Shubham Paikrao

Cyber Security Awareness

What is Cyber Security Awareness?

- Cybersecurity awareness means empowering people connected with the business to do their role in protecting your organization from potential security threats.
- Cybersecurity Awareness utilizes credentialing, resources, solutions, training, and tools to deliver knowledge and actions to protect the business.
- By creating a security awareness-aware workplace culture, a business can ensure its employees, contractors, and suppliers are mindful of the existence of cyber threats, how to recognize them, and their potential impact on the business.
- Prevention being better than cure, for small and medium businesses, pursuing a cyber awareness program provides a cost-effective manner by which to implement a robust defence against cyber threats.

❖ Email Phishing

Phishing attacks are the most common method that cybercriminals use to gain access to an organization's network. They take advantage of human nature to trick their target into falling for the scam by offering some incentive (free stuff, a business opportunity, and so on) or creating a sense of urgency.

Email-based scams are constantly evolving and range from simple attacks to more sneaky and complex threats that target specific individuals. The attack aims to encourage people to click on a link that leads to a malicious or spoofed website designed to look like a legitimate website or open an attachment that contains malicious content.

The hacker first compromises a legitimate website or creates a fake website. They then acquire a list of email addresses to target and distribute an email message that aims to dupe people into clicking on a link to that website. When a victim clicks the link, they are taken to the spoofed website, which will either request a username and password or automatically download malware onto their device, which will steal data and login credential information. The hacker can use this data to access the user's online accounts, steal more data like credit card details, access corporate networks attached to the device, or commit wider identity fraud.

# How to identify email phishing:

- Legitimate information: Look for contact information or other legitimate information about the organization being spoofed, then look to identify things like misspellings or a sender email address that has the wrong domain.
- Malicious and benign code: Be aware of anything, including code that tries to trick Exchange Online Protection (EOP), such as downloads or links that have misspellings.
- Shortened links: Do not click on any shortened links because these are used to fool Secure Email Gateways.
- Fake brand logo: Review the message for any logos that look real because they may contain fake, malicious HTML attributes.
- Little text: Ignore emails that have only an image and very little text because the image might be hiding malicious code.

# Tips for identifying attempted attacks, including:

- Do not trust unsolicited emails
- Do not send any funds to people who request them by email, especially not before checking with leadership
- Always filter spam
- Configure your email client properly
- Install antivirus and firewall programs and keep them up to date
- Do not click on unknown links in email messages
- Beware of email attachments. Verify any unsolicited attachments with the alleged sender (via phone or another medium) before opening them
- Remember that phishing attacks can occur over any medium (including email, SMS, enterprise collaboration platforms, and so on)
- Use email filters: Although normally associated with "spam filters," email filters can also scan for additional risks indicating an attempted phishing attack. For example, cybercriminals often hide malicious code in a PDF's active content or the coding that enables things like readability and editability. Finding the right email filtering solution can help reduce the number of risky phishing emails that make it through to users.

❖ Malware

Malware is malicious software that cybercriminals use to steal sensitive data (user credentials, financial information, and so on) or cause damage to an organization's systems (e.g., ransomware and wiper malware). It can be delivered to an organization in several different ways, including phishing emails, drive-by downloads, and malicious removable media.

1. **Trojans:** A Trojan (or Trojan Horse) disguises itself as legitimate software to trick you into executing malicious software on your computer.

Ultimately, Trojan malware can:

- Delete, modify, or steal data
- Spy on users
- Access networks
- Launch DDoS attacks
- Take remote control of devices

2. **Spyware:** Spyware invades your computer and attempts to steal your personal information, such as credit card or banking information, web browsing data, and passwords to various accounts.

Ultimately, spyware can:

- Breach of personal privacy
- Collects confidential data, including by logging keystrokes
- Steal data
- Result in identity theft or credit card fraud

3. **Adware:** Adware is unwanted software that displays advertisements on your screen. Adware collects personal information from you to serve you with more personalized ads.

Ultimately, the adware can:

- Be an annoyance
- Lure users to malicious sites
- Install spyware
- Share user data with third parties

4. **Rootkits:** Rootkits enable unauthorized users to gain access to your computer without being detected.

Ultimately, rootkits can:

- Take remote control of devices
- Grant cybercriminals admin access to devices
- Spy on users' activity

5. **Ransomware:** Ransomware is designed to steal and encrypt your files and block access to them until a ransom is paid.

Ultimately, ransomware can:

- Hold devices hostage
- Make data inaccessible through encryption
- Result in financial loss

6. **Worms:** A worm replicates itself by infecting other computers that are on the same network. They're designed to consume bandwidth and interrupt networks.

Ultimately, worm malware can:

- Delete or modify files
- Steal data
- Install backdoors for hackers
- Launch DDoS attacks
- Launch ransomware attacks
- Create botnets
- Infect many computers at once

7. **Keyloggers:** Keyloggers keep track of your keystrokes on your keyboard and record them on a log. This information is used to gain unauthorized access to your accounts.

Ultimately, fileless malware can:

- Steal data
- Collects confidential data, including by logging keystrokes

8. **Viruses:** Viruses are a type of malware that often takes the form of a piece of code inserted in an application, program, or system, and they're deployed by victims themselves.

Ultimately, malware viruses can:

- Seize applications
- Send infected files to contact lists
- Steal data
- Launch a DDoS attack
- Launch a ransomware attack

# How to prevent malware:

- Use multi-factor authentication
- Avoid suspicious emails, links, and sites
- Adjust spam filters
- Keep software up to date
- Know the warning signs of a malware infection:
    1. Your device is sluggish, freezing, or crashing
    2. Programs are opening, closing, and modifying on their own
    3. Your device has little to no storage space
- Backup files regularly

# Important tips include:

- Be suspicious of files in emails, websites, and other places
- Don't install unauthorized software
- Keep antivirus running and up to date
- Contact the IT/security team if you suspect a malware infection

❖ Password security

Passwords are the most common and easiest-to-use authentication system in existence. Most employees have dozens of online accounts that are accessed by providing a username (often their email address) and a password.

Poor password security is one of the biggest threats to modern enterprise security.

Password construction:

- The password shall contain more than eight characters.
- The password shall not be a word found in a dictionary (English or foreign).
- The password shall not be a derivative of the user ID, e.g., <username>123.
- The password shall not be slang, dialect, jargon, etc.
- The password shall not be a common usage word, such as names of family, pets, friends, co-workers, fantasy characters, etc.
- The password shall not be based on computer terms and names, commands, sites, companies, hardware, or software.
- The password shall not be based on birthdays and other personal information, such as addresses and phone numbers.
- The password shall not be a word or number pattern like aaa bb, qwerty, zyxwvuts, 123321, etc., or any of the above spelled backward.
- The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g.,!@# $%^&*()_+|~-=\`{}[]:";'<>?,./).

# Some important password security tips to include in training content:

- Always use a unique password for each online account
- Passwords should be randomly generated
- Passwords should contain a mix of letters, numbers, and symbols
- Use a password manager to generate and store strong passwords for each account
- Use multi-factor authentication when available to reduce the impact of a compromised password

❖ Safe internet habits

Security training programs should incorporate safe internet habits that prevent attackers from penetrating your corporate network. Some important content to include in training:

- The ability to recognize suspicious and spoofed domains (like yahooo.com instead of yahoo.com)
- The differences between HTTP and HTTPS, and how to identify an insecure connection
- The dangers of downloading untrusted or suspicious software from the internet
- The risks of entering credentials or login information into untrusted or risky websites
- Protect Your Personal Information With Strong Passwords
    1. When creating a new password, pay attention to strong password requirements.
    2. Change your passwords often.
    3. Don't share your passwords with other people.
- Keep Personal Information Private
    1. When you sign up for something online, read the terms and conditions.
    2. Never enter your financial information on a website that isn't secure (look for the padlock or "HTTPS://" prefix in the browser address bar).
    3. If you suspect your credit card information is being misused online, turn off your card using the mobile banking app or contact the bank.
- Make Sure Your Devices Are Secure
    1. Utilize passwords and other security options like fingerprint readers and face scanning technology. One report stated that 30% of smartphone users didn't use passwords, screen locks, or other security features to lock their phones.
    2. Secure *all* devices, including computers, phones, tablets, and devices like smartwatches and smart TVs.
- Pay Attention to Software Updates
    1. Promptly install software updates, especially when they include important security upgrades.
    2. Set up automatic updates on your devices so you never miss one!
- Be Careful About Wifi
    1. Do not trust public wifi security. Avoid connecting to unsecured public wifi networks.
    2. Make sure your wifi networks are protected with strong passwords.
    3. Remember tip #1 and change your wifi password frequently.
- Set Up Two-Factor Authentication
    1. Enable two-factor authentication to prevent hackers from accessing your accounts and information. Add this extra layer of security to keep your accounts safe even if someone knows your password.
- Back Up Your Personal Data
    1. Back up important personal information on external hard drives.
    2. Create new backups regularly.

❖ **Social networking**

Enterprises use social networking as a powerful tool to build a brand (either locally or globally) and generate online sales. Unfortunately, cybercriminals also use social media for attacks that put an organization’s systems and reputation at risk.

To prevent the loss of critical data, the enterprise must have a viable social networking training program that should limit the use of social networking

Inform employees of the threats of social media:

- Phishing attacks can occur on social media as well as over email
- Cybercriminals impersonating trusted brands can steal data or push malware
- Information published on social media can be used to craft spear-phishing emails

# How to Protect Yourself

- Use strong passwords.
- Keep antivirus software up to date.
- Update the security and privacy settings offered by social networking services to ensure the strongest settings possible.
- Avoid suspicious third-party applications.
- Treat everything as public.
- Share only with people you know.

❖ Removable media

Removable media (such as USBs, CDs, and so on) are a useful tool for cybercriminals since they enable malware to bypass an organization’s network-based security defenses. Malware can be installed on the media and configured to execute automatically.

Removable media can take many forms :

- USB Drives (Pen Drives, Portable Hard Drives)
- Smartphones, music players, and similarly equipped handheld devices
- SD Cards
- Optical Media (CDs, DVDs, Blu-ray)

Prevention Measures:

1. Install anti-malware/anti-virus software on your computer.
2. Disable the auto-run and autoplay features.
3. Implement access controls to protect the data on removable media by password-protecting your removable media or device.
4. Make sure that all removable media and devices are encrypted.
5. Do not allow USB flash drives to be used within an organization.

Employees should be trained to properly manage untrusted removable media:

- Never plug untrusted removable media into a computer
- Bring all untrusted removable media to IT/security for scanning
- Disable autorun on all computers

❖ Physical security

Like cyber-attacks, physical security breaches are often a result of human error or negligence. Developing employees' physical security awareness helps ensure they remain alert to breaches and other potential risks to your personnel, facilities, and other assets.

Employees should be aware of potential security risks in the physical aspects of the workplace, such as:

1. Tailgating:

Tailgating is when an unauthorized person follows an authorized person into a secure area.

This will naturally happen as multiple people pass through doors, and only the front has to present identification or a swipe card. The people following behind will simply follow through, making it easy for any unauthorized person to get in without any difficulty.

Reduce tailgating by providing physical security training for your employees.

2. Theft of documents

Your office is likely to have papers and documents lying around in many places, from desks to printer stations. Sensitive documents can easily become unaccounted for and fall into the wrong hands. Even if they are not taken from the office, a visitor could see information that you wouldn't want them to see.

3. Unaccounted visitors

If you don't know who is or was in your workplace at a specific time, it is impossible to keep a high level of physical security. Unaccounted visitors pose a serious risk, as you will not be able to know if they were present if an incident occurs.

4. Stolen identification

An access control system only works if everyone uses their identification. If people are going in and out of your premises using someone else's identification, the result is the same as if you had no access control at all

5. Social engineering

Social engineering attacks can come in a huge variety of different forms. This is one of the reasons why it is so difficult to combat. Social engineering attacks rely on manipulating your employees, often using information that they have managed to gain to impersonate someone else, or abusing basic human empathy to gain access to secure areas and networks.

6. Insider Threats

Insider threats are employees who inadvertently or intentionally threaten the security of an organization's data.

There are three types of insider threats:

- non-malicious insiders → these are users that can cause harm accidentally, via negligence, or because they are unaware of security procedures.
- Malicious insiders → these are users who actively attempt to steal data or cause harm to the organization for personal gain.
- Compromised insiders → these are users who are not aware that their accounts or credentials were compromised by an external attacker. The attacker can then perform a malicious activity, pretending to be a legitimate user.

Prevention:

- Avoid visitors or new hires watching as employees type in passwords (known as “shoulder surfing”)
- Don’t let in visitors claiming to be inspectors, exterminators, or other uncommon guests without verification, who might be looking to get into the system (called “impersonation”)
- Do not allow someone to follow you through a door into a restricted area
- Don’t leave passwords on pieces of paper on one’s desk
- Don’t leave one’s computer on and unsecured when leaving work for the night
- Don’t leave an office-issued phone or device out in plain sight
- Repair physical security controls (doors, locks, and so on) malfunctioning
- Avoid placing sensitive information on a desk, such as sticky notes, papers, and printouts that can be easily taken by thieving hands and seen by prying eyes.
- A clean desk policy should state that information visible on a desk should be limited to what is currently necessary.
- Before leaving the workspace for any reason, all sensitive and confidential information should be securely stored.

❖ Data management and privacy

Most organizations collect, store, and process a great deal of sensitive information. This includes customer data, employee records, business strategies, and other data important to the proper operation of the business. If any of this data is publicly exposed or accessible to a competitor or cybercriminal, then the organization may face significant regulatory penalties, damage to consumer relationships, and a loss of competitive advantage**.**

# Important training content includes:

- The business's data classification strategy and how to identify and protect data at each level
- Regulatory requirements that could impact an employee's day-to-day operations
- Approved storage locations for sensitive data on the enterprise network
- Use a strong password and MFA for accounts with access to sensitive data

❖ Mobile App Security

1. Data Leakage

Mobile apps are often the cause of unintentional data leakage. For example, "riskware" apps pose a real problem for mobile users who grant them broad permissions but don't always check security. These are typically free apps found in official app stores that perform as advertised, but also send personal and potentially corporate data to a remote server, where it is mined by advertisers, and sometimes, by cybercriminals.

Data leakage can also happen through hostile enterprise-signed mobile apps. These mobile malware programs use distribution code native to popular mobile operating systems like iOS and Android to move valuable data across corporate networks without raising red flags.

2. Unsecured Wi-Fi

No one wants to burn through their cellular data when wireless hot spots are available, but free Wi-Fi networks are usually unsecured. To be safe, use free Wi-Fi sparingly on your mobile device. And never use it to access confidential or personal services, like banking or credit card information.

3. Network Spoofing

Network spoofing is when hackers set up fake access point connections that look like Wi-Fi networks but are traps in high-traffic public locations such as coffee shops, libraries, and airports. Cybercriminals give access points common names like "Free Airport Wi-Fi" or "Coffeehouse" to encourage users to connect.

Because many users employ the same email and password combination for multiple services, hackers are then able to compromise users' email, e-commerce, and other secure information. In addition to using caution when connecting to any free Wi-Fi, never provide personal information. And whenever you are asked to create a login, whether for Wi-Fi or any application, always create a unique password.

4. Phishing Attacks

Because mobile devices are always powered on, they are the front lines of most phishing attacks. According to CSO, mobile users are more vulnerable because they often monitor their email in real-time, opening and reading emails when they are received. Mobile device users are also more susceptible because email apps display less information to accommodate the smaller screen sizes. For example, even when opened, an email may only display the sender's name unless you expand the header information bar. Never click on unfamiliar email links. And if the matter isn't urgent, then let the response or action items wait until you're at your computer.

5. **Spyware**

Although many mobile users worry about malware sending data streams back to cybercriminals, there's a key threat closer to home: Spyware. In many cases, it's not malware from unknown attackers that users should be worried about, but rather spyware installed by spouses, coworkers, or employers to keep track of their whereabouts and activity. Also known as a stalker, many of these apps are designed to be loaded on the target's device without their consent or knowledge. A comprehensive antivirus and malware detection suite should use specialized scanning techniques for this type of program, which requires slightly different handling than other malware, owing to how it gets onto your device and its purpose.

# Prevention:

1. Enforce Strong Authentication **:**

- something that a user knows, such as a password or PIN
- something the user has, such as a mobile device
- or something the user is, such as a fingerprint.

2. Scan Mobile Apps for Malware **:**

- Eliminate malware and adware by testing apps for malicious behavior.
- Malware can be detected using virtual sandboxing or signature-based scanning tools.
- For mobile workspace or virtual mobile solutions, perform malware scans on the server.

3. Optimise Data Caching

- This is a major cause of security issues because those apps and devices become more vulnerable, and it is relatively easy for attackers to breach and decrypt the cached data. This often results in stolen user data.
- You can require a password to access the application in case the nature of your data is extremely sensitive. This will help reduce vulnerabilities associated with cached data.
- After that, set up an automatic process that wipes cached data whenever the device gets restarted. This helps reduce the cache and mitigate security concerns.

❖ Financial Transaction Security

Online banking and shopping are some of the perks of our tech-savvy culture. But providing financial information for online activities can put your money (and your identity) at risk. The key to safe online financial transactions is to be informed and cautious.

- Be Aware of Fake Emails for Online Financial Transactions
- Update Regularly for Online Financial Transactions
- Buy from Secure Websites for Online Financial Transactions
- Use a VPN for Online Financial Transactions
- Don’t Save Your Payment Information for Online Financial Transactions
- Create Strong Passwords for Online Financial Transactions

# Prevention

- Monitor Your Credit Reports:

Keeping an eye on your credit is an important way to make sure no one is trying to mess with your personal financial information. If you want to see who is making inquiries about your credit, you can request a free credit report.

- Be On the Lookout For Unusual Statements Or Bills:

Pay attention to statements, receipts, and bills. If you’re signed up for electronic bills or statements, it’s easy for them to get lost in your email inbox. Regularly looking at statements will help you notice if there is suspicious activity happening in any of your accounts. If you become a target for fraud, you’ll want to catch it as soon as possible and contact your bank for help.

- Shred Documents Containing Financial Or Personal Information:

Don’t throw sensitive documents in the trash. Use a paper shredder or shredding service to dispose of anything with your full name, phone number, address, social security number, bank account information, or other private personal details. Check out helpful shredding guides, and consider shredding documents such as:

1. ATM Receipts
2. Bank and Credit Card Statements
3. Paid Bills and Invoices
4. Pay Stubs
5. Credit Offers

❖ Social Media and Social Engineering

Online scammers are always coming up with new ways to manipulate people on the internet. Be on the lookout for social media scams like fake profiles, catfishing, gossip clickbait, job offer scams, and fake online scams. A good rule of thumb is to always check the validity of a website before allowing it to access your personal information. Never click on suspicious links, and don’t fill out online forms unless the website is legitimate and secure.

1. Celebrity & Company Impersonators

Although many fake celebrity profiles are created in good fun, cyber attackers also frequently pose as someone famous. Hackers can leverage credible or noteworthy names to get victims to click on a malicious link out of curiosity.

And since celebrity photos and information are readily available across the web, it's fairly easy for a criminal to cook up a fake profile in a matter of minutes. Perhaps a more dangerous form of impersonation occurs when impostors pretend to be a real company on social media and respond to consumer complaints, in an attempt to harvest account details.

□ How to Detect and Avoid a Social Media Impersonator:

- Look for a “verified” badge. If a profile portrays someone famous, look for a “verified” blue checkmark next to the owner's name.
- Check the profile's details. If the profile was recently created, has little activity, a minimal following, or zero contacts in common with you, be suspicious.
- Perform your search. If you're looking to follow a company or someone famous, do a Google or Web search to find their real social media profile for yourself.
- Never share account information on social media. Legitimate companies should never contact you on social media and ask for your account information.
- If someone calls in response to your social media complaint, be wary of sharing information. If in doubt, hang up the phone, wait five minutes, and call the company's direct customer service line to verify.

2. Profile Hijacking

A profile hijack is a type of identity theft where the criminal poses as a friend or family member on social media to earn your trust and eventually trick you into sending money or clicking on a malicious link. Two main types of profile hijacking can occur:

1. Cloned Account: A criminal creates a fake account impersonating someone you know.
2. Hacked Account: A criminal hacks into a person’s real account, changes their password, and uses their network to scam unsuspecting friends and family.

□ Ways to Detect and Avoid a Hijacked Profile

- Keep your profile information private. Make use of your privacy settings to avoid being hijacked yourself.
- Verify requests with common friends. Before you accept a friend request, check for other friends you have in common with the profile and signs of their long-term social profile usage (number of friends, posts, photos, etc.). You could even go so far as to call or text the friend to verify they're the one who sent the request.
- Be wary of changes in tone and money requests. If a friend doesn't sound the way they usually do when you chat in person or if they are directly asking you for money or financial assistance, be suspicious.

3. Catfishing & Romance Scams

Thanks to online match sites and popular dating apps, it's estimated that nearly 1 in 5 relationships now begin online (Psychology Today). However, criminals are also using the backdrop of online dating as an opportunity to con victims into giving away money or worse. These types of scams are often referred to as “catfishing.”

Catfishers are extremely adept at gaining the victim's trust, sometimes putting in weeks or months of messages and conversations before ever asking for money. When they do finally make the ask, they'll say it's for something like a "plane ticket" to finally meet in person or help an ailing relative, only to back out at the last minute or never be heard from again.

In worst-case scenarios, predators have used social media in an attempt to lure victims into human trafficking

□ How to Detect and Avoid a Romance Scammer:

If you meet someone online through a dating site or social media App, watch out for these warning signs:

- It sounds too good to be true. They’re too good-looking or rich, have a glamorous job, and so on. If someone sounds too good to be true, they're usually not real.
- Professing love quickly, without actually meeting you. Oftentimes, a scammer will express strong emotions (potentially even love) before meeting you. If someone is in a rush to move the relationship along, be suspicious.
- Attempting to lure you off the dating site. Scammers prefer that you leave the dating site and start using a personal email or instant messaging to continue communication. This makes it easier to scour your personal information, starting with your primary email address.
- Giving excuses not to meet you in person or video chat. If a scammer plans to visit but always cancels at the last second, stop interacting with them immediately. This is one of the biggest red flags that the person is not who they say they are. If you do meet in person, arrange to meet in a public place and make sure a friend or family member knows where you are.
- Asking for money or things from you. Be suspicious of anyone who asks you for financial assistance, no matter how dire they claim their circumstances are. Common storylines include sick relatives, short-term loans for plane tickets, startup money for a business venture, or a service member overseas who needs money.

4. Gossip Clickbait

“Clickbait” headlines and messages feed on a human being's curiosity through misleading or sensationalized text. Some clickbait is harmless, and just an attempt to ratchet up web traffic; however, other clickbait can lead to hidden dangers like malware or viruses that put your private data in jeopardy.

One piece of prominent chain clickbait spam involves a message from someone you know, claiming to have proof or a photo that you did something scandalous. If you click on the link, a malicious bot sends the same message to all your friends, and the chain keeps going. In the meantime, the link may also have included malware that has compromised your information.

□ How to Detect and Avoid Clickbait Spam and Scams:

- No name? No click. If a general message with a link doesn't explicitly say your name, ignore it or delete it. Even if it comes from someone you know.
- Contact your friend differently. If you receive a suspicious message from a friend, verify through a text or phone call that they sent it.
- Don't click on unrecognizable links. Before clicking on a shortened URL on social media, use a link-lengthening service such as Check Short URL to verify the source.

Prevention:

- Think twice before posting anything. Even if you delete it, posts can live forever in screen captures and may lose context.
- When away from home for extended periods, don’t reveal your location. Watch out for the information you share in photos.
- Customize your privacy settings to be as restrictive as possible regarding who can read and see posts. Consider an account for people you trust and another for public use.
- Use multi-factor authentication.
- Don’t click on links, files, games, or applications within the confines of social media. While it’s difficult to mitigate the risk of being victimized by profile cloning, ensuring your company’s antimalware tools are up to date is a step in the right direction. Try to foster a culture of not clicking on links, even from people employees know.

Cyber safety tips - protect yourself against cyberattacks

1. Update your software and operating system: This means you benefit from the latest security patches.

2. Use anti-virus software: Security solutions will detect and remove threats. Keep your software updated for the best level of protection.

3. Use strong passwords: Ensure your passwords are not easily guessable.

4. Do not open email attachments from unknown senders: These could be infected with malware.

5. Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that malware is spread.

6. Avoid using unsecured WiFi networks in public places: Unsecured networks leave you vulnerable to man-in-the-middle attacks.