A COMPLETE GUIDE TO

CYBERSECURITY AWARENESS

FOR MORE INFORMATION CONTACT US AT
sales@mailsafi.com

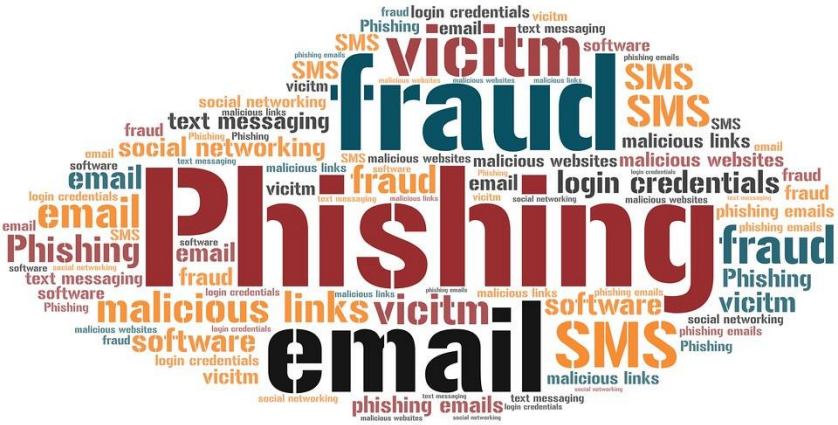
Table of contents

Contents

Cybersecurity Awareness 101: Protecting Yourself Online

As more sensitive data moves online and threats grow more sophisticated, it is vital that everyone knows how to protect themselves in cyberspace. That is why we created this resource as part of Cybersecurity Awareness Month.

The goal of this guide is to provide individuals with actionable information on key cybersecurity best practices. While technology brings many conveniences, it also comes with added responsibilities. We hope this guide will help readers develop sound cyber hygiene habits that lead to greater vigilance and safety when using digital systems and services. Cybersecurity is a shared challenge - with cooperation and education, individuals and organizations can learn how to effectively minimize risks. Let us work together in building a culture of cyber awareness.



Types of Cyber Threats

Cybercriminals employ various techniques to breach security systems and gain unauthorized access to data or networks. Being aware of the most prevalent threats is key to improving vigilance.

Malware

Malware refers to malicious software programs designed to infect, damage, or gain control of computer systems. Malware includes viruses, worms, trojans, spyware, adware, and other unwanted programs that can disrupt operations, steal data and enable cyber attacks.

Phishing

Phishing involves scammers using fraudulent messages and websites to deceive victims and trick them into sharing sensitive information or installing malware. Phishing can occur via email, text messages, phone calls, and social media.

Ransomware

Ransomware is a form of malware that encrypts important files and data until a ransom is paid. Ransomware often spreads through infected email attachments and compromised websites. Paying the ransom does not guarantee the return of your data.

Social engineering

Social engineering relies on psychological manipulation to trick users into handing over confidential information or granting access to systems. This could involve impersonating trusted entities or appealing to natural human emotions and tendencies.

Strong Passwords and Authentication Management

"Your password is the key to your digital life; make it strong, unique, and something only you hold."

Using strong, unique passwords is one of the most basic yet critical steps for security. Passwords act as the frontline defense to protect access to devices, accounts and sensitive data.
What you need to do is;

- Create long passwords at least 12 characters in length, using a mix of letters, numbers and symbols. Avoid common words, phrases or personal information.
- Use a unique password for every account. Password reuse allows compromise of one account to spread.
- Consider using a password manager to securely store and organize passwords.
- Never share passwords publicly, in emails or over the phone. Watch for shoulder surfing.
- Change passwords periodically and immediately if compromised. Don't just tweak existing passwords.

Multi-factor authentication (MFA) provides an added layer of security beyond passwords. MFA requires users to verify through two or more credentials when logging in, like a one-time code sent to your phone. Enabling MFA is highly recommended to enhance account security.

With a strong, unique password and MFA properly implemented, users create a robust barrier against unauthorized access by cybercriminals.

Recent Data Breaches and Cyber Attacks

10/17/2023

Hong Kong Ballet Reports Data Breach From Ransomware Attack

Hong Kong Ballet has reported a data breach caused by a ransomware attack on its computer systems. In an official statement released on Oct. 16, the renowned cultural institution said it had recently discovered its network systems had been infected with ransomware, allowing intruders to illegally access files stored on computers. Data including personal user details and the organisation's internal information had been viewed by the intruders, the company said, adding it was still working to determine the full scope of the attack. The ballet institution, financially backed by the government, said it had launched an internal investigation upon detecting the incident and hired external cybersecurity experts to assess the extent of the breach and implement measures, and also notified police and the Office of the Privacy Commissioner for Personal Data. Full Story

Source: South China Morning Post

10/16/2023

Long Island Fortune 500 Company Suffered Cyber Incident, Took Systems Offline

On Oct. 14, Melville, N.Y.-based Henry Schein, Inc. (Nasdaq: HSIC) determined that a portion of its manufacturing and distribution businesses experienced a cybersecurity incident. They promptly took certain systems offline and other steps intended to contain the incident, which has led to temporary disruption of some of its business operations. The Company is working to resolve the situation as soon as possible and has engaged outside cybersecurity and forensic information technology experts to help investigate any data impact and respond to this situation, and they have notified relevant law enforcement authorities. Henry Schein is a solutions company for health care professionals with operations or affiliates in 33 countries and territories, and sales of $12.6 billion in 2022. Press Release

Source: Businesswire

10/14/2023

CDW Investigating Ransomware Gang Claims Of Data Theft

The multibillion-dollar technology services firm CDW said it is investigating claims made by a ransomware gang that data was stolen during a cyberattack. A spokesperson for the company – which reported revenues over $23 billion in 2022 – said they are currently "addressing an isolated IT security matter associated with data on a few servers dedicated solely to the internal support of Sirius Federal, a small U.S. subsidiary of CDW-G." CDW-G is a secondary division of the company dedicated to providing technology services to U.S. government organizations like schools, hospitals and state-level

entities. The LockBit ransomware gang allegedly demanded an $80 million ransom in return for the data but was only offered $1 million.
Source: The Record

10/13/2023

Cloud Gaming Firm Shadow Says Hackers Stole Customers' Personal Data

Paris-based cloud gaming startup Shadow has confirmed a data breach involving customers' personal information including full names, email addresses, dates of birth, billing addresses and credit card expiry dates. "At the end of September, we were the victim of a social engineering attack targeting one of our employees," Shadow CEO Eric Sèle said in an email this week. "This highly sophisticated attack began on the Discord platform with the downloading of malware under cover of a game on the Steam platform." An individual who posted on a popular hacking forum on Oct. 11 claiming responsibility for the Shadow breach said they are selling the stolen database, which allegedly contains the data of 530,000 Shadow customers. The company is advising customers to be wary of suspicious-looking emails and to set up multi-factor authentication on their accounts.
Source: TechCrunch

10/12/2023

Simpson Manufacturing Hit By Cyberattack, Working To Investigate

Simpson Manufacturing Co. (NYSE: SSD), an engineering and building materials producer, said it was the subject of a cybersecurity incident on Oct. 11 that disrupted its IT infrastructure and applications. The Pleasanton, Calif.-based company has hired third-party experts to support a probe and recovery efforts. "The investigation to assess the nature and scope of the incident remains ongoing and is in its early stages," the company said in a regulatory filing. SSD took some of its systems offline in order to stop and remediate activity stemming from the incident, according to a report filed with the SEC. The stock has gained 61 percent in the year to date, while the S&P 500 has gained 13.5 percent. SSD has annual revenues of over $2 billion and more than 5,158 full time employees.
Source: MarketWatch

10/11/2023

UK-Based Tech Manufacturing Giant Volex Hit With Cyberattack

One of the biggest manufacturing technology providers in the world was hit with a cyberattack this past weekend that affected its IT systems at several international sites. Volex plc (AIM:VLX), a U.K-based company that produces a range of power products for data centers, electric vehicles and more, said on Oct. 9 that hackers gained access to some of its IT systems and data. "On becoming aware of the incident, the Group enacted its established IT security protocols and took immediate steps to stop the unauthorized

access to its systems and data," they said in a cyber incident notice. Volex has been a major player in the electrical products space for more than a century, reporting revenues in 2023 of more than $722 million. They have 19 manufacturing locations and 11,500 employees across 24 countries.
Source: The Record

10/10/2023

Spanish Airline Air Europa Hit By Credit Card System Breach

Spanish airline Air Europa said today it suffered a cyberattack on its online payment system that left some of its customers' credit card details exposed. The airline emailed customers whose credit card details were affected and notified the relevant financial institutions, it said in a statement. Passengers who have recently purchased tickets were urged to immediately cancel their bank cards, since the hackers have obtained the key data to be able to make purchases with those payment systems. The airline did not specify the number of customers affected, nor did it estimate the financial impact of the cyberattack. The company said no other information has been exposed. Madrid-based Air Europa, Spain's third largest airline, is in the process of being taken over by British Airways-owner International Consolidated Airlines Group.
Source: Reuters

10/07/2023

23andMe User Data Stolen In Targeted Attack On Ashkenazi Jews

The genetic testing company 23andMe confirmed on Oct. 6 that data from a subset of its users has been compromised. The company said that attackers gathered the data by guessing the login credentials of a group of users and then scraping more people's information from a feature known as DNA Relatives. Users opt into sharing their information through DNA Relatives for others to see. Hackers posted an initial data sample on the platform BreachForums earlier this week, claiming that it contained one million data points exclusively about Ashkenazi Jews. There also seem to be hundreds of thousands of users of Chinese descent impacted by the leak. On Oct. 4, the actor began selling what it claims are 23andMe profiles for between $1 and $10 per account, depending on the scale of the purchase.
Source: WIRED

10/06/2023

Australia's Home Affairs Department Hit By DDoS Attack Claimed By Pro-Russia Hackers

The department responsible for Australia's cybersecurity, national security and immigration has confirmed it was hit with a distributed denial-of-service attack on Oct. 5 that took its website offline for five hours, after a pro-Russia hacker group said it would target the site over Australia's support for Ukraine. The group posted on Telegram that it was targeting the home affairs department with a

distributed denial-of-service (DDoS) attack after Australia announced this week that Slinger technology aimed at combating drones would be sent to Ukraine in the push back against the Russian invasion. The home affairs website was taken down mostly while Australia was sleeping – between 10pm and just after 3am AEDT.
Source: The Guardian

How to Recognize Phishing Attempts

Phishing is a deceptive and malicious practice in which cybercriminals impersonate trusted entities or individuals to trick you into revealing sensitive information or taking harmful actions. They typically use various communication channels to carry out their schemes. Here are some common forms of phishing:

Email Phishing: In email phishing, attackers send fraudulent emails that appear to be from legitimate organizations, urging you to click on malicious links or provide personal information like passwords or credit card details.

Text Phishing (Smishing): Smishing involves sending fraudulent text messages, often containing links or phone numbers, with the aim of tricking you into revealing personal information or taking actions that can compromise your security.

Voice Phishing (Vishing): Vishing uses phone calls, often automated or pre-recorded, to deceive you into sharing sensitive data or following specific instructions. These calls can impersonate banks, government agencies, or even tech support.

Identifying Phishing Attempts

Recognizing phishing attempts is crucial to protect yourself from falling victim. Here are some tips to help you spot phishing attempts:

1. Check the Sender's Email Address: Examine the sender's email address closely. Phishers may use a slightly altered domain or a free email service.

2. Beware of Urgency and Threats: Phishing emails often create a sense of urgency or threaten negative consequences if you don't act immediately. Be cautious when you see such tactics.

3. Inspect Links and URLs: Hover your mouse over links in emails or text messages to see the actual URL before clicking. Verify that it matches the official website of the organization it claims to be from.

4. Watch for Spelling and Grammar Errors: Many phishing attempts contain spelling mistakes or awkward grammar. Legitimate organizations typically proofread their communications.

5. Think Before You Share: Be skeptical about sharing personal information online, especially if you didn't initiate the communication. Legitimate organizations won't ask for sensitive data through email, text, or phone calls.

6. Don't Trust Caller IDs Blindly: Vishing calls may spoof caller IDs to appear genuine. If you receive a call requesting personal information, hang up and call the organization back using a verified phone number.

What to Do When You Encounter Phishing

If you come across a phishing attempt, follow these steps:

- Do not click on any links or open attachments in suspicious emails or texts. Clicking can trigger malware downloads or direct you to phishing sites to steal your information.
- Do not reply to the suspicious message. Replying alerts the sender that your email/number is active, potentially enabling further attacks.
- Report phishing emails by forwarding them as attachments to your organization's IT/security team. Provide key details like sender address. Reporting helps block future attacks.
- For phishing calls, hang up immediately. Do not provide any personal information over the phone, even just to confirm identity.
- Double check the sender's email and web addresses carefully. Phishers often create lookalike domains.
- Verify out-of-band using known contact information before taking any requested action, like resetting a password or sending money. Do not trust contact info in the message alone.
- Install anti-phishing browser extensions that cross check sites against blacklists of known scams and highlight suspicious URLs or content.
- Clear browser cookies/caches after clicking any links in suspicious messages to erase potential tracking tools. Run anti-malware scans to check for infections.
- Change any compromised credentials immediately if you accidentally provided information on a phishing site. Notify affected companies.

How to Protect Personal Information

Your personal information is invaluable, and safeguarding it is key. Data privacy is not just a matter of keeping your information safe; it's about preserving your identity, security, and personal freedom for example

I. Identity Protection: Your personal information, such as your name, address, and date of birth, is what makes you, well, you. Protecting this data prevents identity theft and fraud.

II. Financial Security: Financial information, like bank account details and credit card numbers, is a prime target for cybercriminals. Safeguarding it is vital to avoid financial losses.

III. Personal Freedom: Maintaining data privacy helps you control your online presence and reputation. It keeps you safe from scams and harassment, allowing you to interact online with confidence.

IV. Preventing Cyberattacks: When you protect your personal information, you're also fortifying your digital defenses. Cybercriminals often use your data to craft phishing attempts and other cyberattacks.

Tips for Protecting Personal Information Online

Here are some practical steps you can take to safeguard your personal information online:

- Use Strong, Unique Passwords: Create complex and unique passwords for your online accounts. Avoid using easily guessable information like birthdays or "password."

- Enable Two-Factor Authentication (2FA): Whenever possible, enable 2FA on your accounts. This adds an extra layer of security by requiring a second verification step.

- Beware of Sharing: Be cautious about sharing personal information on social media. Cybercriminals often gather data from your profiles to craft targeted attacks.

- Use Secure Websites: Look for the padlock symbol (https://) in your web browser's address bar when sharing sensitive information. It signifies a secure connection.

- Review App Permissions: When installing apps, review the permissions they request. Only grant necessary access to your data.

- Regularly Monitor Your Accounts: Keep an eye on your financial and online accounts for any suspicious activity. The sooner you spot a problem, the easier it is to resolve.

- Install Updates and Patches: Regularly update your device's operating system, apps, and security software. Updates often include fixes for security vulnerabilities.

- Avoid Public Wi-Fi for Sensitive Transactions: Public Wi-Fi networks can be insecure. Avoid conducting sensitive transactions, such as online banking, on public Wi-Fi.

Effective Use of Privacy Settings

Take advantage of privacy settings on social media platforms and online services. Here's how to make the most of them:

- Adjust Visibility: Customize who can see your posts and profile information. You can often choose to share with friends, specific groups, or the public.

- Review App Access: Periodically review and revoke access for apps that you no longer use or trust.

- Limit Personal Information: Share only essential information on your profiles. Minimize the details you provide, such as your address and phone number.

- Understand Data Sharing: Be aware of what data you're sharing with the platform and how it's being used. Read privacy policies and terms of service.

- Regularly Update Privacy Settings: Platforms may change their settings and policies. Check and update your settings as needed to maintain your desired level of privacy.

General Guidelines for Securing Your Devices

Your devices, whether it's your smartphone, computer, or anything in between, play a crucial role in your daily life. Keeping them safe is a top priority when it comes to cybersecurity awareness.

Besides software updates and security software, there are some general rules you should follow:

1. Use Strong, Unique Passwords: Ensure your device is locked with a strong and unique password or PIN. This adds an extra layer of protection in case it's lost or stolen.

2. Lock Your Device: Enable a screen lock to prevent unauthorized access. Whether it's a fingerprint, face recognition, or a PIN, it keeps your device and your data secure.

3. Be Cautious with App Downloads: Only download apps from official app stores, like the Apple App Store or Google Play. Avoid downloading apps from untrusted sources.

4. Review App Permissions: Regularly check and limit the permissions you grant to apps. Not all apps need access to everything on your device.

5. Backup Your Data: Regularly backup your important data, just in case something goes wrong.

Why you should Regularly update the Software

Think of your device's software as the front door to your digital world. Just like you'd lock your front door to keep unwanted guests out, regularly updating your device's software is like securing it against digital intruders. Here's why it's so important:

Security Patches: Software updates often include important security patches that fix vulnerabilities that cybercriminals could exploit. By keeping your software up-to-date, you're making it harder for them to break in.

Improved Features: Updates can also bring new and improved features, making your device work better and smarter.

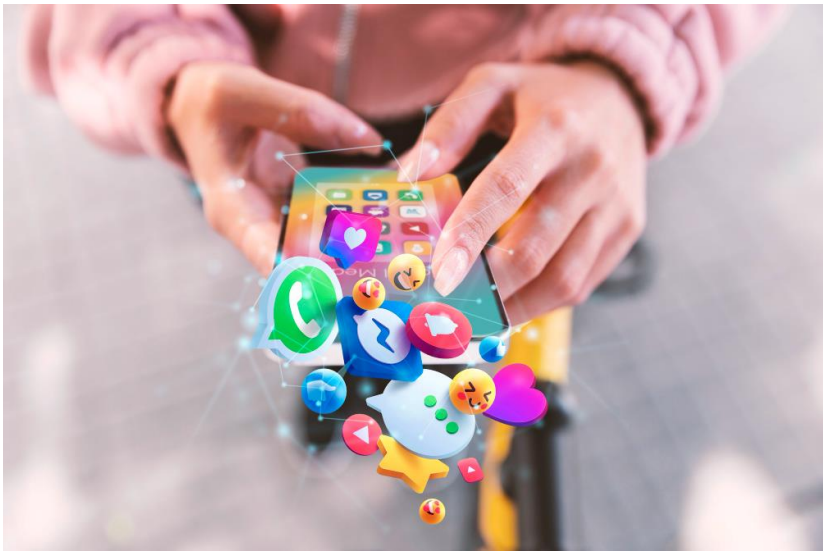
Reliability: Outdated software can slow down your device and cause it to crash. Regular updates keep your device running smoothly.

So, the next time your phone, computer, or tablet nudges you to update, don't ignore it. It's a small but crucial step in your cybersecurity journey.

Use Antivirus and Anti-Malware Software

You wouldn't leave your home unprotected without some form of security, right? Your digital devices are no different. Antivirus and anti-malware software act as guards for your device against threats such as viruses worms, and other malware that may infect your systems.

Social Media and Online Behavior



Social media is a wonderful way to connect, share, and interact with others, but it's essential to maintain a level of caution to protect your privacy and security.

How to practice a safe social media behavior:

Avoid Oversharing Personal Information: While sharing aspects of your life is natural, avoid oversharing sensitive personal information, like your home address, phone number, or detailed daily routines. This information can be exploited by cybercriminals.

Adjust Privacy Settings: Most social media platforms allow you to customize your privacy settings. Review and configure these settings to control who can see your posts and personal information. Choose settings that align with your comfort level.

Be Wary of Friend Requests: Only accept friend requests or follow requests from people you know or have a legitimate reason to connect with. Cybercriminals often use fake profiles to gather information.

Think Before You Post: Before sharing a post, consider the potential consequences. Once something is online, it's challenging to control who sees it and how it's used.

Secure Your Account: Use strong, unique passwords for your social media accounts and enable two-factor authentication whenever possible. This reduces the risk of unauthorized access.

Verify the Authenticity of Online Content: Verifying the authenticity of online content is essential to avoid falling victim to misinformation, scams, or fake news.

With the above measures in place, it is important for further measures to be set in place for additional security. These include

Check the Source of the content: Examine the source of the content. Is it from a reputable news organization, government agency, or a well-known website? Independent verification can be necessary for less-known sources.

Cross-Reference Information: Look for multiple sources reporting the same information. If multiple credible sources corroborate a story, it's more likely to be accurate.

Look for Citations: Authentic content often includes citations and references to primary sources. These citations provide a way to trace information back to its origins.

Use Fact-Checking Websites: Fact-checking websites like Snopes, FactCheck.org, and PolitiFact can help verify the accuracy of claims and stories.

Be Skeptical of Sensational Claims: Extraordinary claims often require extraordinary evidence. If a story seems too good (or bad) to be true, it might be a hoax.

Check Dates: Ensure that the content is up-to-date. Outdated information can be misleading, especially in fast-paced fields like technology and politics.

Look for Visual Clues: Doctored images and videos can be used to mislead. Reverse image searches and video analysis tools can help determine if content has been manipulated.

Wi-Fi and Network Security

Securing your home Wi-Fi network is important to protect your devices and personal data from an array of cyber threats.

Encryption: Encryption is like a secret code for your data. It scrambles information so that only someone with the proper "key" can unscramble and read it. Without strong encryption, your data could be intercepted and stolen. WPA3 encryption, as mentioned earlier, is currently one of the most secure methods.

Router Settings: Your router is the hub of your home network. Its settings control how devices connect and communicate. If an attacker gains access to your router settings, they can compromise your entire network. By changing default settings, you make it much more challenging for cybercriminals to exploit vulnerabilities.

These tips can help ensure your network's security:

Change Default Router Credentials: The default usernames and passwords for routers are widely known, making them vulnerable to unauthorized access. Change these credentials to something strong and unique.

Enable WPA3 Encryption: WPA3 is the latest and most secure Wi-Fi encryption protocol. Ensure your router and devices support it, and set it up to protect your network from eavesdropping.

Use a Strong Network Name (SSID): Avoid using obvious or easily identifiable SSIDs. A unique name makes it harder for attackers to identify your network.

Implement a Strong Wi-Fi Password: Create a complex Wi-Fi password that includes a mix of letters, numbers, and special characters. Longer passwords are generally more secure.

Enable Network Encryption: Ensure your network traffic is encrypted. Use secure protocols like WPA2 or WPA3, and avoid leaving your network open (unsecured).

Keep Router Firmware Updated: Regularly update your router's firmware to patch security vulnerabilities. Check your router manufacturer's website for updates.

Change Default IP Addresses: Changing the default IP address of your router can add an extra layer of security. Most routers use common default addresses, making them an easy target for attackers.

Safe Downloads and Online Shopping

Downloading files and engaging in online shopping are everyday activities, but they come with potential risks. In this section, we'll explore the dangers of downloading from untrusted sources and provide guidelines for safe online shopping and financial transactions.

Dangers of Downloading from Untrusted Sources

Downloading from untrusted sources can expose your devices and data to a range of risks. Here are some key dangers to be aware of:

Malware and Viruses: Untrusted downloads, especially from shady websites or peer-to-peer networks, can contain malware and viruses that can infect your device and compromise your data.

Privacy Violations: Some downloads may include tracking software or spyware that monitors your online activities and collects personal information without your consent.

Legal Consequences: Downloading copyrighted material without permission, such as movies or software, from untrusted sources may result in legal repercussions.

Fake or Fraudulent Software: Unverified sources can distribute counterfeit or tampered software, putting your device's security at risk and potentially causing system instability.

Guidelines for Safe Online Shopping and Financial Transactions

Safe online shopping and financial transactions are essential for protecting your personal and financial information. Here are guidelines to follow when making purchases online:

1. Shop from Trusted Websites: Stick to well-known, reputable online retailers. Look for secure, encrypted websites with "https://" in the URL, and research the seller's reputation before making a purchase.

2. Use Secure Payment Methods: Use credit cards or secure payment services like PayPal for online transactions. These methods often offer additional protection and fraud prevention.

3. Avoid Public Wi-Fi: Avoid making financial transactions on public Wi-Fi networks, as they may not be secure. Use a secure, private network for online shopping.

4. Verify the Website's Legitimacy: Be cautious of websites that seem too good to be true. Scam websites often offer deals that are too good to pass up. Research the website's reviews and ratings.

5. Check Your Statements: Regularly review your credit card and bank statements to detect any unauthorized or fraudulent charges. Report any suspicious activity immediately.

6. Keep Software Updated: Ensure your device's operating system, antivirus, and browser are up-to-date. This helps protect against security vulnerabilities.

7. Beware of Phishing Emails: Avoid clicking on links in emails that claim to be from online retailers. Instead, manually type the retailer's website address into your browser to ensure you're visiting the correct site.

8. Protect Personal Information: Don't overshare personal information during the checkout process. Only provide necessary information for the transaction, such as shipping and payment details.

9. Use Strong Passwords: Create strong, unique passwords for your online shopping accounts. Enable two-factor authentication if available.

10. Keep Receipts and Confirmations: Save transaction receipts and confirmations as proof of purchase in case of disputes.

Reporting Cyber Incidents

The importance of reporting cyber incidents cannot be overstated. Reporting cyber incidents is not only about individual safety but also the collective security of our digital world.

When reporting a cyber-incident, be as detailed as possible, providing information about the incident's nature, any financial losses, and any evidence you may have. Your report is essential for addressing the incident and preventing further harm.

Here's why reporting is essential:

Preventing Further Damage: When an incident occurs, immediate action can prevent further damage. Reporting allows experts to mitigate the threat and secure vulnerable systems.

Collecting Evidence: Reporting incidents preserves crucial evidence. This evidence can be used to identify and apprehend cybercriminals, potentially preventing future attacks.

National Security: Some cyber incidents may have implications for national security. Reporting helps law enforcement and government agencies respond appropriately.

Protecting Others: By reporting an incident, you contribute to the safety of others who may have fallen victim to the same attack or vulnerability. Timely reporting can lead to alerts and advice for potential victims.

Statistical Data: Incident reports help governments, law enforcement, and cybersecurity organizations understand the evolving landscape of cyber threats. This data informs policy, research, and the allocation of resources.

Additional Resources:

Stay Safe Online (National Cyber Security Alliance): Offers a wealth of information on online safety, resources for businesses, and a variety of cybersecurity awareness materials.
Cybersecurity and Infrastructure Security Agency (CISA): CISA's Cybersecurity Awareness Month page provides resources, tips, and events to help you stay safe online.
OnGuard Online (Federal Trade Commission): Provides practical tips for online safety and cybersecurity.
Stop. Think. Connect.™: A national public awareness campaign offering resources to help individuals and businesses stay safe online.
Cybersecurity Awareness (National Institute of Standards and Technology): NIST provides awareness resources, including posters and tip sheets, to educate individuals and organizations about cybersecurity.