YE THI HA HTWE

CYBERSECURITY FOR NON-PROFITS

CYBERSECURITY
FOR
NON-PROFITS

BY

YE THI HA HTWE, DR.

Introduction

Why are non-profit organizations more vulnerable to cyber attacks?

Profit-driven businesses typically take precautions against all possible ways of losing their profits. They don't hesitate to invest in defensive measures. Non-profit organizations, on the other hand, tend to focus primarily on public service activities. Donor organizations are relatively less interested in allocating significant budgets for cybersecurity measures within the organization.

While most businesses deal with sales documents and detailed pricing calculations, non-profit organizations may have a lot of personal information. Healthcare organizations, in particular, need to be more cautious about security. When receiving healthcare, people usually use their real names, and information such as current illnesses, presence of infectious diseases, and regular medications are recorded, making them more susceptible to attacks.

One of the common methods of attack is *hyper-personal social engineering*, which uses individuals' personal information for deception. In technical terms, this targeted attack is also called *spear phishing*. It typically targets those with privilege to view and edit financial information in non-profit organizations.

AI is also significantly enhancing these types of attacks. We're not talking about publicly accessible AI like ChatGPT or Gemini, but custom-trained AI that isn't available for public use. These AIs can quickly gather vast amounts of information about organizations.

Software used for Spear Phishing can be studied at:

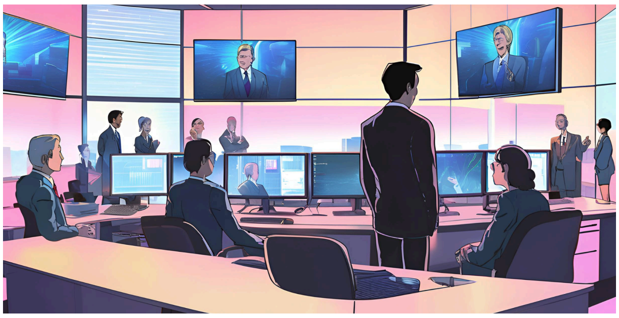
https://github.com/trustedsec/social-engineer-toolkit

https://github.com/UndeadSec/SocialFish

Software for secretly recording video through webcams can be studied at:

https://github.com/hangetzzu/saycheese

Deepfake technology has also become nearly indistinguishable from real people in English language content. With just 30 seconds of voice recording, deepfake technology can make a person say anything desired. Therefore, for financial matters, phone calls and voice files can no longer be relied upon exclusively.



Types of Attackers

Solo hackers

This refers to attacks by individuals or small groups. In the early days of the internet, solo attackers were quite prevalent and successful, similar to what you might see in movies. However, in today's world, due to improved cybersecurity systems, significant attacks from solo operators are less likely.

State-backed organizations

National-level attack groups mostly target other nations. On a country-to-country scale, while nations might appear cordial on the surface, state-level cyber attacks are ongoing. They're usually busy with activities like stealing information from other countries or trying to leak trade secrets, so the likelihood of them directly attacking your organization is low.

Organized crime groups

What we really need to be cautious about are systematically organized criminal enterprises. Most of these operate under the guise of security system companies. They have legally registered businesses in their respective countries, complete with HR departments, and systematically recruit and train their staff. These are large operations that offer good employee salaries and performance-based bonuses, which is why many solo hackers end up joining such large enterprises. The main difference between organized groups and solo operators is the ability to scale operations as needed. For example, suppose they discover a security vulnerability in Windows that allows them to record all keystrokes on a user's computer. If Microsoft discovers this weakness, they'll quickly patch it with a Windows Update. Therefore, organized crime groups can launch massive, coordinated attacks on multiple targets within a short period before the update is released. This kind of large-scale, rapid operation is only possible for well-organized enterprises.

Motivation for Attacks

The root cause is that they attack for money. The benefits that can be gained from attacks include:

Ransom

After stealing an organization's email system, they demand a certain amount of money to return the emails.

Extortion

After obtaining confidential information, they demand money to prevent it from being leaked publicly.

Data sale

If you don't pay them anything, or if selling the data is more profitable than what they can get from you, they sell your data on the dark web. For example, if they steal your Zoom Pro account, selling that account to many people might be more profitable than extorting money from you. Non-profit organizations are most often affected by ransom and extortion.

According to the Verizon 2024 Data Breach Investigation Report, the motives behind cyber attacks are: *Financial gain (95%) Espionage (5% to 7%) Other (1%)*

The FBI's Internet Crime Report states that in 2022, cyber attacks resulted in losses of up to $10.3 billion in the United States. This figure is based on cases reported to the FBI, so the actual amount could be much higher, considering unreported cases resolved privately. Paying to resolve such issues often goes unreported due to concerns about stock price drops and reputational damage if made public, suggesting that actual losses could be significantly higher.

Data Breaches

In recent years, there have been several notable incidents where non-profit organizations were primarily targeted.

2019	The American Medical Collection Agency (AMCA) experienced a leak of personal and financial data of millions of patients.
2020	The food organization Philabundance paid a $1 million advance to a contractor for building construction. However, the money didn't reach the contractor but was instead received by scammers using fake emails.
2022	The Red Cross organization had data stolen from 515,000 individuals.
2023	Save the Children suffered a theft of approximately 6.8 TB of financial, health, and medical data.

The majority of these data breaches are said to have occurred through Enterprise Resource Planning (ERP) software, which are business process management systems. Currently, popular ERP systems include SAP, Oracle, and Microsoft Dynamics. While they can be beneficial when used properly, they also pose a risk because they are the central location for all of an organization's data. If a password of a high-level individual is compromised, there's a danger that all data could be leaked.

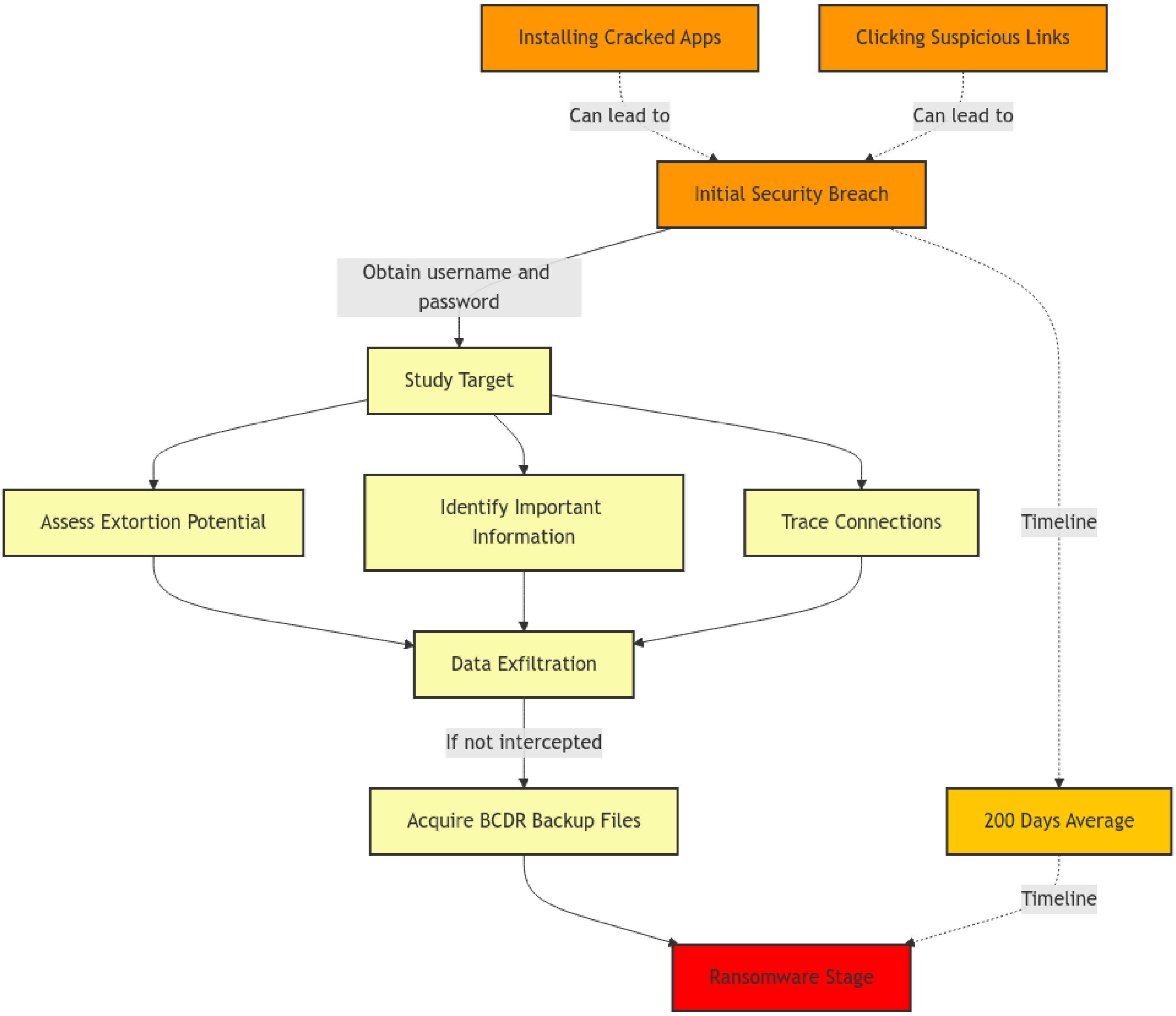
How can security systems be breached

The majority of organizational security breaches are caused by people within the organization. According to research results, 80% of security breach causes are due to information inadvertently or knowingly provided by users within the organization. Once a password is obtained, it will be used to attempt access in multiple places.

Websites like https://whatsmyname.app/ can show accounts from various websites associated with a target person's name when entered. Most of us tend to use the same password across multiple websites because it's difficult to remember many complex passwords.

Attackers might send links via SMS messages to phones or via email to computers to steal information or install programs that can slowly steal data. This type of phishing attack can be reduced by email filtering, which is explained later.

Understanding Cyber Threats



Stages of a Cyber Attack

Once an attacker obtains the username and password of the target from a fake user account login page, they first study the target's business activities. They assess whether this person could afford to pay if extorted, which information is important, and also trace the connections to other people associated with the target.

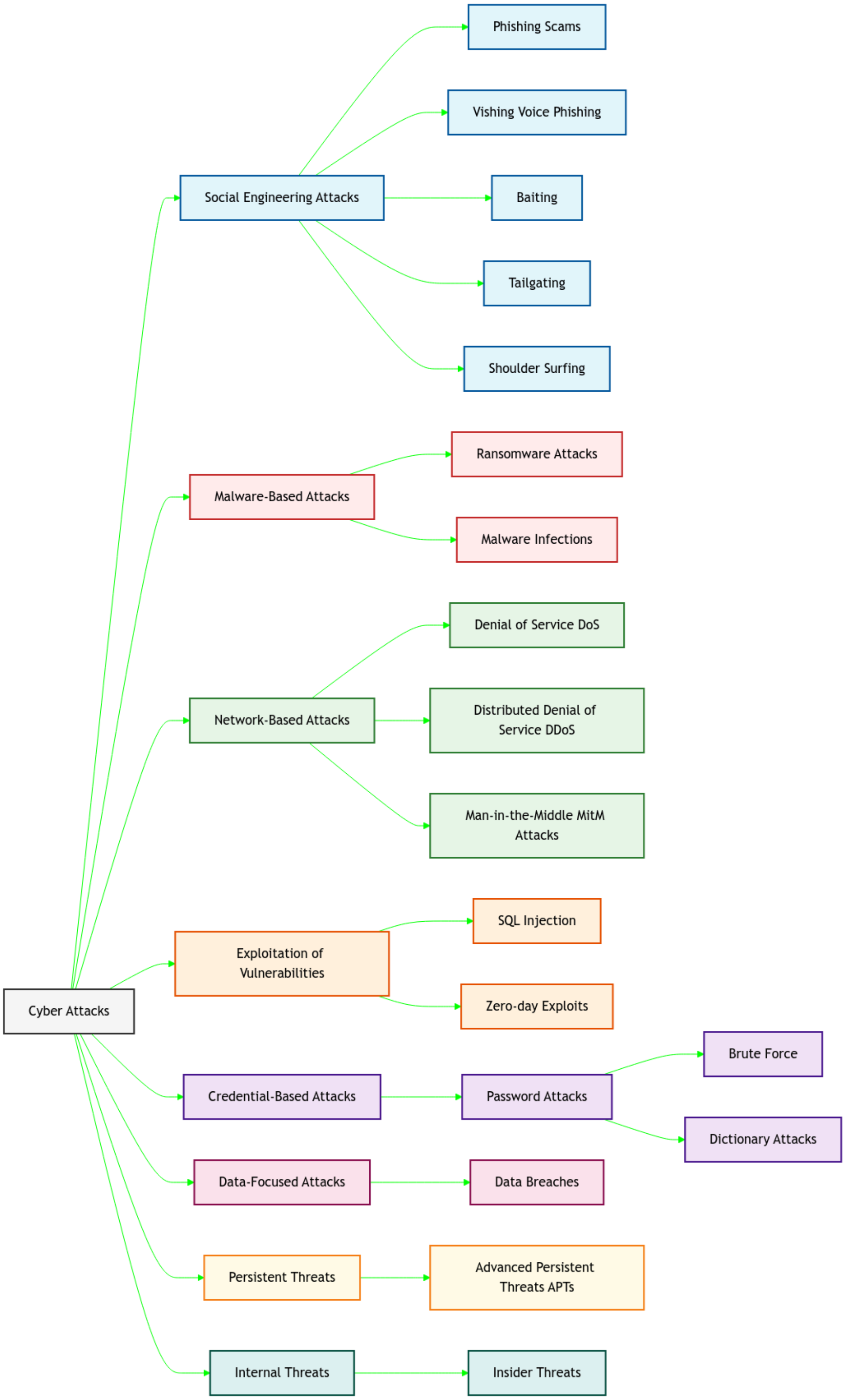
After careful study, they proceed with data exfiltration. If interception and prevention can be done at this stage, it may prevent escalation to ransomware attacks, limiting the damage to extortion attempts or selling data on the dark web.

Some organizations practice Business Continuity Disaster Recovery (BCDR), an emergency data recovery system. Well-prepared attackers often manage to acquire even these BCDR backup files.

After obtaining all desired information, they move to the ransomware stage. Research shows that on average, it takes about 200 days from the initial security breach to the ransomware stage.

Installing cracked applications or carelessly clicking suspicious links in messages often don't cause immediate problems, so people tend to forget about them. Data thieves will take more time studying the information flow within your business if the data is more valuable. They typically attempt extortion only when they're certain, which is why some businesses still end up paying large sums to recover their data.

Common Types of Cyber Attacks



Social Engineering

Social engineering is a manipulation technique that exploits human behavior to gain unauthorized access or information.

Types of Social Engineering Attacks

Phishing Scams

You may remember the first scam email you received that almost succeeded in tricking you. The scammer would claim to have access to significant funds but needed your help to claim them you'll get a portion of it. These scams succeeded because they targeted people's desire to help others and on the dark side: greed.

Today's phishing attempts have become far more sophisticated. These can include potential donors promising large contributions, grant-making organizations, board members requesting urgent fund transfers, partner organizations seeking collaboration, or vendors requiring immediate payment.

Vishing

Imagine this scenario: Your phone rings with an unknown number. The caller introduces himself as someone from your internet service provider, claiming they've noticed your network needs important security updates. He offers free assistance and asks if you're at your computer. This is "vishing" being phone-based phishing. Such calls often try to trick people into downloading malware or spyware under the guise of technical support. Though many vishing attacks involve live scammers attempting social engineering, automated robocalls with spoofed numbers are increasingly common, trying to reach as many potential victims as possible.

Baiting

Baiting is a social engineering technique where attackers exploit human psychology—specifically greed, shame, or curiosity—by offering an enticing lure.

The attack works in various ways:

1. Digital Baiting:
- Fake movie download sites offering recently released films
- Deceptive ads promising free expensive products
- Malicious software disguised as a free and useful software
2. Physical Baiting:
- Planted USB drives in parking lots or public spaces
- In-person scams offering gift cards for personal information
- Fake surveys promising rewards

Tailgating

Tailgating is when unauthorized individuals gain access to secure areas by exploiting social norms and human kindness. Think of it like bank robbers in movies who first scout their target – except in real workplaces, it's often more subtle. For instance:

- Following closely behind someone with legitimate access
- Using convincing pretexts or stories to gain trust
- Taking advantage of people's natural helpfulness (like pretending to be a pregnant woman carrying heavy boxes)

Shoulder surfing

Shoulder surfing is another security risk, especially in open-plan offices. This occurs when someone observes confidential information by simply looking over someone's shoulder or at their screen.

This can happen at workstations in open office layouts, while using ATMs (hence the warnings to cover your PIN) and in any situation where sensitive information is visible on screens.

Malware based Attacks

Ransomware Attacks

"All your important files have been encrypted. If you pay $50,000 in Bitcoin within 48 hours, you can retrieve your files. If you don't pay, all files will be destroyed, and donors' information will be made public."

You might receive a similar email when hit by a ransomware attack. Almost immediately, you may find that files on all of the organization's computers are inaccessible. Donor lists, health records, financial records, photos, emails - all may become inaccessible, and even backed-up files are often affected.

In this situation, the management team should immediately seek help from their IT service provider. The incident should be reported to the cyber police. The office operations should be temporarily suspended and staff should be explained about the situation. Donors should be notified as well to withhold any financial transactions. Paying the ransom means unnecessarily spending donation money. Not paying could result in losing crucial data and halting operations. At the same time, it could compromise donors' privacy.

Malware Infections

Unlike ransomware, which has a specific goal of extorting money, other types of malware can have various objectives and effects.

Viruses	Programs that replicate themselves and spread to other computers, often causing system slowdowns, file corruption, or data theft.
Trojans	Disguised as legitimate software, trojans can create backdoors in your system, allowing attackers to gain unauthorized access.
Spyware	This type of malware secretly monitors user activity, potentially capturing keystrokes, screenshots, or browsing history.
Adware	While less harmful, adware can bombard users with unwanted advertisements and significantly slow down system performance.
Rootkits	These are designed to conceal certain processes or programs from detection, making them particularly difficult to identify and remove. It's like a toolbelt for hackers, giving them various ways to attack. Stuxnet is a famous example of a rootkit.
Wiper Malware	Wiper malware erases data from your computer. It doesn't make money for attackers but causes disruption. NotPetya, released in 2017, was a very destructive wiper malware targeting Ukrainian businesses.

Malware can enter a system through downloading infected files or software, opening malicious email attachments, visiting compromised websites, or using infected USB drives or other external devices.

Signs of a malware infection may include unexpected system slowdowns or crashes, strange pop-ups or browser redirects (*your searches being shown in an unknown search engine other than Google, Bing etc), u*nexplained changes to files or settings, unusual network activity.

Network based Attacks

Denial of Service (DoS) Attacks

The goal is to overwhelm a system, network, or website to make it unavailable to its intended users. A DoS attack might manifest as extremely slow internet speeds, inability to access your organization's website or online services, or frequent system crashes.

Distributed Denial of Service (DDoS) Attacks

A DDoS attack is a more sophisticated version of a DoS attack. Instead of using a single source, it utilizes multiple compromised computers (often referred to as a "botnet") to target a single system.

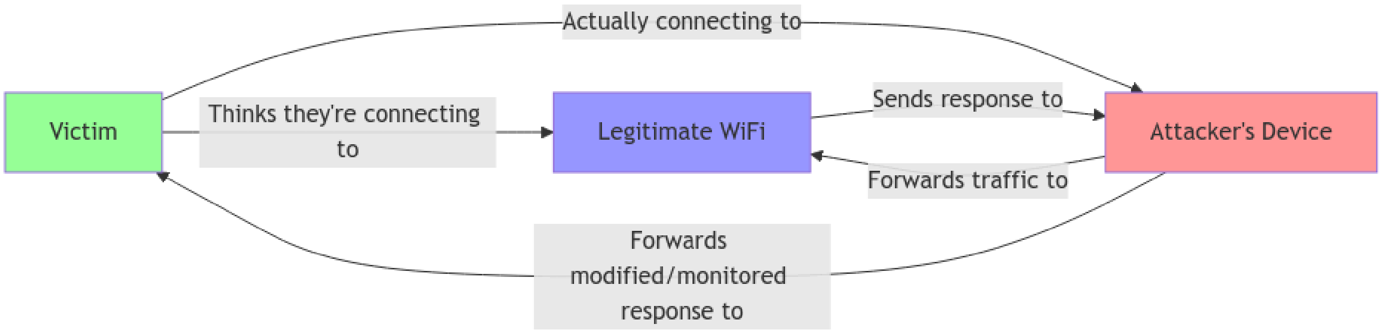
DDoS attacks might target the organization's main website, preventing information dissemination or online donations, email servers to disrupt communication and online platforms used for service delivery.

Man-in-the-Middle Attack

Risk of public WiFis

Most public WiFi networks are open networks, meaning anyone can connect without a password. Public networks don't encrypt traffic between users and the access point, meaning data is transmitted in plain text. Users on the same network can potentially see each other's traffic.

Man-in-the-Middle attack is one of the most common attacks on public WiFi.



Here's how a MITM attack typically works. The attacker sets up a rogue access point (often called an "evil twin") that mimics a legitimate WiFi network. When victims connect to this fake network, all their traffic goes through the attacker's device first. The attacker can then intercept sensitive information (passwords, credit card numbers), inject malicious content into web pages, monitor all network traffic and modify data being sent or received.

Exploitation of Vulnerabilities

SQL Injection

SQL injection is a technique where attackers insert malicious code into your organization's databases through vulnerable web applications.

Zero-day Exploits

These are attacks that target previously unknown vulnerabilities in software. The use of the word ‘zero day’ initiated from pirating movies or music where pirated copies are released at the same time or before the movie or music is officially launched.

Credential-based Attacks

Password Attacks

While social engineering and phishing steals by tricking you to enter passwords by yourself, attackers can also attempt to crack your passwords using password cracking tools. The OpenBullet is one of them.

https://docs.openbullet.dev/docs/intro

Brute Force Attacks

A brute force attack is a method of trying every possible combination of characters to guess a password or encryption key.

Dictionary Attacks

Attackers use common words to guess passwords. A wordlist of common passwords can be imported to the password cracking tool. A sample wordlist can be found at:

https://github.com/danielmiessler/SecLists/blob/master/Passwords/2023-200_most_used_passwords.txt

Persistent Threats

Advanced Persistent Threats (APTs)

APTs are long-term, targeted attacks aimed at stealing data over time.

Internal Threats

Insider Threats

These come from within the organization, either maliciously or accidentally. Departed employees might still have access to the organization's email system as well as cloud storage drives.

Protecting yourself

Password Management

Password Managers are specialized tools that securely store encrypted passwords. They can generate random, strong passwords automatically. You only need to remember one master password to access all your other passwords.

When using a password manager, protect your master password carefully and update it regularly. Make sure your passwords are complex and secure whatever method you choose.

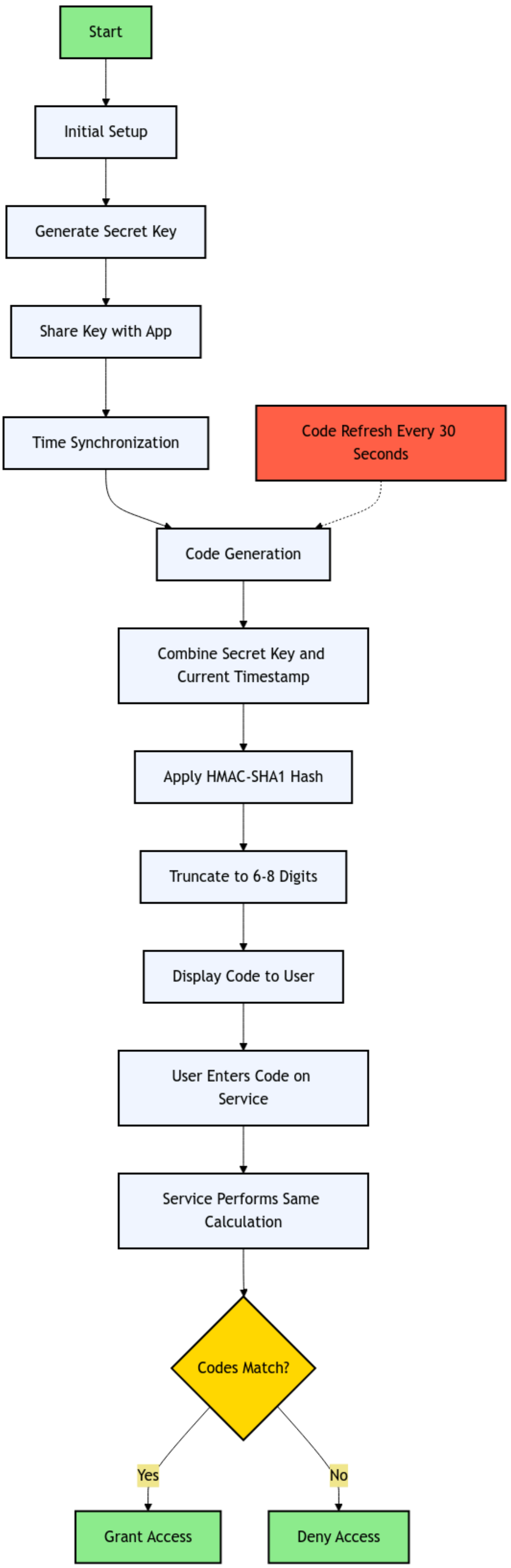
Authenticators

Authenticators, also known as two-factor authentication (2FA) or multi-factor authentication (MFA) apps, provide an additional layer of security for user accounts. They generate time-based one-time passwords (TOTP) that users enter along with their regular password to prove their identity.

Trusted Authenticator Apps

Some widely trusted authenticator apps include Google Authenticator, Microsoft Authenticator and Authy. These apps are considered trusted due to their robust security measures, regular updates, and backing by reputable companies.

How Authenticators work



Protecting your Email

Your main email account probably connects to everything important in your digital life - your photos, documents, bank accounts, and messages. Just like you wouldn't leave your house key under the doormat, you need to protect your main email address.

Start by creating a strong password for your main email. Make it at least 20 characters long. Don't worry about remembering it - use a password manager to keep track of it for you.

Add an extra layer of security by turning on multi-factor authentication. This is like having both a key and an alarm code for your house. When you log in, you'll need to confirm it's really you through your phone or an authentication app.

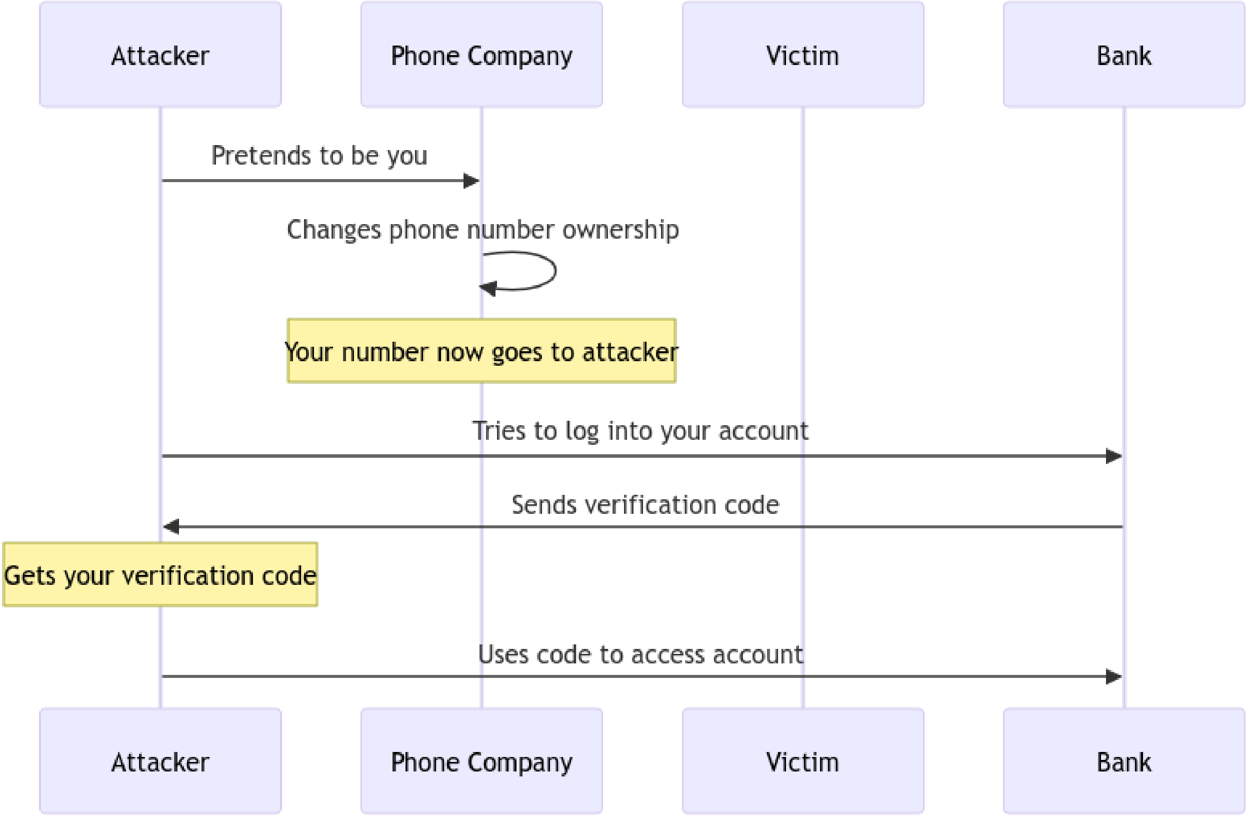
Here's a smart trick: create a second email address for everyday use. This second email address acts like your public-facing mailbox, while keeping your main email private and secure. Don't use your name in this second email address - make it harder for others to connect it to you.

When you sign up for new accounts - whether it's shopping, social media, or newsletters - use your second email address. This keeps your main email address private and protected.

Protecting your phone number

When you use your phone number for work or personal accounts, you receive special codes by text message to prove it's really you logging in. This is especially important for accessing work systems or banking websites. Unfortunately, criminals can use your phone number to try to break into your accounts or pretend to be you.

SIM Swapping


Attacker
Phone Company
Victim
Bank
Pretends to be you
Changes phone number ownership
Your number now goes to attacker
Tries to log into your account
Sends verification code
Gets your verification code
Uses code to access account
Attacker
Phone Company
Victim
Bank

Don't answer calls from numbers you don't recognize. Let them go to voicemail. If it's important, they'll leave a message. By not answering unknown calls, you make your number less attractive to spam callers. Avoid sharing your phone number on public websites. If someone can't find your real phone number, they can't use it to cause problems.

Protecting your name

When someone has your name, they can find other details about you.

Using Aliases

When you sign up for online accounts, try not to use your full name. Use a nickname or your initials instead. Only use your real name when it's legally required. This helps keep your personal information separate from your online presence. The less your real name appears online, the safer your personal information will be.

Removing Search Results

Google has tools to help remove your personal information from search results. When you find your information in Google search, you can go to this link and submit a removal request.

https://support.google.com/websearch/contact/content_removal_form

Bonus Tip: How much google knows about you?

You can take a look at google's ad center to see how accurately google has stored your personal information. You might not have provided your information to google but based on your search history, google can accurately guess your personal information.

https://myadcenter.google.com/controls

You can turn off the ad features if you don't want to.

Social Media Safety

Many people accidentally share too much when posting about everyday things. Your vaccination cards, travel tickets, or boarding passes contain personal details that others could misuse. Even sharing your vacation plans can tell potential thieves when your home will be empty.

Scammers can use photos and information about your relatives to create convincing stories. They might pretend to be your relative in trouble just because they saw a family photo you shared. Pay attention to what friends and family post about you. Have open conversations with them about your privacy preferences. Let them know if you're uncomfortable being tagged or appearing in their posts.

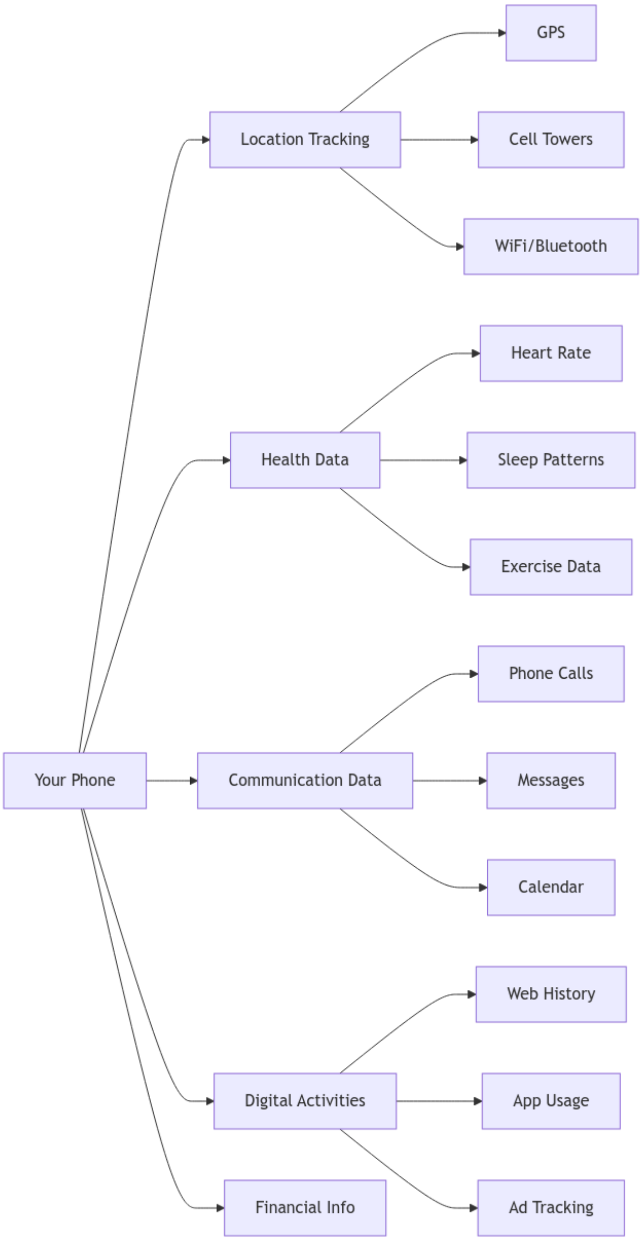
Avoid announcing your current location or future plans on social media. This information helps bad actors know when you're away from home or where they might find you.

Digital Footprint

Everything you post creates a permanent record online. Even if you delete a post seconds later, someone might have already saved it. Only share things you're comfortable having online forever.

Your Phone and Your Privacy

Your phone tracks where you are through GPS, cell towers, WiFi, and Bluetooth. It knows if you're walking, running, or taking an elevator. It can even detect if you've been in an accident. These tracking features work together to create a detailed picture of your daily movements. Your device records who you talk to and meet with. It maintains records of your conversations, messages, and meeting schedules. Your browsing history, app usage, and online behaviors are tracked. This includes which websites you visit and how you use different applications on your phone. Modern phones collect health-related data through fitness apps and connected devices. This includes heart rate, sleep patterns, exercise routines, and dietary habits. Your financial information, daily routines, and personal habits are stored on your phone. This creates a comprehensive profile of your lifestyle and behaviors. Your phone has a unique advertising identifier. Companies use this to track your activities and create targeted advertisements. This data is often bought and sold between companies. When you install new apps, they request access to different parts of your phone. Each app can collect and send data back to the company that created it.



Protecting Your Privacy on Mobile Devices

Location Services

On iPhones, go to Settings, then Privacy & Security, and find Location Services. You can turn off all location tracking, but this might affect your phone's usefulness. Instead, choose which apps can use your location. Turn off Product Improvement under System Services to stop Apple from collecting data. Check which apps have used your location recently and adjust permissions as needed. Only allow location access for apps that truly need it, like navigation apps.

On Android, find Location in Settings. You can turn off all location services or choose specific settings. Manage your Location History in your Google account settings. Consider turning this off or setting it to auto-delete after three months. Review which apps have location permissions and adjust them as needed.

Advertising Tracking

On iPhones, find Apple Advertising in Privacy & Security settings and switch off personalized ads. Also consider turning off analytics sharing.

For Android, go to Settings, then Security & Privacy, and find the Ads option in More Privacy Settings. Delete your advertising ID to stop tracking. While there, turn off usage and diagnostics sharing too.

Health Data

Be careful with health data on your device. On iPhones, go to Health in Settings to see which apps access your health information. Review and adjust these permissions. You can also use the Health app to manage this data.

On Android, find Health Connect in More Privacy Settings. Review app permissions for health data and adjust as needed. Always share the minimum amount of data necessary for the service you want.

App Permissions

Be selective about app permissions. Ask yourself if you trust the app developer and if the app really needs the access it's requesting. A calculator app, for example, doesn't need your location. Give each app only the permissions it needs to function. If an app asks for unnecessary permissions, consider using a different one.

Protecting your organization

Recognizing Phishing Attacks

There are several common red flags to watch out for in potential scam attempts. These include urgent requests for fund transfers, unexpected changes in payment instructions, requests for sensitive information, pressure to act quickly, grammar and spelling errors, and unusual sender addresses.

It's important to verify unusual requests through alternative communication channels, such as SMS or phone calls. Always double-check sender email addresses carefully. Never share passwords or sensitive information via email. Implement a multi-person approval process for financial transactions. Regularly backup important data. Lastly, keep all software and systems updated to maintain security.

Common Indicators of Phishing Attacks

Email Header and Sender Information

Emails appear to be from a legitimate company but use a public email domain (e.g., @gmail.com). There might be slight misspellings in domain names (e.g., microsft.com, arnazon.com). Sender display names often don't match the email addresses.

Unusual sending patterns

Emails sent at odd hours for your timezone. An email coming from your timezone should be within working hours of your timezone. Multiple similar messages from different addresses should also be considered suspicious. Emails from persons or organizations you've never interacted with should be verified by sending an email to the official email address of that organization.

Content Red Flags

Urgency and pressure tactics such as threats of account closure or legal action, limited-time offers that are "too good to be true", demands for immediate action are generally risky and should be studied thoroughly before taking actions.

Generic greetings like "Dear Sir/Madam", "Dear Valued Customer" and no personalization in the greeting might be coming from automated programs.

Non-professional English such as poor grammar or spelling errors, inconsistent formatting, mix of fonts or writing styles and awkward sentence structures are usually coming from attackers.

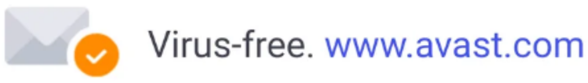
Links and URLs

Slight misspellings of legitimate domains like *telegarm*, teIegram (Capital `i` instead of small `l`) might be accidentally considered safe. Urls with random strings of characters such as `wer09as.000webhost.com` are unsafe because these are provided by free web hosting services as some attackers are not willing to invest in buying a domain name. Unusual top-level domains like ayabank.blogspot.com, kbank.wordpress.com are absolutely tricky.

Numbers substituting for letters as in '1drive.com' as well as link texts showing one URL but hovering reveals another are misleading too. URLs using URL shorteners (bit.ly, adf.ly) to hide true destination and IP addresses instead of domain names are non-professional and should always be avoided.

Attachments

Suspicious file types such as executable files (.exe, .scr, .bat), multiple extensions (invoice.pdf.exe), compressed files (.zip, .rar) containing executables should not be downloaded before an anti-virus scan. Some email attachments may come together with a description e.g. 'Scanned with Avast antivirus' or 'Virus-free' but this is often tricking the user to consider the attachment is safe.



Virus-free. www.avast.com

Request Patterns

Unusual or sensitive information requests such as login credentials, financial information, social security numbers, personal identifying information and unusual payment requests like wire transfers, gift cards, cryptocurrency, payment to unfamiliar accounts should be taken with extreme caution.

Protection from Phishing

Always verify independently by contacting organizations through known, legitimate channels. Don't use contact information provided in suspicious emails. Call known phone numbers to verify requests and never act under pressure. Take enough time to evaluate unexpected requests because legitimate organizations won't demand immediate action.

Ensure technical safeguards by enabling spam filters, keeping software and systems updated, and multi-factor authentication.

Email authentication protocols (SPF, DKIM, DMARC) are mandatory. (Usually included in mail services: Google Workspace, Microsoft 365 etc). Suspicious emails should be forwarded to IT or relevant authorities. Built-in phishing reports or spam reports can also be done and the incidents should be documented for future reference.

Protection from Vishing

To protect yourself and your organization from vishing, only take action when you initiate the contact. Legitimate organizations like banks, law enforcement, and the service providers rarely make phone calls unless previously arranged. It's best to be skeptical of unexpected calls, even if they seem urgent.

Protection from Baiting

Organizations often defend against USB-based attacks by disabling USB ports on company devices. However, the most effective defense is employee education. Staff should know legitimate company communication channels for rewards/prizes. They should understand common baiting techniques and be able to identify suspicious offers. A security-aware culture should be created by sharing knowledge with colleagues.

Tailgating Protection

While it might feel awkward, it's crucial to verify everyone's identification, even if they seem legitimate. Just as you wouldn't let an unverified repair person into your home, the same caution should apply at work.

Shoulder-surfing Protection

Always verify identification before allowing anyone into secure areas. Use privacy screens on monitors to limit viewing angles. Stay aware of your surroundings, especially when handling sensitive information. Make sure your devices are screen-locked whenever you’re away from your table. Consider requesting privacy measures when working with confidential materials

Ransomware Attack Protection

Organizations should maintain secure backup systems. Staff should be provided cybersecurity training for potential threat awareness. Robust IT security systems should be installed followed by developing emergency response plans. Consider getting cyber insurance if feasible.

Malware Protection

To protect against malware infections, all software and operating systems should be up-to-date. Use reputable antivirus and anti-malware. Be cautious when opening email attachments or clicking links. Avoid downloading software from untrusted sources. Regularly backup important data to an offline or cloud-based storage. Backing up offline to hard disk drives is generally considered safe since they are not connected to the internet.

If a malware infection is suspected, it's crucial to disconnect the affected device from the network immediately and seek professional IT support to properly diagnose and clean the system.

Response to DoS

Unusual slowdowns or outages immediately to IT staff. Office devices should be regularly updated and secured. If a DoS attack is suspected, employees should notify IT immediately and follow any instructions provided, such as logging off certain systems or disconnecting from the network.

Protecting MITM attack

Use a VPN when on public WiFi. VPNs usually encrypt data and connect to a foreign server making the MITM attack difficult. Only visit HTTPS websites since SSL encryption makes the attacker take an extra step to decrypt. Avoid accessing sensitive information (banking, emails) on public WiFi. Enable your device's firewall. Disable automatic WiFi connections. Verify the network name with the business providing it. Another layer of protection is using your mobile data instead of public WiFi for sensitive operations.

Protecting insider threat

The organization should add in their policy to delete or deactivate emails of departed employees, revoke access to cloud storage drives and remove them from social media page administration.

Cybersecurity Systems and Measures for IT

AV (Antivirus)

Can be viewed as a regular iron gate installed in front of a house. It protects against predictable threats like thieves and robbers. The AV comes with preloaded virus signatures in a database and checks every file entering the computer against this database. AVs need regular updates to recognize new viruses.

DNS & Web Filtering

DNS (Domain Name System) can be described as the internet's address book. It's a system that translates website addresses we're familiar with (e.g., www.google.com) into IP addresses that computers understand (e.g., 142.250.196.110). Web Filtering is a technology that filters and controls content on the internet. It's primarily used for the following purposes:

- To protect against unwanted malware, viruses, etc.
- To block websites unrelated to work in office networks
- To restrict inappropriate content for child protection

The main Web Filtering methods include:

1. DNS Filtering - Blocking unwanted domains at the DNS level
2. URL Filtering - Scrutinizing website addresses
3. Content Filtering - Examining internet page content based on keywords
4. Protocol Filtering - Inspecting internet protocols

The benefits of DNS & Web Filtering include:

- Prevents employees from accessing websites that are major distributors of malware (e.g., gambling websites)
- Blocks or warns about suspicious links in emails
- Can block sites like YouTube and Facebook in strict work environments, reducing internet bandwidth usage on non-work-related activities and improving employee productivity

Basic Requirements to install DNS & Web Filtering

Hardware requirements

- A router (capable of running open-source firewall software like pfSense)
- A server or computer (for DNS filter software like Pi-hole)
- Internet connection

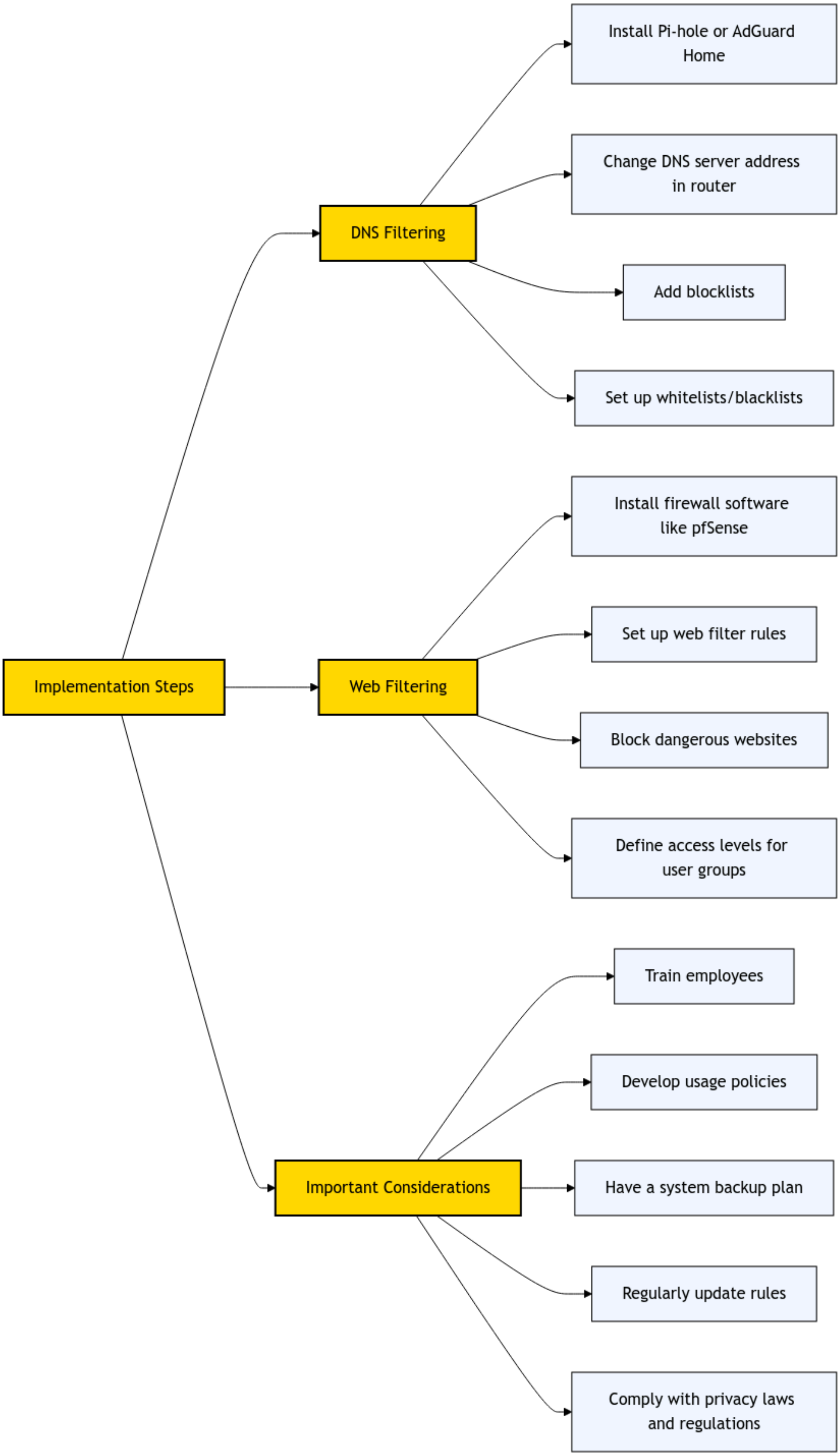
Software options Free or low-cost choices

- Pi-hole (free DNS filtering)
- OpenDNS (free basic version)
- Cloudflare for Teams (has a free version)
- AdGuard Home (free)

Estimated costs

- Hardware: $200-500 (Raspberry Pi or server for Pi-hole)
- Software: Free or $1-5/user per month
- Installation: Can be done by yourself

The above points are for a basic setup and can be improved based on requirements. For a larger number of users, consider cloud-based solutions. When implementing this system, it's advisable to seek assistance from an IT expert for a more effective setup.


Implementation Steps

DNS Filtering

Install Pi-hole or AdGuard Home

Change DNS server address in router

Add blocklists

Set up whitelists/blacklists

Web Filtering

Install firewall software like pfSense

Set up web filter rules

Block dangerous websites

Define access levels for user groups

Important Considerations

Train employees

Develop usage policies

Have a system backup plan

Regularly update rules

Comply with privacy laws and regulations

Access Management

Access Management controls how individuals can access an organization's data.

Basic functions

- Create separate accounts for each user
- Establish password policies (e.g., minimum 8 characters, must include special characters)
- Implement Two-factor/Multi-factor authentication
- Use authenticator phone applications (such as Microsoft Authenticator, Google Authenticator, Authy)

Setting permissions

- Grant only necessary privileges based on employees' responsibilities
- Review privileges whenever there is staff departure or change of departments

EDR (Endpoint Detection and Response)

This can be described as a security system with modern sensors. It can detect not only common thieves and robbers but also suspicious behaviors, and monitors unknown individuals entering the house. Modern EDRs use Machine Learning and AI technologies. They continuously monitor processes, network traffic, and file changes in the system. They can detect behaviors like sudden increases in CPU usage, modifications to system files, or suspicious network connections. When such suspicious activities are detected, it can automatically prevent, stop processes, or cut off network connections.

MDR (Managed Detection and Response)

This is like a private security service that monitors 24 hours a day. They constantly monitor the EDR system and respond immediately in emergency situations. The EDR system sends real-time information to security expert staff to analyze log data and perform threat hunting. It uses real-time monitoring dashboards to observe the system's status.

SOC (Security Operations Center)

This can be viewed as a large security team providing MDR services. For example, it's like a large police station monitoring the security of houses in an entire city. Skilled staff monitor continuously and are ready to prevent and respond to threats. It uses SIEM (Security Information and Event Management) systems to collect log data. For example, if office files are stored on Google Drive, normal logins from office computers on the office WiFi network are fine. But if the same account logs in from a different country's IP address within minutes, it can automatically change the password, temporarily close the account, and immediately notify the user and the cybersecurity team. At the same time, it can block that IP address group, log the entire incident, and generate a report. It is usually connected to Threat Intelligence Platforms to stay informed about the latest cyber threats. As the system grows, it uses automated playbooks to respond to emergencies. Security analysts, incident responders, and threat hunters work in shifts to provide 24-hour monitoring in a SOC.

Business Continuity and Disaster Recovery (BCDR)

BCDR is planning to ensure that an organization's critical business functions can continue operating during cyberattacks, natural disasters, or other crises.

Basic Preparations

A list of critical data should be created to follow a monthly backup system. Prepare an emergency contact list in case of emergency.

Security Fundamentals

Install antivirus softwares and a firewall system. Provide security awareness training to employees

BCDR does not require a large investment. It can be effectively implemented through careful planning, regular practice, and participation from all employees.