Introduction to IT Security

Topics to be covered:

- Fundamentals of Cyber Security
- Importance of Cyber Security
- Essential Terminologies
- Possible Threats and Attacks
- Associated Risks

Prepared By: Muhammad Farzad Ali | R&D Officer | Sialkot Chamber of Commerce & Industry

When you think of security, what's the first thing you think of?

It's probably

- Physical security
- Stuff like making sure your belongings are safe from potential thieves
- Locking your front doors at night
- Putting your valuables in a safe place.

What is security in Today’s Digital World?

It’s not about protecting your money only. Most of our entire personal world lives on mobile phones.

Here is the list:

- Messages / Voice Notes
- Photos / Videos
- Personal Data (Home address, Identity information and interests etc.)
- Application Logins
- Bank Details
- Client Data
- Confidential Product Information

How can I fight against a Hacker?

Digital thieves don't have a team of hackers and dark hoodies furiously typing into computer terminals all day hoping to break into multi-billion dollar companies. That's not to say that doesn't happen because we all know it does. But most of the time.

The average Internet attacker is someone who looks just like you and me, a regular person who happened to stumble upon a hole in your security system and then took advantage of it. It could have been something as simple as figuring out that you use your dog's name as your password.

Is it still necessary?

Recent attacks like the WannaCry cryptoworm and large scale attacks using the Mirai botnet highlight the scope and scale of how security affects us all.

Because of our widespread dependence on technology, digital security is more important than ever before, and it's going to continue to have a growing impact on all industries and aspects of our lives.

CIA Triad

CIA what does it stands for?

CIA means Confidentiality, Integrity and Availability

"Confidentiality" signifies that data is only viewable by those authorized to view it; "Integrity" denotes that data won't be manipulated or corrupted; and "Availability" means that services remain reachable and available.

These three principles will help you develop security policies in the workplace and for your own personal environments.

Confidentiality means keeping things hidden. One particular method of confidentiality that you probably use everyday is password protection. For confidentiality to work, you need to limit access to your data. Only those who absolutely need to know how to gain access, should.

The I in CIA stands for integrity. Integrity means keeping our data accurate and untampered with. The data that we send or receive should remain the same throughout its entire journey. Imagine if you downloaded a file off the Internet, and the website you're downloading it from, says the file is three megs. Then, when you download it, it turns out to be about 30 megs. That's a red flag.

Let's look at the A in CIA, which stands for availability. Availability means that the information we have is readily accessible to those people that should have it. This can mean many things, like being prepared if your data is lost or if your system is down.

Some security attacks will hold your system hostage, until you pay a ransom for it.

Essential Security Terms

The first one is ***Risk***. The possibility of suffering a loss in the event of an attack on the system.

Next up is the term ***Vulnerability***. A flaw in the system that could be exploited to compromise the system.

There's a special type of vulnerability called a ***0-day vulnerability*** or zero day for short. Which is a vulnerability that is not known to the software developer or vendor, but is known to an attacker.

Another key term is ***Exploit***. Software that is used to take advantage of a security bug or vulnerability.

The next term to know is ***Threat***. The possibility of danger that could exploit a vulnerability.

Next up, ***Hacker***. A hacker in the security world is someone who attempts to break into or exploit a system.

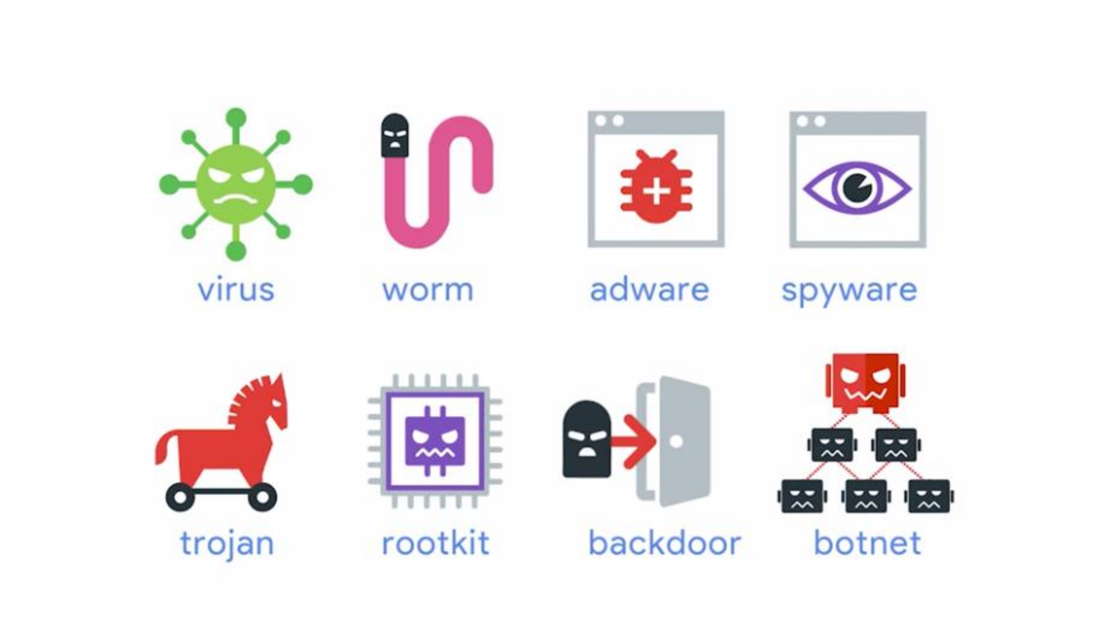
But there are actually two common types of hackers. You have ***black hat hackers***, who try to get into systems to do something malicious.

There are also ***white hat hackers*** who attempt to find weaknesses in a system, but also alert the owners of those systems so that they can fix it before someone else does something malicious.

The last term to know is ***Attack***. Which is an actual attempt at causing harm to a system.

0101010

Common Attacks



Types of Attacks

Malware is a type of malicious software that can be used to obtain your sensitive information or delete or modify files.

Examples : viruses, worms, adware, spyware, Trojans, root kids, backdoors, botnets

Virus:

In a computer virus, the virus attaches itself to some sort of executable code like a program. When the program is running, it touches many files, each of which is now susceptible to being infected with the virus. So, the virus replicates itself on these files, does the malicious work it's intended to do, and repeats this over and over until it spreads as far as it can. Scary, right?

Worms:

Worms are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network. One case of a famous computer worm was the ILOVEYOU or Love Bug which spread to millions of Windows machines. The worm would spread via email.

Adware:

Adware is one of the most visible forms of malware that you'll encounter, most of us see it every day. Adware is just software that displays advertisements and collects data. Sometimes we legitimately download adware. That happens when you agree to the terms of service that allows you to use free software in exchange for showing you advertisements.

Trojan:

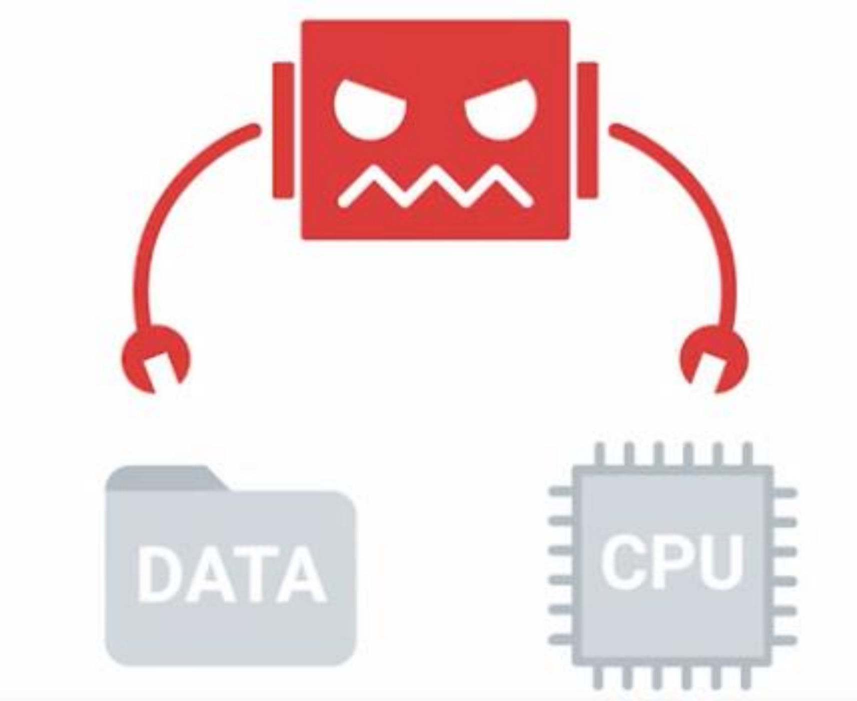
A ***Trojan*** is malware that disguises itself as one thing but does something else. A computer Trojan has to be accepted by the user, meaning the program has to be executed by the user. No one would willingly install malware on their machine, that's why trojans are meant to entice you to install them by disguising themselves as other software.

Spyware:

Spyware is the type of malware that's meant to spy on you. Which could mean monitoring your computer screens, key presses, webcams, and then reporting or streaming all of this information to another party,

Ransomware:

Ransomware is a type of attack that holds your data or system hostage until you pay some sort of ransom.


DATA
CPU

Botnets

There is Malware out there that can utilize someone else's machine to perform a task that is centrally controlled by the attacker. These compromised machines are known as Bots. If there are a collection of one or more Bots, we call that network of devices a Botnet.

Botnets are designed to utilize the power of the Internet-connected machines to perform some distributed function. Take mining Bitcoin, for example, mining Bitcoin requires a machine to perform some computation that takes up your machine's resources. At the end, you may be rewarded with some amount of Bitcoin. A popular attack has been creating Botnets to do stuff like mine Bitcoins. So instead of having one computer run computations, attackers can now have a thousand computers running computations and raking in more and more Bitcoin.

Backdoor

A backdoor is a way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers. Backdoors are most commonly installed after an attacker has gain access to your system and wants to maintain that access. Even if you discovered your system has been compromised, you may not realize that a backdoor to your system exists. If it does, you need to lock it up before more damage can be done.

rootkit

A rootkit by its name is a kit for root, meaning a collection of software or tools that an admin would use. It allows admin level modification to an operating system. A rootkit can be hard to detect because it can hide itself from the system using the system itself.

The rootkit can be running lots of malicious processes, but at the same time those processes wouldn't show up in task manager because it can hide its own presence.

Logic Bomb

A logic bomb is a type of Malware that's intentionally installed, after a certain event or time has triggered, it will run the malicious program.

There's a popular logic bomb case that happened in 2006, wherein unhappy systems administrator at a bank, set off a logic bomb and brought down a company's services in an attempt to drop their stock prices. The former employee was caught and charged with fraud, then sentenced to eight years in prison

Read more at:

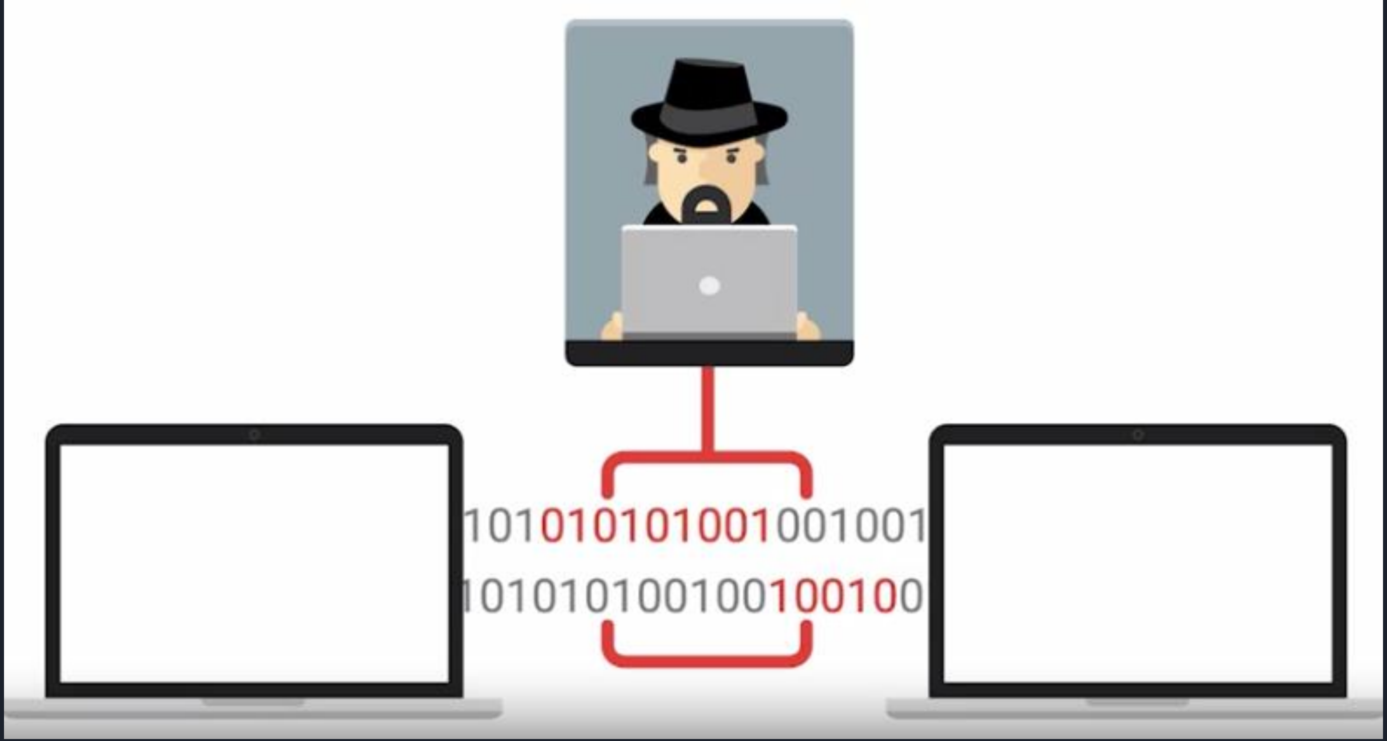
https://www.independent.co.uk/news/business/news/disgruntled-worker-tried-cripple-ubs-protest-over-32-000-bonus-481515.html

Network Attack

A DNS Cache Poisoning attack works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server. It then feeds you fake DNS addresses when you try to access legitimate websites. Not only that, DNS Cache Poisoning can spread to other networks too. If other DNS servers are getting their DNS information from a compromised server, they'll serve those bad DNS entries to other hosts.

A man-in-the-middle attack, is an attack that places the attacker in the middle of two hosts that think they're communicating directly with each other.

Man in the Middle

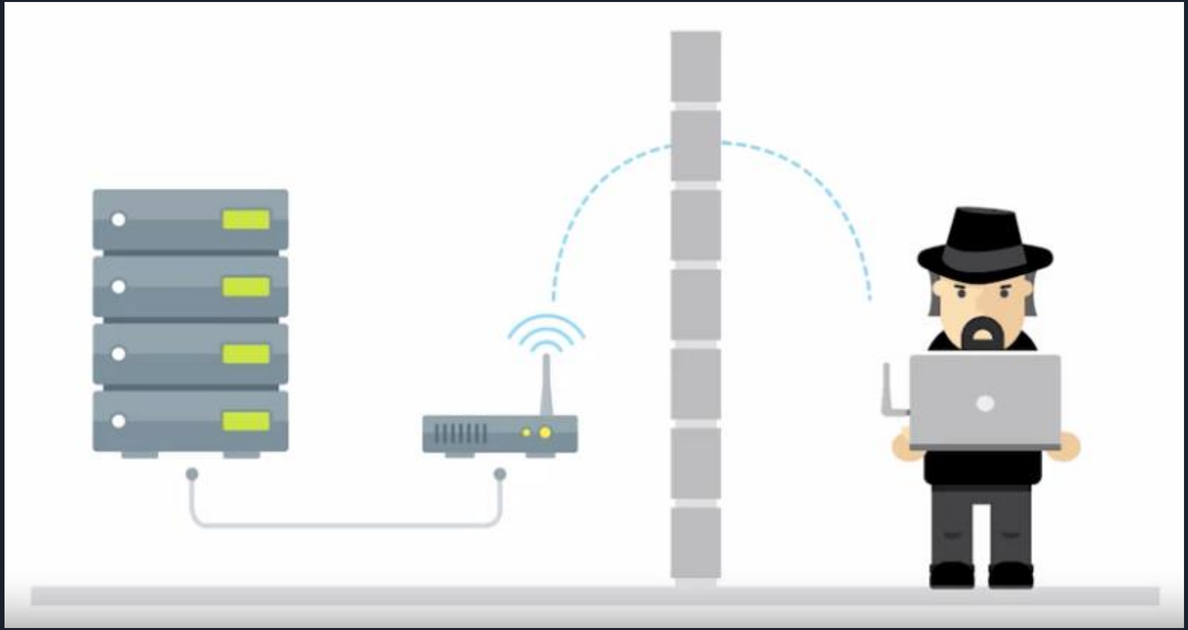


Man-in-the-middle Attack

A common man-in-the-middle attack is a session hijacking or cookie hijacking. Let's say you log into a website and forget to log out. Now, you've already authenticated yourself to the website and generated a session token that grants you access to that website. If someone was performing a session hijacking, they could steal that token and impersonate you on the website,

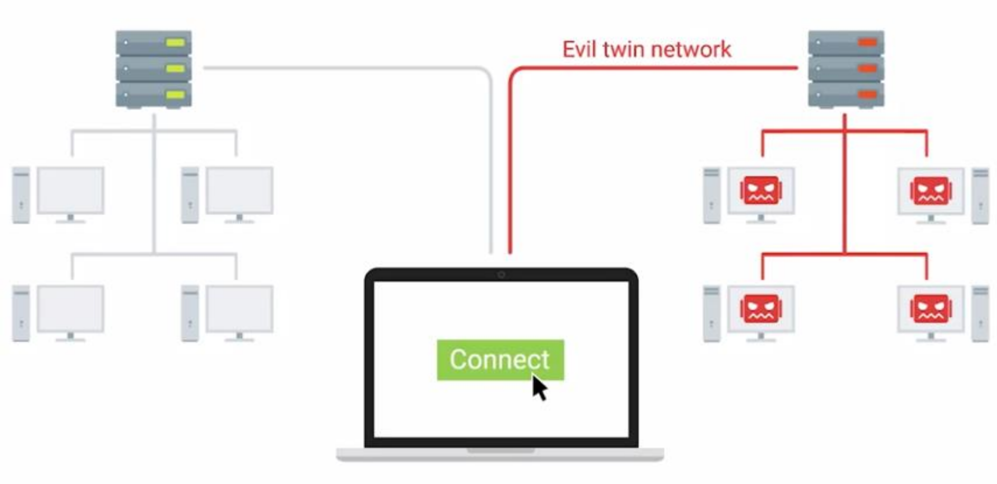
Another way a man-in-the-middle attack can be established is a rogue access point attack. A rogue AP is an access point that is installed on the network without the network administrator's knowledge. Sometimes, in corporate environments, someone may plug a router into their corporate network to create a simple wireless network. Innocent enough, right? Wrong. This can actually be pretty dangerous, and could grant unauthorized access to an authorized secure network. Instead of an attacker having to gain access to a network by plugging directly into a network port, they can just stand outside the building and hop onto this wireless network.

Rogue AP



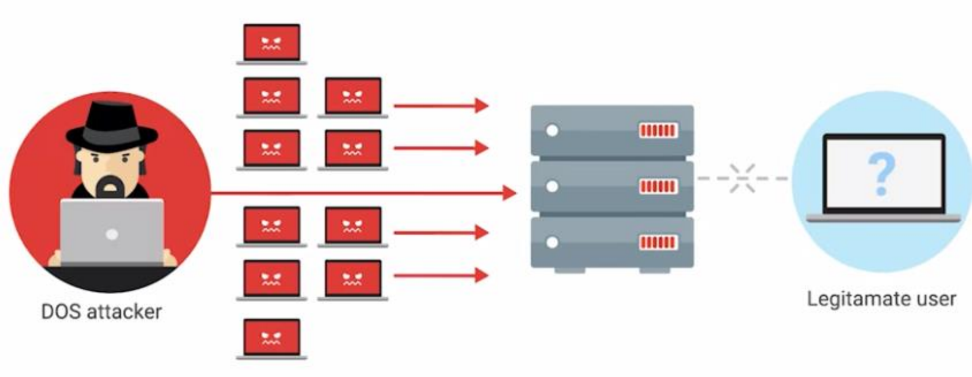
Evil Twin

A final man-in-the-middle method will cover is called an evil twin. It's similar to the rogue AP example but has a small but important difference. The premise of an evil twin attack is for you to connect to a network that is identical to yours. This identical network is our networks evil twin and is controlled by our attacker. Once we connect to it, they will be able to monitor our traffic.



Denial of Service

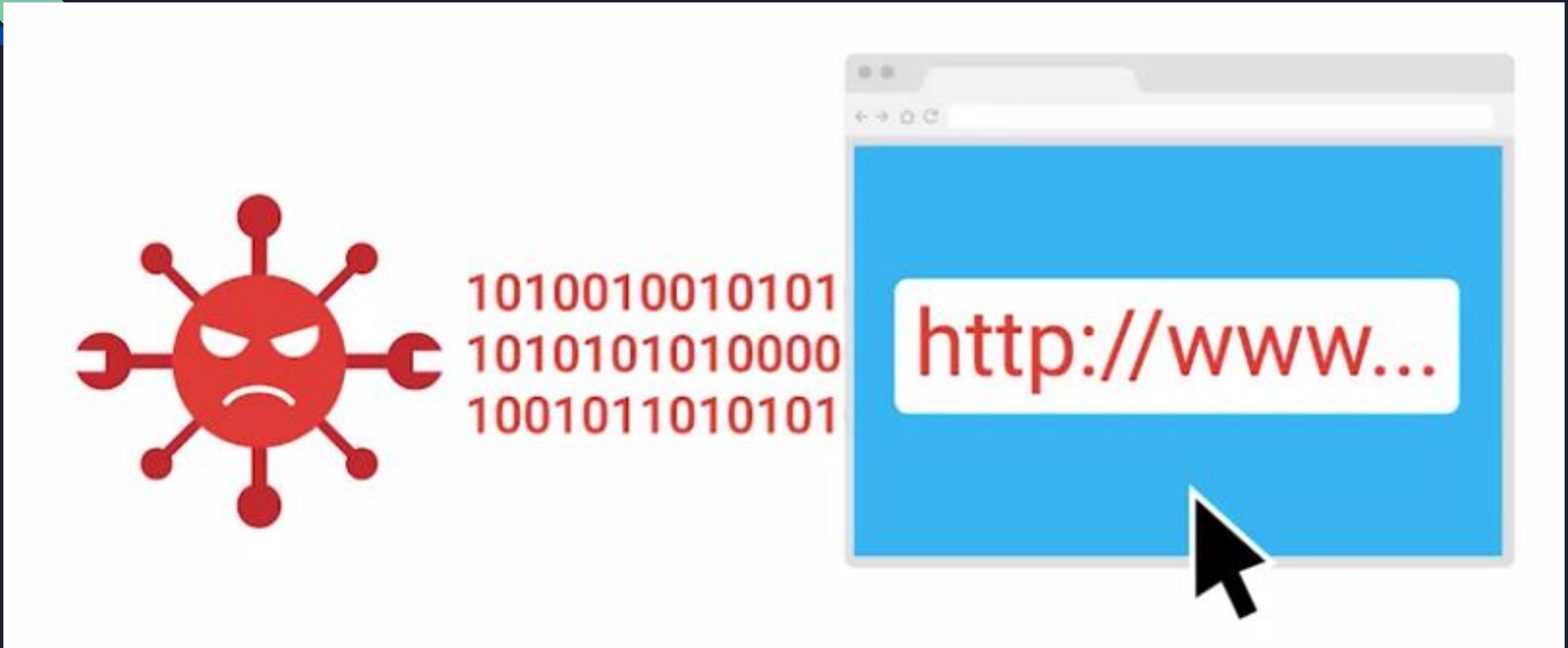
A Denial-of-Service, or DoS attack, is an attack that tries to prevent access to a service for legitimate users by overwhelming the network or server. Think about how you normally get on a website. Most major websites are capable of serving millions of users. But for this example, imagine you have a website that could only serve 10 users. If someone was performing a Denial-of-Service attack, they would just take up all 10 of those spots, and legitimate users would have been denied the service, because there's no more room for them.



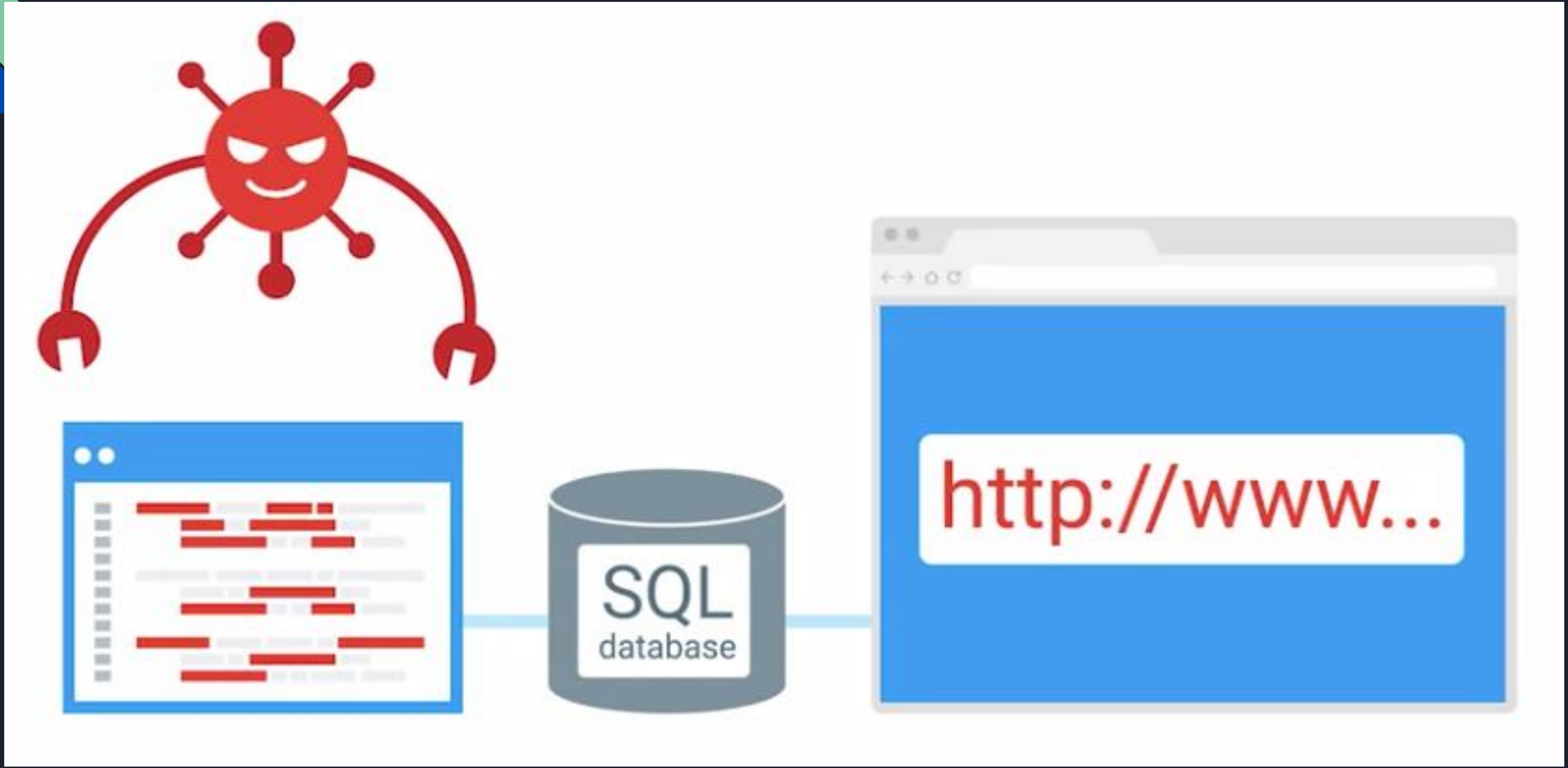
Other Attacks

Cross-site scripting, or XSS attacks, are a type of injection attack where the attacker can insert malicious code and target the user of the service. The script could then do malicious things like steal a victims cookies and have access to a log in to a website.

Another type of injection attack is a SQL, or S-Q-L, injection attack. Unlike an XSS that targets a user, a SQL injection attack targets the entire website if the website is using a SQL database. Attackers can potentially run SQL commands that allow them to delete website data, copy it, and run other malicious commands.


10100100010101
1010101010000
1001011010101
http://www...

10101010101
01010110101
****


SQL
database
http://www...

Password Attack

Password attacks utilize software like password crackers that try and guess your password. And they work extremely well, so don't try to reuse that fido password. It didn't secure your bank account and it's not going to work here. Okay, moving on. A common password attack is a brute force attack, which just continuously tries different combinations of characters and letters until it gets access.

Have you ever seen a CAPTCHA when logging into a website? CAPTCHAs are used to distinguish a real human from a machine. They ask things like, are you human, or are you a robot, or are you a dancer?

Don't include real words you would find in a dictionary and make sure to use a mix of capitals, letters, and symbols.

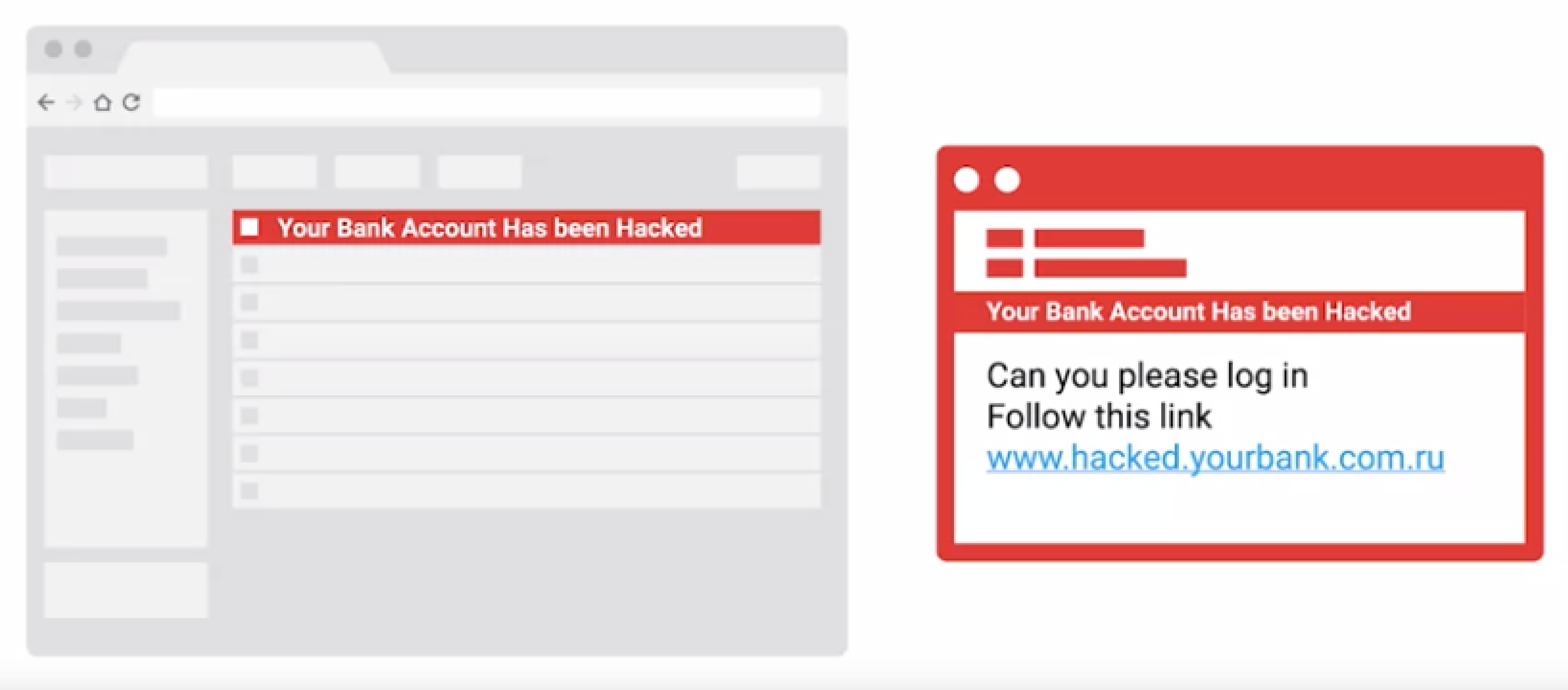
Deceptive Attack

Social engineering is an attack method that relies heavily on interactions with humans instead of computers. You can harden your defenses as much as you want. You can spend millions of dollars on State of the Art Security Infrastructure. But if Susan the systems administrator has all the access to your system, and gets tricked into handling over her credentials, there's nothing you can do to stop it.

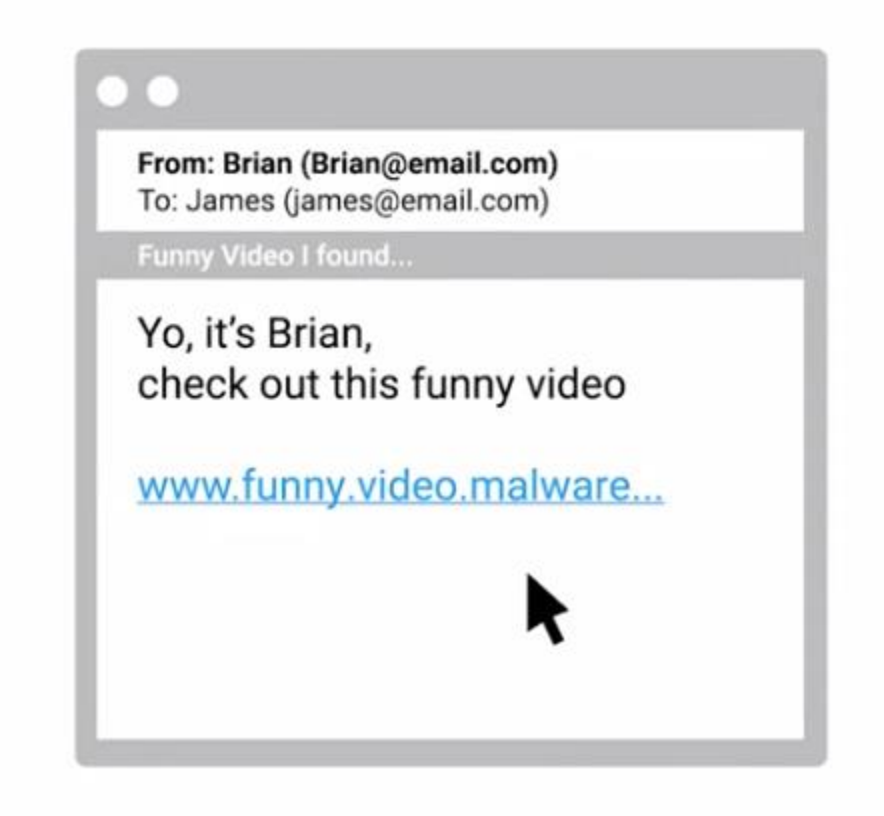
A popular type of social engineering attack is a phishing attack. Phishing usually occurs when a malicious email is sent to a victim disguised as something legitimate. One common phishing attack is an email, saying your bank account has been compromised. And then, gives you a link to click on to reset your password. When you go to the link, it looks like your bank's website but it's actually a fake website.

user
****

Phishing attack


Your Bank Account Has been Hacked
Your Bank Account Has been Hacked
Can you please log in
Follow this link
www.hacked.yourbank.com.ru

Email Spoofing



From: Brian (Brian@email.com)
To: James (james@email.com)

Funny Video I found...

Yo, it's Brian,
check out this funny video

www.funny.video.malware...

Thank You.