Social Engineering

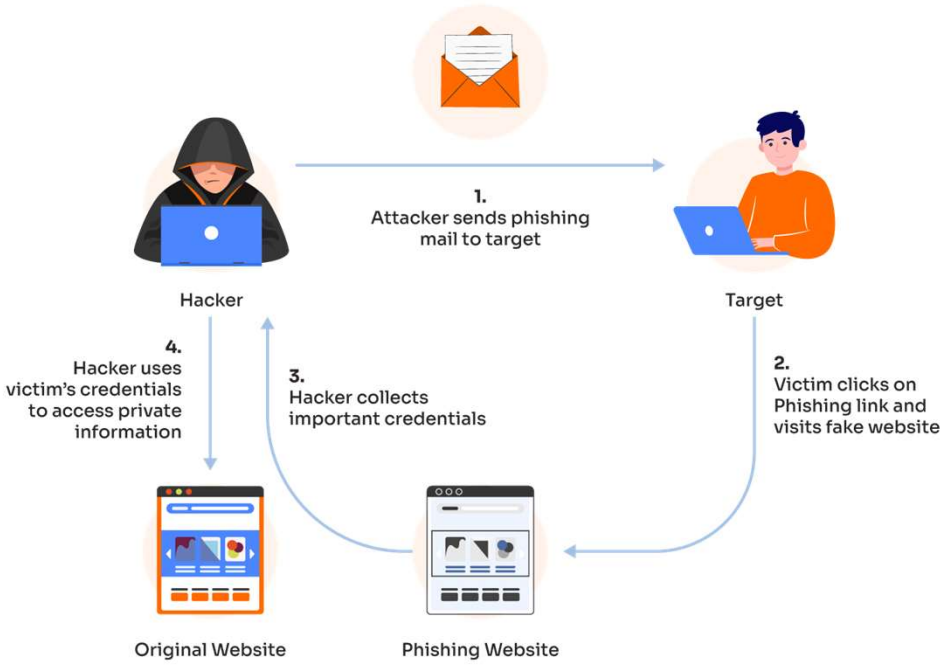
Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user’s behavior. Once an attacker understands what motivates a user’s actions, they can deceive and manipulate the user effectively.

Phishing & phishing website

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions. Some will extract login credentials or account information from victims.

Deceptive phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than it is to break through a computer's defenses. Learning more about phishing is important to learn how to detect and prevent it.



Differentiate phishing & original webpage

1. The Domain Name

First of all, the domain name is the one thing that you need to look at. All the legitimate websites will have at least an https domain name, which means that the protocol that it uses should begin with https. This is especially true for sites that require you to log into your account. On the other hand, the phishing site will only provide you with the http domain name. Their name might also be similar, but with very slight alteration to the letters. For instance, the real site might have an address like https://www.google.com/ while the fake site will have an address like http://www.go0gle.com/. So, take a look carefully at the domain name in the address bar.

2. The Website Security

A good, legitimate, and secure website will usually have a strong security protocol that protects it from various online threats. The SSL security will always exist in any legitimate website that requires your login information. Remember that unless the company is legitimate, the SSL certificate will not be handed to the company since it requires rigorous tests before their application is accepted. Meanwhile, the fake site will not have any security protocol installed on it, thus confirming that the website is not trustworthy. Take a look at the address bar of your browser. If there is a green lock at the left side of the address bar, and you can see that the site is verified by a legitimate security provider, then it means that it is a real website.

3. The Link Sender

Most of phishing websites are “promoted” via spam emails to their victims. They might also be promoted via direct messages in various social media platforms. If you get a link that asks you to log into your account, make sure that the one giving you link is a trustworthy person or company. This is because many people that fall into this trap gave their private information via a suspicious link. Instead of verifying its trustworthiness, they decided to ignore it. So, make sure that you really trust the person or company that gives you the link to the website. If you are asked to log into your account in any website, make sure that the one giving you the login link is the company itself.

4. The Site Design

Another thing that you have to take a look to differentiate between a real website and a phishing website is the overall site design. Of course, a fake website will try to imitate the real one as much as possible, but it will always be imperfect. Even though they can imitate the site design at first glance, they can’t fool the people if they really compare the design of the real and fake website. So, take a look carefully at the site design. If you see something off, then it might be the sign that this is not the real site that you usually use.

5. Available Website Pages

A fake site will never be able to copy the entire web pages of the real one. So, when you visit a suspicious website that resembles a real one, you have to click on various links available in that website. If they cannot display any other pages other than the login page, then it is certainly a fake site. But, if you can browse the website as usual without any problem, then you are dealing with the real one. So, take some time to browse the website and see if you can access the web pages as usual. Otherwise, stay away from that site.

Defend against phishing attacks

1. Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.

2. Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:

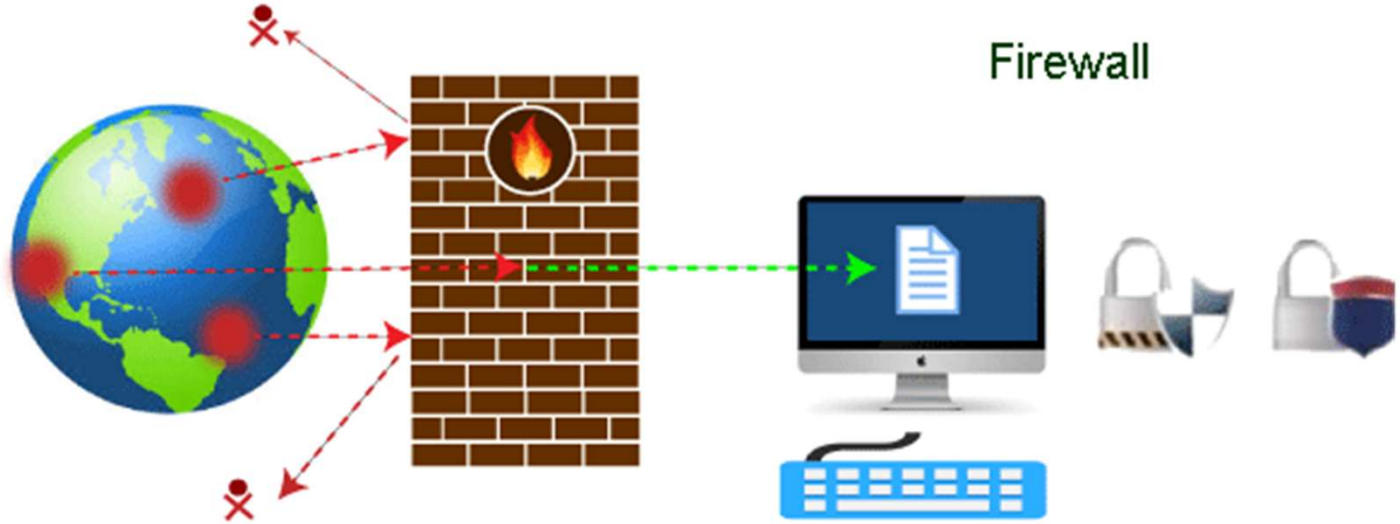
something you know — like a passcode, a PIN, or the answer to a security question.
something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key
something you are — like a scan of your fingerprint, your retina, or your face
Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

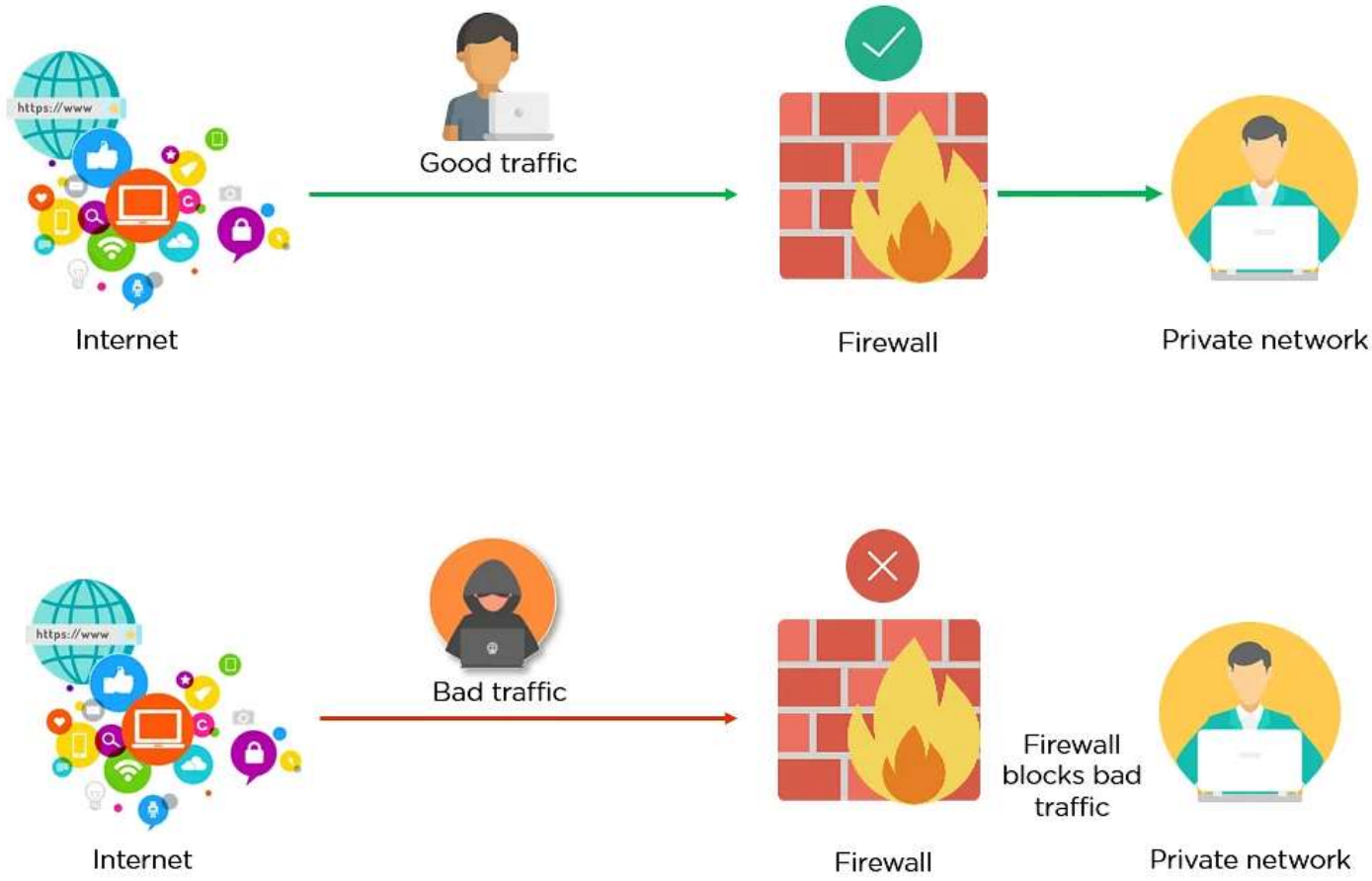
4. Protect your data by backing it up. Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

Firewall

Firewalls prevent unauthorized access to networks through software or firmware. By utilizing a set of rules, the firewall examines and blocks incoming and outgoing traffic.

Fencing your property protects your house and keeps trespassers at bay; similarly, firewalls are used to secure a computer network. Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks.




https://www
Good traffic
Internet
Firewall
Private network
https://www
Bad traffic
Internet
Firewall
Firewall blocks bad traffic
Private network

Functions of Firewalls

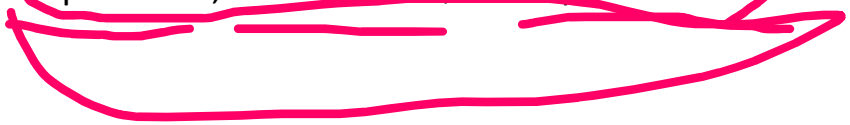
- Firewalls can be used in corporate as well as consumer settings.
- Firewalls can incorporate a security information and event management strategy (SIEM) into cybersecurity devices concerning modern organizations and are installed at the network perimeter of organizations to guard against external threats as well as insider threats.
- Firewalls can perform logging and audit functions by identifying patterns and improving rules by updating them to defend the immediate threats.
- Firewalls can be used for a home network, Digital Subscriber Line (DSL), or cable modem having static IP addresses. Firewalls can easily filter traffic and can signal the user about intrusions.
- They are also used for antivirus applications.
- When vendors discover new threats or patches, the firewalls update the rule sets to resolve the vendor issues.
- In-home devices, we can set the restrictions using Hardware/firmware firewalls.

Types of Firewall

There are mainly three types of firewalls, such as software firewalls, hardware firewalls, or both, depending on their structure. Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.

Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.



Network Address Translation (NAT) Firewalls

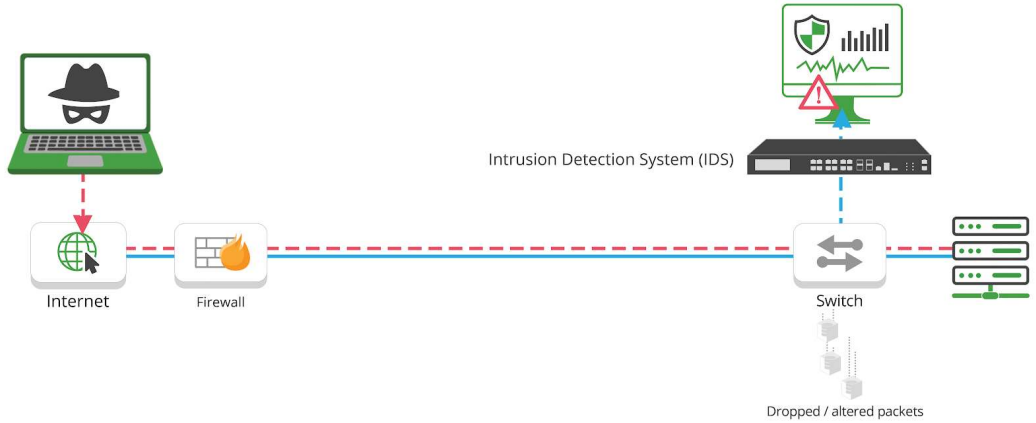
Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.

IDS & its work

Intrusion Detection Systems and firewalls are both cybersecurity solutions that can be deployed to protect an endpoint or network. However, they differ significantly in their purposes.

An IDS is a passive monitoring device that detects potential threats and generates alerts, enabling security operations center (SOC) analysts or incident responders to investigate and respond to the potential incident. An IDS provides no actual protection to the endpoint or network.

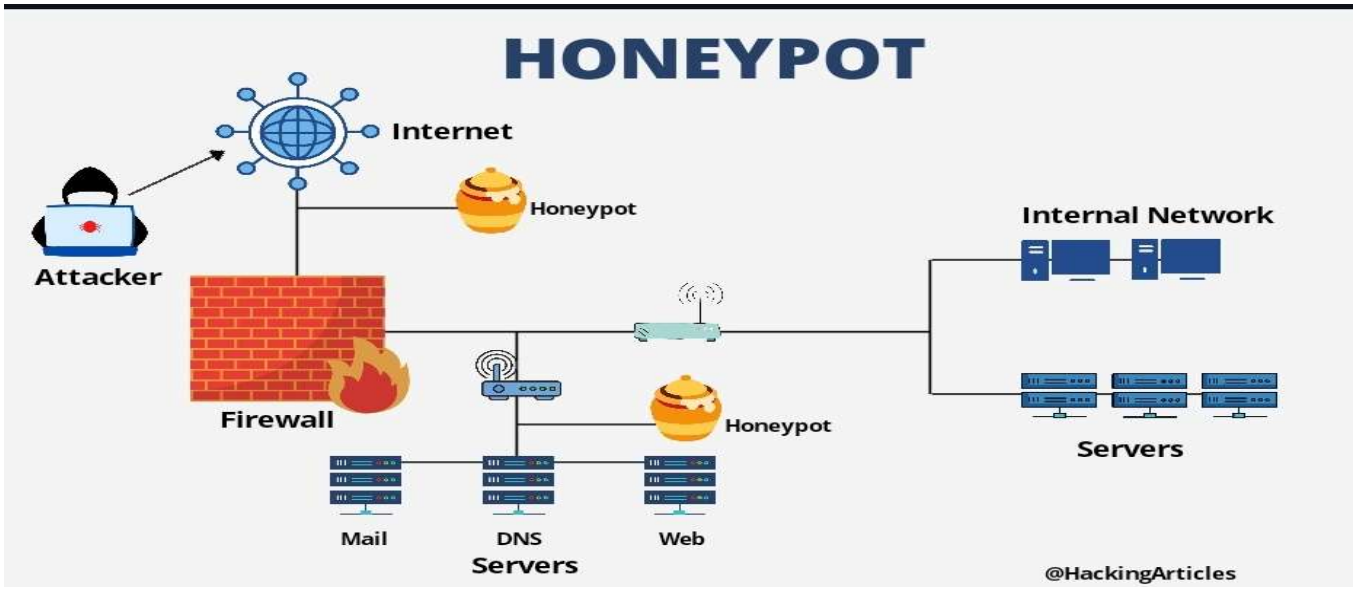
An Intrusion Detection System (IDS) is used for the purpose of detecting malicious network traffic and system misusage that otherwise conventional firewalls cannot detect. Thus, IDS detects network-based attacks on vulnerable services and applications, attacks based on hosts, like privilege escalation, unauthorized login activity and access to confidential documents, and malware infection (trojan horses, viruses, etc.). It has proven to be a fundamental need for the successful operation of a network.



Honeypot

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers.

Honeypots are a type of deception technology that allows you to understand attacker behavior patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cybersecurity measures, because they are unlikely to attract legitimate activity.



kali linux

Kali Linux is a Debian-based Linux distribution that is designed for digital forensics and penetration testing. It is funded and maintained by Offensive Security, an information training company. Kali Linux was developed through the rewrite of BackTrack by Mati Aharoni and Devon Kearns of Offensive Security. Kali Linux comes with a large number of tools that are well suited to a variety of information security tasks, including penetration testing, computer forensics, security research, and reverse engineering.

Uses of kali linux

Metasploit framework

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.