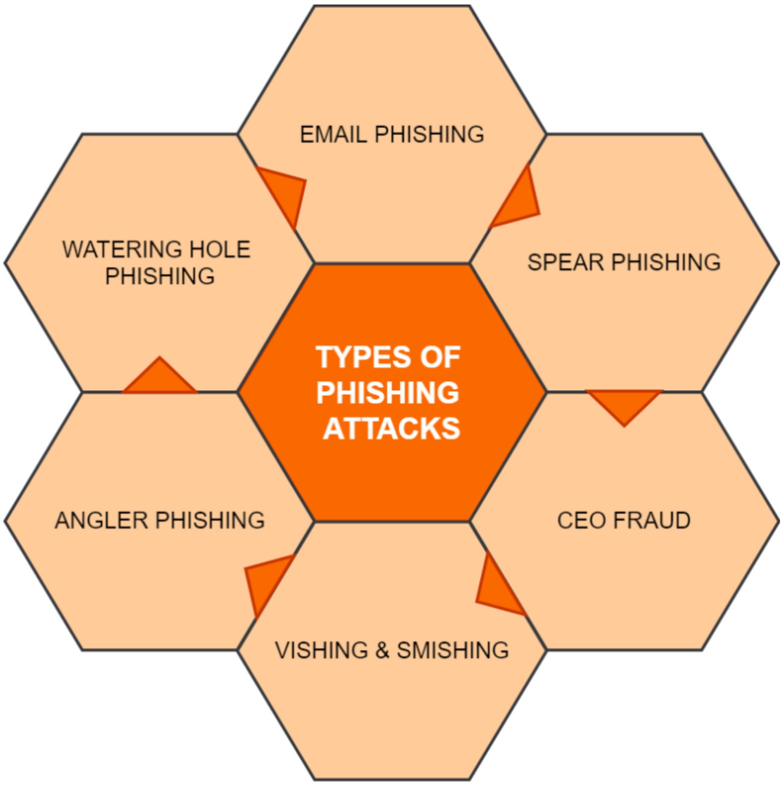
Finally here, cold as ice. Might as well have not brought it at all. Never ordering from @dominos again.

Domino's Pizza @dominos

@sreese25 Sounds like we dropped the ball and I'd like to help make this right! Can you pls follow/DM store info, your name, phone & email?

Organisations often use these as an opportunity to mitigate the damage – usually by giving the individual a refund.

However, scammers are adept at hijacking responses and asking the customer to provide their personal details. They are seemingly doing this to facilitate some form of compensation, but it is instead done to compromise their accounts.



TYPES OF PHISHING ATTACKS

EMAIL PHISHING

SPEAR PHISHING

CEO FRAUD

VISHING & SMISHING

ANGLER PHISHING

WATERING HOLE PHISHING

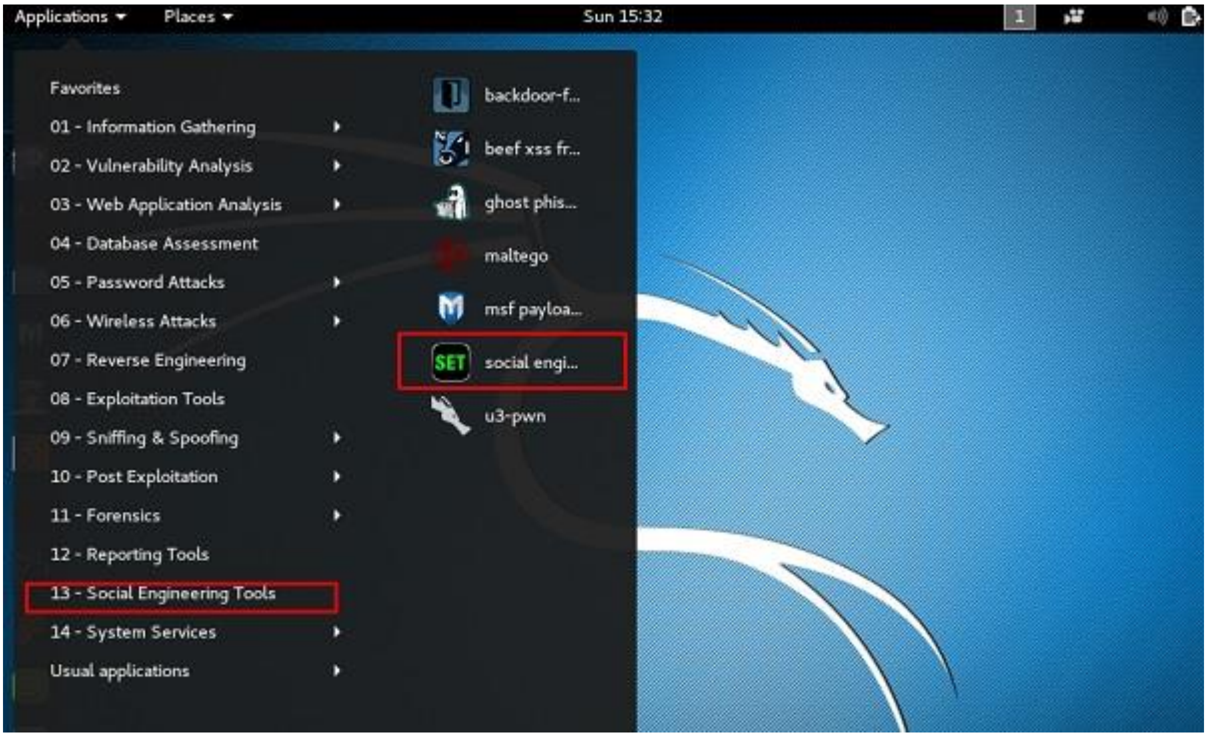
Social Engineering Toolkit :

A lot of people think social engineering is about lying to people to get information or deceiving them to steal something from them which is totally wrong. Social engineering has a lot of definitions but this one is so accurate:
"The act of manipulating a person to take any action that may or may not be in the target's best interest."

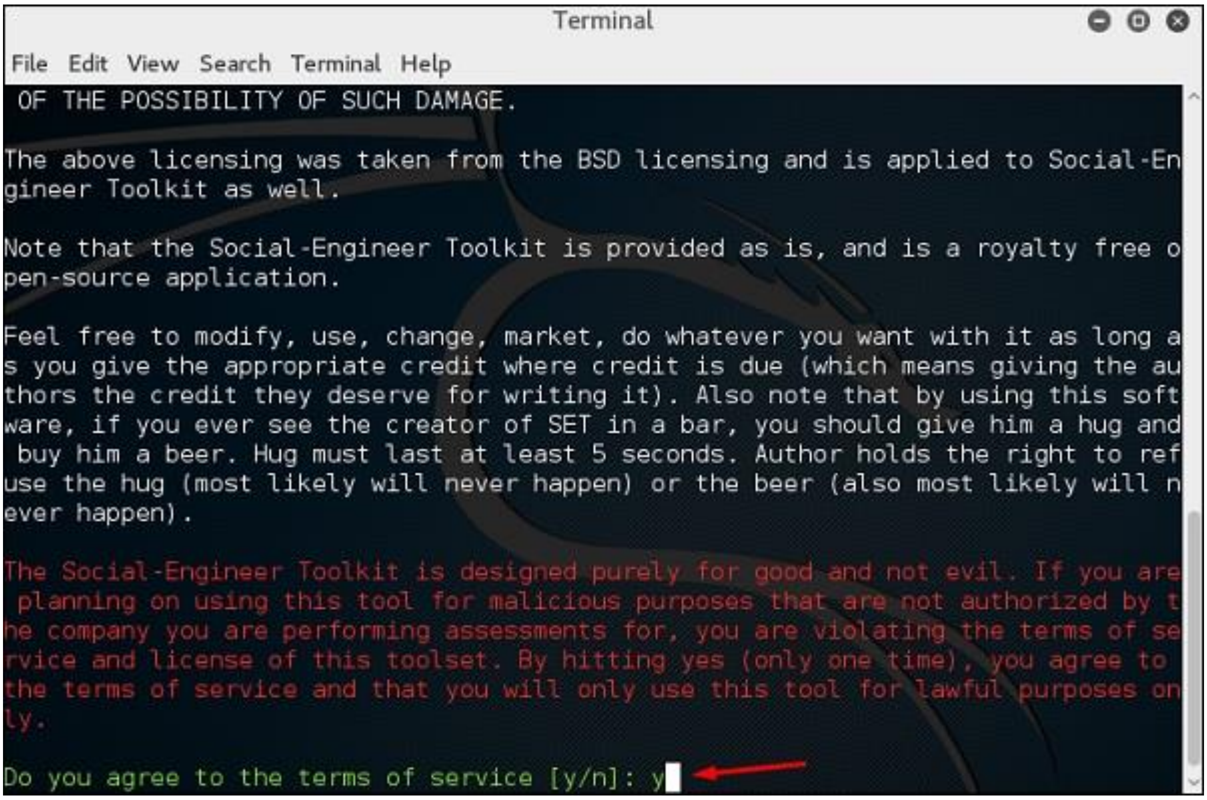
The **Social-Engineer Toolkit** (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

Let's learn how to use the Social Engineer Toolkit.

Step 1 − To open SET, go to Applications → Social Engineering Tools → Click "SET" Social Engineering Tool.

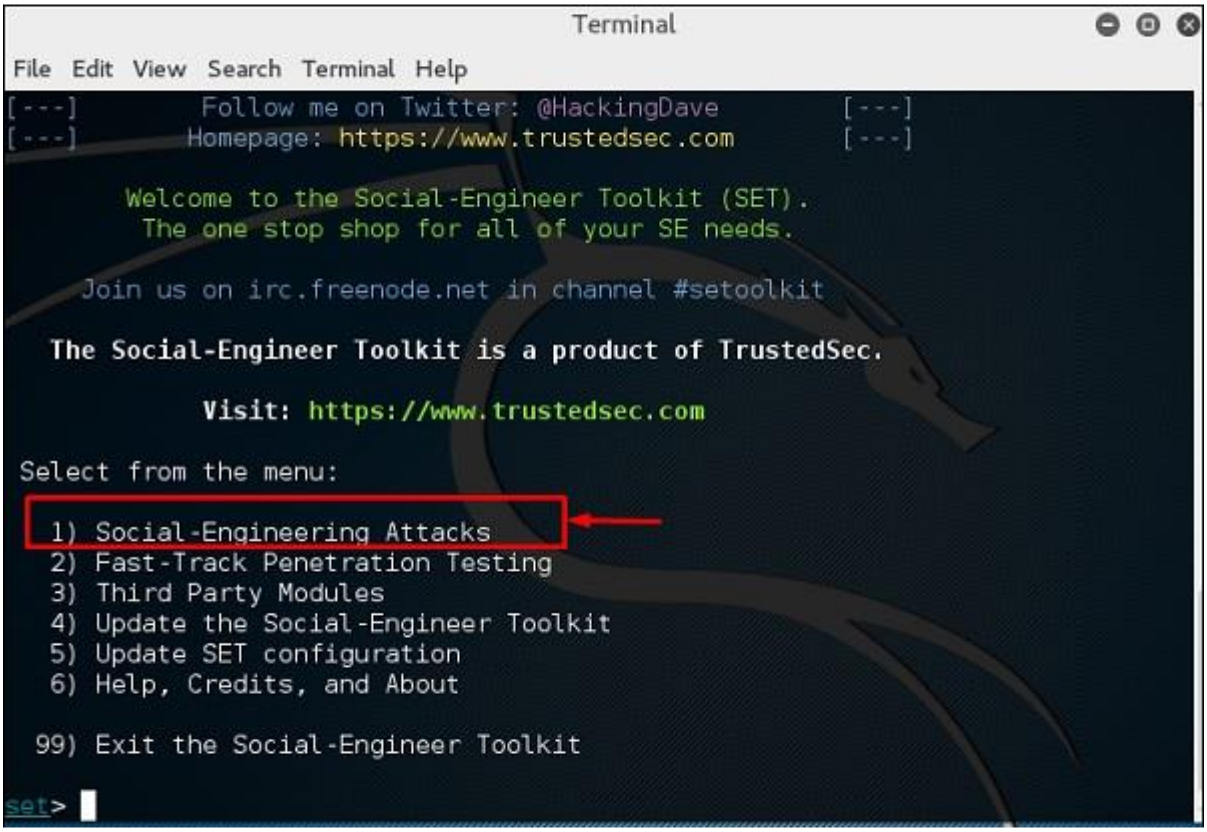


Step 2 − It will ask if you agree with the terms of usage. Type **"y"** as shown in the following screenshot.



```
 OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-En
gineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free o
pen-source application.

Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit is due (which means giving the au
thors the credit they deserve for writing it). Also note that by using this soft
ware, if you ever see the creator of SET in a bar, you should give him a hug and
 buy him a beer. Hug must last at least 5 seconds. Author holds the right to ref
use the hug (most likely will never happen) or the beer (also most likely will n
ever happen).

The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.

Do you agree to the terms of service [y/n]: y
```

Step 3 − Most of the menus shown in the following screenshot are self-explained and among them the most important is the number 1 “Social Engineering Attacks”.



```
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

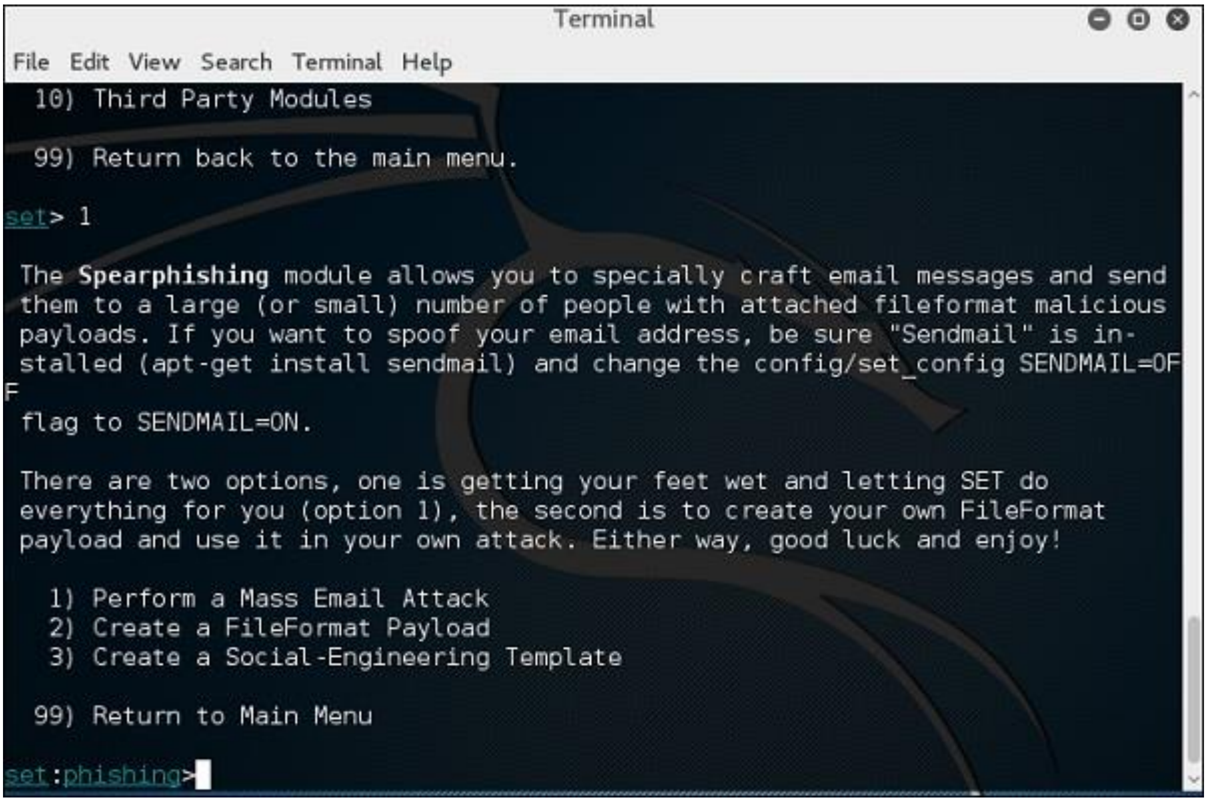
Step 4 − Type **“1”** → Enter. A submenu will open. If you press the **Enter** button again, you will see the explanations for each submenu.

The Spear-phishing module allows you to specially craft email messages and send them to your targeted victims with attached **FileFormatmalicious** payloads. For example, sending malicious PDF document which if the victim opens, it will compromise the system. If you want to spoof your email address, be sure “Sendmail” is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options for the spear phishing attack −

- Perform a Mass Email Attack
- Create a FileFormat Payload and a Social-Engineering Template

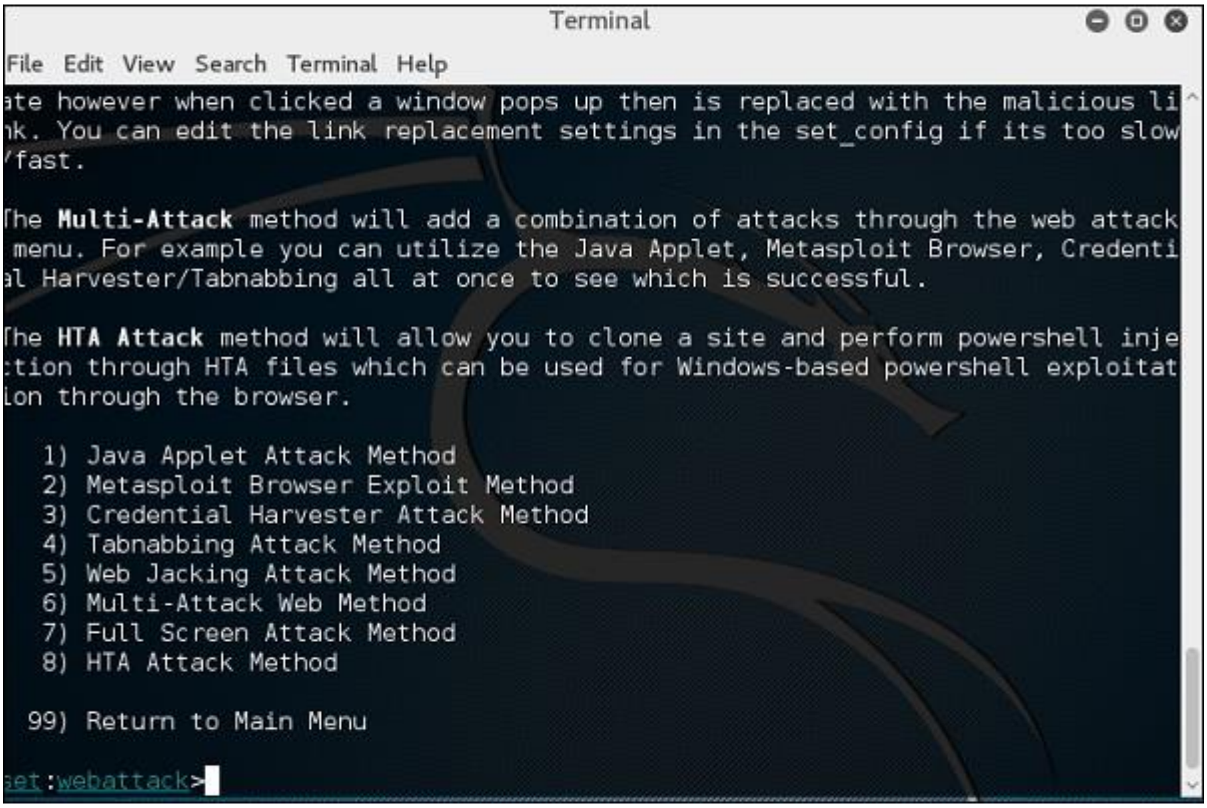
The first one is letting SET do everything for you (option 1), the second one is to create your own FileFormat payload and use it in your own attack.



```
  10) Third Party Modules

  99) Return back to the main menu.

set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OF
F
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

Type **“99”** to go back to the main menu and then type **“2”** to go to “The web attack vectors”.

The web attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim. This module is used by performing phishing attacks against the victim if they click the link. There is a wide variety of attacks that can occur once they click a link.



```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

Type **“99”** to return to the main menu and then type **“3”**.

The infectious USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. The payload and autorun file is burned or copied on a USB. When DVD/USB/CD is inserted in the victim’s machine, it will trigger an autorun feature (if autorun is enabled) and hopefully compromise the system. You can pick the attack vector you wish to use: file format bugs or a straight executable.