assemble you

Introduction to Malware

Brought to you by Assemble You.

It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

Today we are discussing malware. We've all fantasized about throwing our computer or laptop out of the window. It could be the system suddenly slowing down, or it might be encountering unusual errors and crashes. It's pretty common to discover unrecognized programs installed on our system. But is it okay? Well, not really. Even though a system can slow down, a sudden slowdown or the discovery of software you can't explain should alert you. These issues can be indicative of malware on your system.

So, what is malware, and why should we be worried about it?

Malware is a portmanteau, a combination of the words – "malicious" and "software." It's malicious software that is designed to cause harm to a system. It could be simply deleting data or, even more perniciously, hiding like a spy in the system, monitoring our activities. It can capture your keystrokes and send them to the person, the hacker, who planted the malware in our system. This means that if we are entering a password somewhere, let's say in our online bank account, that person controlling the malware also gets to know it. Almost everything is visible to the hacker: our data, confidential files, photographs... almost everything.

Sounds scary, right? It is, but that doesn't mean we're helpless. Over the next few minutes, we'll go through some of the different types of malware and what you can do to protect yourself against them.

Malware itself is not an entity but a broad term often used interchangeably with "virus." Many of us would call all malicious software **either** malware **or** virus, but this isn't accurate. A virus is just one subset of malware.

We need to understand each type to differentiate between them, as they all have unique characteristics.

So, let's take a look at them, starting with...

Virus

A virus alters the behavior of an existing application. When a virus does this, the existing application may start behaving strangely. For example, suppose a Word file is infected with a virus. The virus won't execute until we open the file. Once it is opened, the virus triggers itself. The result may be for the virus to add random text or delete the existing file content.

Next up, the worm.

A worm is another variant of malware that crawls from one system to another. It uses email or file sharing to traverse through a network. For example, if a malicious attachment comes via email and we double-click to open it, the worm is triggered. It will then start replicating itself on the network, infecting as many systems as possible. Unlike a virus, it does not cause any damage to the data, but it can slow down the network performance.

Onto the next type of malware, the Trojan.

In the famous story, the Greek army laid siege to the city of Troy for 10 years. Eventually, one morning the Greek troops retreated from their camp, leaving a large wooden horse outside the gates of Troy. After much debate, the Trojans pulled the mysterious gift into the city. When night fell, the horse opened up, and a group of Greek warriors climbed out and sacked the Troy from within.

So, as you might expect, a ***Trojan*** horse in computing is any malware that misleads users of its true intent. It disguises itself as a regular program, and when clicked, it triggers to cause damage, like deleting data.

Another form of malware is Keyloggers.

We almost all need type to use our systems, and hackers are desperate to know what we're typing. They aim to acquire sensitive information, such as passwords, by capturing keystrokes using a keylogger. Every key that is pressed, the keylogger captures and sends to the hacker. For example, suppose we enter user credentials to log on to our bank account. In that case, the keylogger will capture all the keystrokes and send them to the hacker. This means your user credentials are now known to the hacker.

Moving on from keyloggers, another type of malware is spyware

Hackers watch our activities on a system by planting spyware on our system. Spyware tracks every action we perform and reports it to the hacker. Spyware can also be designed to steal data and gather sensitive and confidential information. For example, it will send copies of your files to the hacker.

Ransomware is next on the agenda.
A ransom is a demand made by a criminal in exchange for a captive or a hostage. In computing, the ransom is demanded not for the captive but for the system and its data. A hacker can encrypt our files using ransomware and demand ransom. The hacker encrypts the files, and they can only be decrypted with the decryption key that the hacker has. Even once we've paid the ransom, the hacker may or may not decrypt the files. We can never be sure.

Next on the agenda is backdoor malware.
When programmers develop software, they usually want an easy way to get into an application. To do this, they leave a backdoor opening into the applications. Hackers use this method to get an easy entry into the system.

For a hacker, it is difficult to hack into a system again and again. The easiest method is to hack once and leave a backdoor. That allows them to go in and out of the system without problems.

Logic Bomb
A logic bomb works on predefined conditions, such as time or date. It may exist in the system but triggers only when predefined conditions are met. For example, a hacker may create a small script executed at a specific date and time. Once executed, it can cause severe damage, including inflicting harm via file deletion. One of the most famous logic bombs attacks was The Siemens Corporation spreadsheet debacle. It involved contract employee David Tinley, who provided software to Siemens' Monroeville PA offices. He was a trusted employee for nearly a decade and would create spreadsheets to manage equipment orders. However, Tinely planted a logic bomb within one of the spreadsheets. The bomb went undetected for two years. Whenever a script would malfunction, Siemens would have to call Tinley, who would "fix it" for a fee. However, the scheme eventually ended when Tinley was out of town and gave the spreadsheet password to Siemens' IT staff during another crash. The logic bomb was found, and Tinley pled guilty in May 2019.

Moving on from the logic bomb attack, we have the Fileless Virus.
Almost all types of malware exist in the form of some file. Fileless malware, on the other hand, exists only in a computer's random-access memory (RAM), meaning that nothing is ever written directly to the hard drive. This makes it more difficult to detect as there are no stored files for defensive security software to scan. It becomes even more difficult if forensic processes are performed on the system. Since memory is volatile and does not retain information, then if the system is rebooted, the fileless virus disappears.

All of this is why, as reported by the Ponemon Institute, 77% of all breaches in 2017 used fileless techniques, which are also ten times more likely to succeed than file-based attacks.

Protecting Yourself

So, now we know the different types of malware. But how do we safeguard ourselves?

One of the most straightforward tips is to avoid opening attachments from unknown email senders. If you receive an email about million-dollar prize money and need to download the attached PDF file, remember that no one gives out a million dollars for free! The attached PDF file is likely infected with malware, so don't open it.

Our next tip is to keep your systems and applications updated. You should also install only legitimate and licensed programs to avoid licensing and malware issues.

Next, ensure that you have a SPAM filter on all incoming emails.

Finally, your systems must be equipped with a firewall with rules configured to filter the incoming and outgoing traffic.

Other than this, we should have antimalware or antivirus programs installed with the updated signatures. A virus signature (also known as a virus definition) is **a file or multiple files downloaded by a security program to identify a computer virus**. The files enable malware detection by the antivirus (and other antimalware) software in conventional file scanning and breach detection systems. Remember that antimalware is only effective if updated with the latest signatures. Every day, thousands of malware get released, and therefore, the antimalware or antivirus vendors keep releasing the updates regularly.

So, that's a lot of information to digest. But now is time to take action. Check your system and determine whether you have an antivirus or antimalware installed. If there's an update available, install it.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] Malware: Difference Between Computer Viruses, Worms and Trojans
- [Video] 10 Signs of Malware on Computer | How to Know if you're Infected?
- [Video] 6 Signs Your Computer Is Affected By Malware, Spyware, Or Virus
- [Article] Introduction to Malware: Definition, Attacks, Types, and Analysis
- [Article] Fileless Malware, Awake Security
- [Article] Malware | What is Malware & How to Stay Protected from Malware Attacks

assemble
you

Introduction to Social Engineering

Brought to you by Assemble You.
It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

What does "Black Friday" mean to you? For millions of people, it's the biggest shopping day of the year. But it's also a very clever piece of marketing. We all fall victim to the time pressure that 24-hours-of-low-prices thrusts upon us, and many of us save specifically for it. This 24-hour time pressure is not the only strategy deployed by marketers, either. There are always news stories and viral videos showing people camping outside stores to get inside first and desperate people physically fighting over flat-screen TVs. But this colossal fear of missing out on amazing deals is artificial and very much intentional. Creating a fear of missing out - or FOMO as it's often shortened to - is a specific, deliberate strategy.

Black Friday is an example of what's called "social engineering." It is the art of manipulating human behavior to get someone to do something.

In cybersecurity specifically, though, social engineering implies something more menacing.

In his book *How to Hack a Human: Cybersecurity for the Mind*, security expert Raef Meeuwisse defines social engineering as

> *...the act of constructing relationships, friendships or other human interactions for the purpose of enticing the recipient to perform an inadvisable action or reveal secret information.*

In cybersecurity terms, this means preying on our emotional responses to make us voluntarily compromise our own security.

Today, we'll learn about social engineering attacks, the standard techniques used in them, and how we can protect ourselves against them.

Security vendor PurpleSec claims that 98% of cyber attacks use social engineering. Hackers need a vulnerability to start their security breach - most frequently a human. In *Secrets and Lies: Digital Security in a Networked World*, Bruce Schneier writes that

> *People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.*

Bad actors exploit people by tricking them into doing something they want them to do using various methods. Once a barrier is removed via social engineering, hackers have a way into a system or a network to steal confidential and sensitive information.

A prominent example of successful social engineering is the US Department of Justice's data breach in 2016. 200GB of confidential data was exposed after a hacker successfully impersonated a staff member. A compromised internal email address and some basic deception allowed the attacker to convince other staff to provide full access to internal files.

This is an excellent example of how damaging even the simplest social engineering techniques can be.

The DOJ example seems laughable, but it's easy to be misled. Have you ever received a text or email claiming that "your parcel was undeliverable" which included a code that looked legit? Delivery scams are big business - Caleb Barlow, vice president for IBM Security says it's a $445 BILLION scam.

Maybe you've received an email stating that your bank account is locked because of various unsuccessful login attempts. The email also contains a link to unlock the account or reset the password. When an email scam is well-designed, most of us would simply click on the link that the hackers wanted. When we visit the website, a perfect replica of the actual bank website, we enter our credentials. The hackers on the other side receive your login credentials. Alternatively, clicking on that link can drop malware onto your system, which can pass on a lot of information from your system to hackers. That's their successfully executed first step. This is an example of a specific technique - **trust** - in action.

It's not the only technique. So, let's quickly learn about some more.

The next is **authority**.

With this, the hacker pretends to be someone with authority, such as a police officer. They use that authority to get information from the target. For example, the hacker pretending to be a police officer may call the CEO's assistant and ask for the CEO's mobile number and email address. If the assistant refuses, the hacker can pressurize and threaten consequences for non-cooperation until the receptionist eventually complies.

Another technique is **urgency**.

With this approach, the hacker creates a sense of urgency for the target. It's done via email or through a phone call, and the target is given no choice to think but instead forced to act quickly. For example, the hacker may call a target to get their user credentials under the pretense of helping them to reset their password. The hacker can inform the target that the organization's user accounts have been leaked, and before any user account is compromised, the passwords need to be reset. The target may simply reveal the password, as they're under the illusion that the clock is ticking.

The final technique we'll discuss is **intimidation**. Suppose your boss had a presentation to prospective investors coming up, and you received a phone call. On the other end, someone claiming to be with your boss says his files - including a confidential revenue file - are corrupt, so you need to email them immediately. Perhaps you'd decline initially, but the bad actor could intimidate you by saying something like, "Look, if you want to be responsible for this six-figure opportunity falling through, that's okay. I'll tell him you refused to help." The hacker has created a situation where you feel trapped and afraid of the consequences.

Using one of these techniques, hackers conduct various attacks in social engineering. We need to understand each type to differentiate between them, as they all have unique characteristics. So, let's take a look at them, starting with phishing.

Phishing is considered the most common type of social engineering attack. It is performed via email with spoofed email addresses containing a specific message in the body text. For example, it can talk about a locked bank account or the recipient winning a million-dollar through a lottery. The email body also contains links to trick the recipient into providing personal information, such as a credit card or social security number. The email might even ask you to reset your password by clicking on a link.

So, why do hackers rely so heavily on phishing to conduct security breaches? The answer is simple – they only need an email address to send out a phishing email, and email addresses can be easily acquired with ea. Astonishingly, in 2020, **75% of companies** globally were phishing victims.

Recent data on hostingtribunal shows that 60% of the companies lost data in phishing. In comparison, 52% had been compromised with the user credentials. Another 29% ended up with malware infection, which damaged their networks.

Next up, the whale phishing.
It is a type of phishing attack. Think of catching the big fish in the ocean – this is what symbolizes the whale phishing attack. The hackers go after the top executives in an organization to get confidential information. They use the same method of sending out a phishing email but only to the senior executives. For example, a spoofed email from the CEO is sent to the Chief Financial Officer (CFO) with the latest revenue and profit information.

Similar to whale phishing, spear phishing is another type of phishing attack. Whereas a normal phishing attempt may be sent to many email addresses, a spear-phishing attack is more targeted.

Another type of social engineering attack is tailgating, and it's a bit more old-fashioned.

Have you ever walked through a door behind someone without flashing your ID badge? The first person flashed the ID badge to unlock a door, but you conveniently followed your colleague right through the door. Well, this is tailgating. Tailgating relies on common courtesy and people's natural tendency not to challenge others.

Next up is baiting.
We have all seen the free giveaways via internet ads, emails, or even television ads. Hackers use baiting to exchange confidential information for something valuable. For example, a hacker may offer money or even a gift card to complete a survey hosted on a spoofed website. When we log on to this website thinking it's legitimate, the hacker captures the user credentials

The final type of social engineering attack is a honey trap.
A hacker convinces the victim about romantic feelings. When the victim is convinced, the hacker convincingly gains the information. According to the FBI, romance scammers defrauded Americans out of $1 billion in 2021.

So, now we know the different types of social engineering techniques and attacks, let's get onto how we safeguard ourselves.

It is nearly impossible to stop social engineering attacks from happening. However, several methods can significantly reduce the chances of falling victim to one.

The first method is **training**.
Everyone in an organization should undergo a basic level of security training. Employees should know about social engineering and specifically phishing attacks. Not everyone needs to be a security expert, but fundamental knowledge can prevent security breaches.

The next one is the **restricted access privileges**.

Users within an organization must be assigned permissions on a need-to-know basis. That way, even if the hacker can get into the system, though this method won't protect the data on the network, it will delay the process.

Two-factor authentication is another imperative measure we must take.
In most cases, hackers are after user credentials, which they later use to exfiltrate and steal information. With two-factor authentication in place -even if hackers get the user credentials of a target - they still require the second factor, be it a PIN, One-time Password, or even a smart card.

Another critical method is **security policies**.
Security policies are used to define the security posture of an organization. The security policies should focus on passwords, training, and infrastructure. For example, a password policy should drive the users to use complex passwords and change them after a certain number of days.

Last but not least, **social engineering campaigns**.
These are good to verify the knowledge of social engineering of the users within the organization. The outcome of a social engineering campaign can help you further train the users. You can also conduct a phishing simulation with the users and determine the number still falling for social engineering.

So, that's a lot of information to digest. But now is time to take action. This week, we'd like you to think about your passwords - are they easily guessable if somebody got to know you? Do you use Two-Factor Authentication? If not, we strongly encourage it.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] What is Social Engineering?
- [Video] The Science Behind Human Hacking (Social Engineering) - Christopher Hadnagy
- [Video] The Dark Arts of Social Engineering – SANS Security Awareness Summit 2018
- [Article] What is Social Engineering?, Kasperksky
- [Article] Social Engineering - It’s Not Just About Phishing, K. Townsend
- [Article] Social Engineering Principles, D. Gibson
- [Infographic] Social Engineering and How to Win the Battle for Trust
- [Book] Secrets and Lies: Digital Security in a Networked World, B. Schneier
- [Book] How to Hack a Human: Cybersecurity for the Mind, R. Meeuwisse

assemble you

Using and Managing Passwords

Brought to you by Assemble You.

It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

Today we are discussing using and managing passwords.

Your house often contains the most valuable possessions you own. Family heirlooms, pictures of your family, jewelry, and whatever else. Would you leave the front door open to allow anyone to walk in and take those valuable items? What about if you knew thieves were prowling? Would you lock up then?

People go to great lengths to protect their homes. They have neighbors open and close the curtains and turn lights on and off while they vacation. Buying locks, motion-sensitive lights and alarm systems, and intimidating guard dogs.

So, why are we so willing to forego this level of security online? Where we do our banking. Where we shop for things. Where we have some of our most confidential conversations. 123456 is the most popular password on the internet. 123456!! According to Schneider Downs, it's used by 103 million people. And it can be compromised in less than a second.

Even Meta CEO Mark Zuckerberg has fallen prey to his own lazy password maintenance. Around 80% of people reuse their passwords across sites, and Zuckerberg proved to be no different when his Twitter account was hacked in 2018. Zuckerberg had been a victim of a LinkedIn data breach. The weak password he used across social media - *dadada* - had been compromised and used to access his profiles.

Perhaps when the threat is non-physical, we feel less pressure to protect ourselves - "what we can't see won't hurt us" type of thing. Make no mistake, this is a grave error.

Thankfully though, through just a little bit of diligence and effort, we can go a considerable distance to ensuring we're protected.

Hackers don't have to guess your password manually. They use different methods and tools to automate the entire process and discover the actual password. This is why we must use a secure password - one that's lengthy and complex.

Passwords are low-hanging fruit for hackers, as password attacks are more straightforward than other attacks. To conduct them, hackers use different methods - let's look at some of them.

The first method - **phishing** - is the most common example of what we call a social engineering attack.

Using a spoofed email address, a hacker sends you an email. The email body is intended to trick you into providing personal information, such as a credit card or social security number.

The email might even ask you to reset your password by clicking on a link. Via this link, you're redirected to a fake website, a replica of an actual company, such as a bank. The moment you enter your credentials, they are captured by the hacker in the background. Recent data on Hosting Tribunal shows that 52% of organizations had been compromised this way.

Next up is the **brute-force** attack.
Using specialized tools, hackers use every possible combination of allowable characters. That includes lowercase and uppercase letters, numbers, and special characters. The tool will run and attempt to create a password, and it will continue to run until it finds the correct combination. Such a tool makes thousands of guesses per second to speed up the process.

A subset of the brute-force attack is the **dictionary** attack.
Remember the '123456' password? Earlier, we mentioned that it takes less than one second to break this password. Hackers use "dictionaries," which, as you'd imagine, are lists of millions of words. They run the dictionary entries against a website to detect the passwords within seconds. But the dictionary in these types of attacks isn't limited to single words - it can also be a collection of previously leaked passwords or keyphrases. Given that it appears first alphanumerically and is incredibly popular, 123456 will be guessed immediately.

So, if it's not your bank account, is it still a big deal if your details are compromised? YES. Suppose somebody got ahold of your Facebook or Instagram password. They log on and change the password, the registered mobile number, and the address. Your long friend list and your extensive gallery of photos are gone. You've now lost access to the account, and the chances are you won't get it back.

Protecting Yourself
So, how do we prevent that? How do we safeguard ourselves? Here are several tips that we can use to secure our passwords.

The first tip is to **stop sharing your passwords**.

Using social engineering techniques, a hacker might pretend to be from the technical support team and ask you to share your password. Never share it.

Passwords are like house keys, except when you get the house keys back, you don't need to change the locks. When somebody appears to have finished with your password, they still know it. Effectively, they still have the keys until you change the locks. And if you give the wrong person your keys, they'll get inside and change the lock themselves.

The second critical tip is to **avoid repeating passwords**.
We should always use different passwords for different websites. Multiple points of security ensure that if one is compromised, we are still safe with the others. Most users, just for the sake of convenience, use the same password across websites. The problem is that most of us aren't aware if our passwords from one website have been breached, so we're careless. Therefore, it is critical to use different passwords on different websites. You can check whether you've been compromised by typing your email address into Have I Been Pwned?. If so, ensure you update your passwords immediately.

You should also be using **two-factor authentication.**
In most cases, hackers are after user credentials, which they later use to exfiltrate and steal information. Even if hackers get your credentials, they still require a PIN, One-time Password, or even a smart card with two-factor authentication.

You should be aiming to **use complex passwords that avoid using dictionary words, names, places, or birth dates**. Short passwords and passwords made from actual words can often be cracked within minutes. You can actually check the time it takes to break a password on PasswordMonster, though we recommend NOT checking your own **real** password there. But, let's test a random single word, in this case, a name - 'JOSEPH.' As per PasswordMonster, it would take **less than a second** to crack this password. Let's consider another password, 'JCRJSW,' which is random but the same length. It would take PasswordMonster about **24 days** to crack. If we extended it to 'JCRJSW1100', it would take **17 centuries** to break! So, the strength of your password depends on its length and how random it is. A good rule of thumb for a great password is to aim for a total of 16 letters, numbers, and special characters.

The final tip is about the **use of password managers**.
When we create complex, lengthy passwords, we have difficulty remembering them. For the sake of convenience, some of us write the password on a piece of paper or in a diary. That's bad practice. Anyone who gets their hands on the piece of paper or diary has

access to the passwords as well. It's also too easy to lose those things. We should use a password manager to resolve this situation, such as LastPass. We not only get to save all our passwords, but we also lock the password manager with a master password. Instead of remembering 20 passwords, we need to remember the master password.

Password managers also allow us to copy the password and paste it into the password field if a website allows it. This prevents us from typing the password, which can be captured if a keylogger is installed on the system. Since we are not typing the password, the keylogger does not detect the password.

Additionally, when we need to generate a complex password, we can use a password manager, which can generate a long, complex password for us to use.

So, that's a lot of information to digest. But now is always the best time to take action.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] watch how a PRO Hacker Hack and Crack Passwords!
- [Video] This is How Hackers Crack Passwords!
- [Video] Generating Rainbow Tables With RainbowCrack
- [Article] Impressive Password Statistics to Know in 2021
- [Article] What Are The Most Common Passwords of 2021?

assemble
you

Common Types of Attack

Brought to you by Assemble You.

It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

Nowadays, most of our work involves the Internet, making us vulnerable to bad actors and invisible enemies.

These enemies conduct cyberattacks – sometimes on networks and systems,but adversaries have discovered it's much easier to hack a human. Today, we'll discuss some of those attacks, as well as how to protect ourselves against them.

PurpleSec researchers discovered that in the United States alone in **2019**, **164.68 million** sensitive records were exposed through **1473 attacks**. The average cost of a data breach resulting from these attacks was **$3.92 million**. Hacking is big business, and - directly or indirectly - we're all potential victims.

There's a very high chance your passwords have been compromised in data breaches. Hackers sell this data, use it to conduct social engineering attacks, and even use it for identity theft. In fact, in 2020, consumers lost over 56 BILLION dollars to identity theft.

Hackers conduct cyber attacks to steal information, sabotage one or more systems, or bring down a working network. They can also attack several systems at once, gain control, and use these systems to initiate another attack on a different network altogether. Hackers conduct various types of attacks, but today we'll focus on:

- social engineering
- malware
- ransomware
- distributed denial of service
- Man-in-the-middle (MITM) attacks

- insider threats
- credential reuse
- And mobile attacks

So, let's begin with social engineering attacks. Cybersecurity expert Bruce Schneier once said, ***"Amateurs hack systems; professionals hack people."*** You may feel that your data is safe once you've activated firewalls and downloaded antivirus software, but you'd be wrong. Hackers can bypass your defenses by taking a non-digital approach. In his book *Secrets and Lies: Digital Security in a Networked World,* Schneier says

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

Hackers use diverse methods to trick subjects into acting. Once the action is performed, they have a way into a system or a network. From there, they are free to steal confidential and sensitive information.

Phishing utilizes email and is the most common social engineering attack. For example, it involves an attacker, masquerading as a trusted entity, duping a victim into opening an email, instant message, or text message. The email often contains links to trick the recipient into providing personal information, such as a password, credit card number, or social security number.

Then, the next attack is **malware**.
Malware is a portmanteau, a combination of the words – "malicious" and "software." It's malicious software that is designed to cause harm to a system. It could be simply deleting data or, even more perniciously, hiding like a spy in the system, monitoring our activities. It can capture your keystrokes and send them to the hacker who planted the malware in our system. This means that if we are entering a password somewhere, let's say in our online bank account, that person controlling the malware also gets to know it. Almost everything is visible to the hacker, including our data, confidential files, photographs.

After **malware**, the next one is **ransomware**.
Hackers can encrypt our files using ransomware and demand a ransom. They encrypt the files, which then can only be decrypted with a decryption key. Even if the ransom is paid, the hacker may not decrypt the files.

This type of attack is more common on individuals but still happens to organizations. According to heimdalsecurity.com, 37% of the organizations were hit by ransomware. Of those, 32% paid the ransom to get their data back, but they only retrieved 65% of the data.

The next one on the list is **Denial-of-Service**, commonly known as **DoS**.

DoS typically targets the webservers hosting a website. A webserver, by definition, is a server that hosts a website or a web application. Users connect to the website, such as google.com, and access information. The hackers target the webserver, sending an enormous volume of malformed requests. The webserver attempts to handle these requests, but eventually, the load becomes too high. The webserver then runs out of processing power and memory and crashes. Legitimate users now can't access the site because the webserver is unavailable.

A single system conducts the DoS attack. It can be amplified when several hundred, thousands, or even millions of systems perform the attack against one or more web servers. This type of attack is known as Distributed Denial-of-Service (DDoS) attack. In 2007, a massive DDoS attack on Estonia was reported by ccdcoe.org. Around a million systems were used to conduct this attack.

The obvious question is: how did the hackers get a million systems to do this? The answer is malware - these were malware-infected systems controlled by hackers, these machines are collectively known at ‘botnets’.

One type of attack you may not have heard of is **the man-in-the-middle (MITM) attack**. A **man-in-the-middle** attack is a general term for when a perpetrator positions themself in a conversation between a user and an application. They do it either to eavesdrop or to impersonate one of the parties.

The aim is to reveal personal information, such as usernames, passwords, credit card numbers, etc.
This does not have to be a person literally eavesdropping on a conversation, simply using an open Wi-Fi network would allow anyone on that network to perform an MITM attack. However, this is less frequent today due to the adoption of secure web standards such as HTTPS, the green padlock you see next to supported sites on your browsers.

Broadly speaking, a **man-in-the-middle** attack is the equivalent of a mailman opening your bank statement, writing down your account details, and then resealing the envelope and delivering it to your door.

Moving on, let's talk about **credential reuse**.
We all access several websites in a day. Some of them require us to log in. To do that, we must remember our usernames and passwords. Many of us are guilty of a particular mistake: we keep repeating the passwords from one website to another. When hackers hack one website or web application, they gain access to credentials. They then try the same credentials with other websites and web applications. In many cases, the hackers can match the usernames and passwords. It only takes one database breach and there are openly available tools for testing email/username password combinations against hundreds of sites to check for password reuse. While it only takes a few minutes to set up and properly configure a secure password manager across your devices, it takes hackers seconds to check if you’ve reused a password against many common sites.

Next up is the **insider threat**.

Once you've nailed your outward security, it's essential to remain aware of internal threats. These are often people who are either unhappy with the organization or are frustrated with their work. They can initiate the attack themselves or provide information to the people who initiate it. Tessian reports an increase of 47% insider threats between 2018 and 2020.

Last but not least is the **mobile attack**.
With the popularity of mobile devices, attacks have become equally common. Hackers target vulnerable mobile apps, and when they are used, they gain access to mobile devices to steal information. Hackers also post malicious fake apps into the app stores. Once users download and start using them, the hackers can access their mobile devices, allowing them access with more control than the end user of the device. One standard method is sending malicious links through SMS messages and letting the curious users click on those links. Once that happens, malware can be downloaded onto a mobile device.

Protecting Yourself
So, we have learned about several types of common attacks. But how do we safeguard ourselves?

The first method is **training**.
Everyone in an organization should undergo a basic level of security training. The user should be informed about social engineering, specifically phishing attacks. We don't need to make everyone a security expert, but fundamental knowledge can prevent many security breaches. For example, the users should never click on a link in an email or an SMS message sent by an anonymous person. This training should be refreshed on a schedule and as the threat landscape and you or your organization’s exposure widens.

The next method involves **restricted access privileges**.
The users within an organization must be assigned permissions on a need-to-know basis. The users should never be allocated more access privileges than they need to have, as this minimizes the scope of any potential breach.

Another tactic you may be familiar with is **multi-factor authentication.**
In most cases, hackers obtain the user credentials, which they later use to steal information. With multi-factor authentication in place, even if hackers get ahold of user credentials, they still require a PIN, One-time Password, or even a smart card, adding an extra layer of protection. Enable it wherever possible!

The penultimate list entry is called **Defense-in-Depth**.
This just refers to the principle of having multiple layers of security implemented. A solid example might be the combination of a firewall, an anti-malware application, and restricted privileges.

Finally, let's discuss **security policies**.

Organizations need well-designed IT security policies to ensure the success of their cyber-security strategies and efforts. Security policies should focus on passwords, training, and infrastructure. For example, a password policy should drive the users to use complex passwords and change them after a certain number of days. Other important policies involve the protection of data, such as storing/exchanging confidential information on portable drives and ensuring the security of your workstations and laptops.

Equally as important as the policies are their actual enforcement and verification. An IT security policy is worth nothing if it's not followed.

So, that's a lot to mull over. The threat of bad actors online is genuine. Still, thankfully - with the help of the techniques outlined today - you can significantly reduce risk.

This week, update your accounts to make use of multi-factor authentication and consider getting a password manager such as LastPass. It can feel like too much extra effort, but it's certainly worth doing to protect sensitive personal and professional data.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] Top Cyber Attacks In History | Biggest Cyber Attacks Of All Time | Cyber Security | Simplilearn
- [Video] 5 Most Devastating Cyber Attacks | Cybersecurity Insights #18
- [Video] How could cyber attacks affect you?
- [Article] Common Types of Cybersecurity Attacks
- [Article] More and More Companies Are Getting Hit with Ransomware [2021-2022]
- [Article] Man-in-the-middle (MITM) Attack, Imperva
- [Article] Consumers lost $56 billion to identity fraud last year—here's what to look out for, M. Leonhart