Staying SAFE Online: The Complete Guide to Digital Security and Privacy

Introduction: Navigating the Digital World with Confidence

Our modern lives are inextricably woven into the digital fabric. We work remotely, manage our finances from our palms, connect with loved ones across continents, and command our homes with a simple voice command.[1] This hyper-connectivity has unlocked unprecedented convenience and efficiency. However, this same integration has exponentially expanded what cybersecurity experts call the "attack surface"—the sum of all possible points where an unauthorized user can try to gain access to a system.[4]

The nature of online threats has evolved far beyond the random computer viruses of the past. Today's cyberattacks are sophisticated, often well-funded, and increasingly powered by Artificial Intelligence (AI) to create highly convincing and personalized assaults.[5] The consequences are severe, with the global average cost of a single data breach climbing to a staggering $4.88 million, a clear indicator of the financial devastation these attacks can cause.[5]

In this new reality, cybersecurity is no longer the exclusive domain of IT professionals. It is a shared responsibility and a fundamental life skill. This guide introduces the concept of **cyber hygiene**, a set of simple, routine practices that, like personal hygiene, can drastically improve one's health and safety in the digital world.[9]

To provide a clear, memorable, and actionable structure for building this digital resilience, this guide is built upon the **SAFE** framework. This framework will serve as our blueprint for navigating the complexities of the online world with confidence:

- **S**ecure your digital life.
- Be **A**ware of the threats.
- **F**ortify your privacy.
- Know the **E**mergency response.

By understanding the threats we face and systematically applying the principles of the SAFE framework, any user, regardless of technical expertise, can take control of their digital security and protect what matters most.

Part I: Understanding the Modern Threat Landscape

Before one can build effective defenses, it is essential to understand the nature of the attacks. This section deconstructs the primary threats that individuals and organizations face in the current digital environment. Understanding the "how" and "why" behind these attacks is the first step toward building a robust and resilient security posture.

Chapter 1: The Human Element: How Social Engineering Works

The overwhelming majority of cyberattacks do not begin with a brilliant piece of code exploiting a hidden software flaw. They begin with a simple, deceptive act targeting the most vulnerable part of any system: the human being.

The Psychology of Deception

Social engineering is the art of psychological manipulation, a tactic that exploits human vulnerabilities rather than technical ones.[11] It is the foundation of an astonishing 98% of all cyber-attacks, making it the single most significant threat vector in the digital world.[14]
Attackers masterfully leverage powerful human emotions—fear, urgency, curiosity, greed, and even the desire to be helpful—to bypass our rational thought processes. This emotional manipulation tricks victims into making critical security mistakes, such as clicking a malicious link, wiring money to a fraudulent account, or revealing sensitive login credentials.[13]
The effectiveness of these tactics is not accidental; it is a calculated science. An attacker creating a sense of urgency with a subject line like "URGENT: Account Suspension Notice" exploits our fear of loss, prompting a quick, panicked reaction rather than careful consideration. Similarly, a message offering a prize or exclusive deal preys on curiosity and greed. By understanding and weaponizing these psychological triggers, criminals can turn a person's own instincts against them.

The Attacker's Playbook

While the specific scenarios may vary, most social engineering attacks follow a predictable, multi-stage playbook designed to build trust and manipulate behavior.[13]

1. **Investigation and Reconnaissance:** The attack begins with research. The perpetrator investigates the intended victim to gather background information that will make their subsequent approach more believable. They canvass public sources like social media profiles on Facebook or professional details on LinkedIn, company websites, and news articles to learn about the target's job role, relationships, interests, and recent activities.[14] This information is the raw material for a convincing scam.
2. **Establish Trust (Pretexting):** Armed with personal details, the attacker initiates contact

using a "pretext"—a fabricated scenario designed to establish legitimacy and gain the victim's trust. This often involves impersonating a trusted entity, such as a senior manager, a representative from the victim's bank, a vendor, or a tech support agent from a well-known company.[13] For example, an attacker might send an email to a finance department employee that appears to come from the CFO, using the correct name and title gleaned from the company's website, and referencing a real, ongoing project.

3. **Exploitation and Manipulation:** Once a foundation of trust is established, the attacker leverages it to manipulate the victim into performing a specific action that compromises security. This is the core of the attack. The request might be to click a link to "verify account details," download a "critical software update," authorize an "urgent" wire transfer, or simply reply with a password or multi-factor authentication code.[14] The pretext is designed to make this request seem logical and necessary.
4. **Execution and Disengagement:** After the victim has taken the bait and performed the desired action, the attacker achieves their goal. This could be the theft of credentials, the deployment of malware, or a successful fraudulent financial transaction. The final step is disengagement, where the attacker attempts to cover their tracks to avoid or delay detection.[14]

A crucial insight emerges from this playbook: the digital exhaust we leave online directly fuels the effectiveness of these attacks. The modern culture of "oversharing" on social media has created a goldmine of data for criminals. When individuals publicly post their job title, their manager's name, their vacation schedule, their family members' names, and even answers to common security questions (like a first pet's name or high school mascot), they are inadvertently providing attackers with the exact information needed to craft a highly personalized and believable pretext.[15] This direct causal link means that managing one's public digital footprint is not merely a matter of personal privacy; it is a critical, frontline defense against being targeted by social engineering.

Common Social Engineering Tactics Explained

Attackers employ a variety of well-established tactics to execute their playbook. Recognizing these can help individuals identify a potential attack in progress.

- **Baiting:** This tactic lures victims into a trap with a false promise, exploiting greed or curiosity.[13] A classic example is leaving a malware-infected USB flash drive in a public place like an office lobby or parking lot, labeled "Executive Salaries" or "Confidential." An unsuspecting employee who plugs the drive into their computer will inadvertently install the malware.[16] Online, baiting takes the form of tempting ads for free movie downloads or too-good-to-be-true deals that lead to malicious websites.[16]
- **Scareware:** This method uses fear to manipulate victims. It often involves bombarding a user with false alarms and fictitious threats, such as aggressive pop-up banners that mimic legitimate antivirus software and claim, "Your computer is infected with 37 viruses! Click here to clean now".[13] Clicking the link either prompts the user to pay for worthless,

fake security software or directly installs malware onto their device.

- **Quid Pro Quo:** Latin for "something for something," this scam involves an attacker offering a supposed service in exchange for information or access.[16] For example, a criminal might call an employee, pose as an IT support technician, and offer "free assistance" to speed up their computer. In the process, they will ask for the employee's login credentials to gain access to the network.[16] The core principle here is the exploitation of a victim's desire to receive a benefit.
- **Tailgating (or Piggybacking):** This is a physical social engineering tactic where an attacker gains unauthorized entry into a restricted area by closely following an authorized person. For instance, an attacker dressed as a delivery driver carrying boxes might wait by a secure office door and ask an employee to hold it open for them, thereby bypassing the access control system.[14]
- **Dumpster Diving:** A surprisingly effective, low-tech method where criminals rummage through an organization's or individual's trash to find discarded documents containing sensitive information. Bank statements, pre-approved credit card offers, internal memos, and customer lists that have not been properly shredded can provide a wealth of information for an attacker.[16]

Chapter 2: Anatomy of an Attack: Phishing, Malware, and Ransomware

While social engineering provides the method of entry, the ultimate goal of an attacker is often to steal data or money. This is typically achieved through a combination of phishing to deliver a malicious payload, malware to execute the attack, and in the most destructive cases, ransomware to hold data and systems hostage.

Phishing: The Universal Lure

Phishing is a specific and pervasive form of social engineering where threat actors masquerade as legitimate, trustworthy entities in an attempt to steal sensitive data, such as login credentials, credit card numbers, and other personal details.[11] It is the most common initial attack vector, serving as the starting point for over 70% of all data breaches.[14] Its effectiveness lies in its ability to mimic trusted communications, making it difficult for even wary users to distinguish genuine messages from fraudulent ones.

The landscape of phishing is diverse, with attackers tailoring their methods to the target and platform:

- **Email Phishing:** This is the most common and widely recognized form of phishing. Attackers send deceptive emails that appear to originate from trusted sources like banks, social media platforms, or online retailers. These emails often contain urgent requests, such as asking the recipient to update their account information, or enticing offers to trick them into clicking a malicious link or downloading an infected attachment.[11] A classic example is an email impersonating a bank that warns of "suspicious activity" and directs the user to a fake login page designed to steal their credentials.

- **Spear Phishing:** Unlike the broad-cast approach of general phishing, spear phishing is a highly targeted attack aimed at a specific individual or organization. Attackers use personalized information—gathered from social media or company websites—to craft extremely convincing messages tailored to the recipient's interests, job role, or relationships.[11] For instance, an email to an accountant might pretend to be from their manager, referencing a specific project and requesting an urgent invoice payment to a fraudulent account.
- **Whaling:** This is a specialized form of spear phishing that exclusively targets high-profile individuals within an organization, such as CEOs, CFOs, and other senior executives.[11] The goal is to leverage their authority to trick other employees into making large wire transfers or to gain access to the highest levels of confidential company data.
- **Smishing (SMS Phishing) and Vishing (Voice Phishing):** As communication has shifted to mobile devices, so have phishing attacks. Smishing uses fraudulent text messages (SMS) containing malicious links or instructions to call a fake support number.[15] Vishing involves using phone calls (voice phishing), where an attacker might impersonate a government agent or a bank's fraud department to coax sensitive information out of a victim over the phone.
- **Social Media Phishing:** Attackers exploit the trust inherent in social networks by sending malicious links via direct messages or posts. They may create fake profiles or, more effectively, hijack legitimate accounts to send messages that appear to come from a friend or trusted contact, dramatically increasing the likelihood that the recipient will click the link.[11]

The adaptability of these methods is demonstrated by real-world scams that have impersonated widely used services like Google Docs and PayPal, or even exploited global crises like the COVID-19 pandemic by sending fake alerts from health organizations or government bodies offering aid.[11]

Malware: The Malicious Payload

Malware, a portmanteau of "malicious software," is any software or code intentionally designed to harm, disrupt, or gain unauthorized access to a computer system, network, or device.[1] It is the "payload" often delivered by a successful phishing attack. Once a user clicks a malicious link or opens an infected attachment, the malware is downloaded and executed, beginning its intended function.[26] The world of malware is vast, with different types designed for specific malicious purposes.

- **Viruses and Worms:** These are some of the oldest forms of malware. A **computer virus** attaches itself to a legitimate program or file. It remains dormant until that file is opened, at which point it executes and attempts to replicate itself by attaching to other files.[21] A

computer worm, on the other hand, is a standalone piece of malware that can replicate itself and spread across computer networks without any user interaction, often exploiting network vulnerabilities to propagate.[21]

- **Trojans (or Trojan Horses):** Named after the ancient Greek tale, a Trojan disguises itself as a harmless or desirable program to trick users into installing it. Unlike viruses and worms, Trojans do not self-replicate.[26] Once installed, they can perform a wide range of malicious actions, such as stealing data, installing other malware, or creating a "backdoor" that gives the attacker remote control over the infected system.[21]
- **Spyware and Keyloggers:** These types of malware are designed for stealthy surveillance. **Spyware** infects a device to secretly monitor user activity, collecting information such as websites visited, login credentials, and personal files.[26] A **keylogger** is a specific type of spyware that records every keystroke a user makes, making it highly effective at capturing passwords, credit card numbers, and private messages.[21]
- **Adware and Malvertising: Adware** is software that bombards a user's device with unwanted pop-up advertisements. While often just an annoyance, it can degrade system performance and compromise privacy.[21] Its more sinister cousin, **malvertising**, involves injecting malicious code into legitimate online advertisements or ad networks. Clicking on one of these compromised ads can redirect a user to a malicious website or trigger a malware download.[21]
- **Botnets:** A botnet, short for "robot network," is a network of thousands or even millions of malware-infected computers (known as "bots" or "zombies") that are under the remote control of a single attacker, or "bot-herder." These vast networks are used as a platform to carry out large-scale automated attacks, such as sending massive volumes of spam and phishing emails, launching Distributed Denial-of-Service (DDoS) attacks to overwhelm and crash websites, and stealing credentials on an industrial scale.[21]
- **Fileless Malware:** This is a particularly stealthy and dangerous type of malware. Instead of installing malicious files on a computer's hard drive, fileless malware operates directly in the system's memory (RAM). It leverages legitimate, built-in system tools (like PowerShell or WMI on Windows) to carry out its attack. Because it leaves no files behind to be scanned, it is extremely difficult for traditional antivirus software to detect.[4]

Ransomware: The Digital Hostage Crisis

Among the most feared and destructive forms of malware is ransomware. This malicious software is designed to hold a victim's data hostage, effectively locking them out of their own digital life until a ransom is paid.[22] The prevalence of these attacks is surging, with one report indicating an 84% year-over-year increase, now accounting for 35% of all cyberattacks.[5]

The ransomware attack process is methodical and devastating:

1. **Infection:** The attack typically begins with a common entry vector, such as a phishing email with a malicious attachment, the exploitation of an unpatched software vulnerability, or a poorly secured Remote Desktop Protocol (RDP) connection.[22]
2. **Encryption:** Once inside the system, the ransomware activates. It silently scans for valuable files—documents, photos, databases, spreadsheets—and encrypts them using powerful, complex algorithms. The files are not deleted, but they are rendered completely inaccessible without a unique decryption key, which only the attacker possesses. Victims often discover the attack when they find their file icons have changed or their files have been renamed with a strange new extension.[28]
3. **Ransom Demand:** After the encryption is complete, a ransom note appears on the victim's screen. This note explains what has happened and demands a payment, almost always in a cryptocurrency like Bitcoin, in exchange for the decryption key. To create pressure, the note often includes a strict deadline; if the ransom is not paid in time, the price may double, or the decryption key may be destroyed forever.[22]

In recent years, criminals have evolved their extortion tactics to increase the pressure on victims to pay:

- **Screen Lockers:** A simpler form of ransomware that doesn't encrypt individual files but instead locks the user out of their entire computer, displaying a full-screen ransom demand that prevents them from accessing the operating system or any of their data.[22]
- **Double Extortion:** This has become the new standard for ransomware gangs. Before encrypting the data, the attackers first exfiltrate it, stealing a copy for themselves. They then threaten to leak this sensitive information publicly if the ransom is not paid. This "double extortion" tactic adds immense pressure, as victims must now worry not only about regaining access to their data but also about the reputational damage, regulatory fines, and personal embarrassment that would result from a public data leak.[22]

Despite the intense pressure, authorities like the Cybersecurity and Infrastructure Security Agency (CISA) strongly advise against paying the ransom. There is no guarantee that the criminals will provide a working decryption key after payment. Furthermore, paying the ransom funds their criminal enterprise, validates their business model, and marks the victim as a willing payer, making them a more likely target for future attacks.[9]

The evolution of these threats is being rapidly accelerated by the integration of Artificial Intelligence. AI is not just another tool in the attacker's arsenal; it acts as a force multiplier across the entire attack chain. AI algorithms can be used to scrape social media and public data to automate the reconnaissance phase of a social engineering attack, gathering personal details to craft more targeted campaigns.[30] Generative AI is being used to write flawless, convincing phishing emails and even malicious code, eliminating the grammatical errors that were once a key red flag for users.[5] Most alarmingly, AI-powered deepfake technology can be used as the payload of an attack. Imagine a spear-phishing email that directs an employee to a video call where a hyper-realistic deepfake of their CEO instructs them to authorize an urgent wire transfer. This is no longer science fiction; such an attack was used to steal $25 million from the global engineering firm Arup.[7] This synergy—where AI automates reconnaissance, perfects the phishing lure, and creates a convincing deepfake exploit—creates a more integrated and sophisticated attack lifecycle that is harder to detect at every stage. This necessitates a corresponding evolution in our defensive strategies, moving beyond simple advice to a more layered and technologically robust approach.

Chapter 3: Identity Theft: The Ultimate Consequence

For many cybercriminals, phishing attacks and malware infections are not the end goal; they are the means to an end. The ultimate prize is often the victim's identity.

What is Identity Theft?

Identity theft is a crime in which a malicious actor obtains and uses an individual's personal identifying information (PII)—such as their name, Social Security number (SSN), date of birth, or credit card numbers—without their permission, typically for financial gain.[31] It is the culmination of many of the threats previously discussed, turning stolen data into real-world harm.

Criminals can acquire this information through both digital and physical means. Online, they use phishing, malware, and data breaches to harvest PII. Offline, they resort to timeless methods like stealing wallets, purses, and mail; rummaging through unshredded trash for discarded statements; or even buying information from corrupt insiders at businesses.[33]

The Devastating Consequences

The impact of identity theft can be profoundly damaging, extending far beyond a single fraudulent charge on a credit card. The consequences can ripple through a victim's financial, legal, and even physical well-being for years.[32]

- **Financial Ruin:** This is the most immediate and common consequence. Thieves can use a victim's identity to drain bank accounts, run up massive debts on existing credit cards, and open new lines of credit, loans, and utility accounts in the victim's name.[32] The resulting damage to the victim's credit score can be catastrophic, making it incredibly difficult to secure a mortgage, a car loan, or even get a job or rent an apartment in the future.
- **Legal and Criminal Complications:** The ramifications can extend into the legal system. In some cases, an identity thief who is arrested for a crime may present the victim's stolen ID to law enforcement, resulting in a false criminal record and even an arrest warrant being issued in the victim's name.[32] Victims may also find themselves being sued by collection agencies for debts they never incurred.
- **Medical and Tax Fraud:** The misuse of a stolen identity can have life-threatening

consequences. A thief can use a victim's PII and health insurance information to receive medical services. This corrupts the victim's medical records with false information about allergies, blood type, and health conditions, which could lead to a dangerous misdiagnosis or incorrect treatment in a future medical emergency.[31] Criminals also frequently use stolen SSNs to file fraudulent tax returns early in the tax season, claiming a refund in the victim's name. When the actual victim files their return, the IRS rejects it, triggering a lengthy and frustrating process to prove their identity and claim their rightful refund.[33]

Warning Signs of Identity Theft

Early detection is critical to mitigating the damage of identity theft. Individuals should be vigilant for the following red flags that may indicate their identity has been compromised [32]:

- **Unexplained Financial Activity:** Seeing withdrawals from your bank account that you did not make, or finding unfamiliar charges on your credit card statements.
- **Bills and Collection Calls for Unknown Accounts:** Receiving bills, credit cards, or calls from debt collectors for accounts or services you never opened.
- **Credit Denials:** Being unexpectedly denied for a loan or credit application, which can indicate that a thief has damaged your credit.
- **Missing Mail:** Suddenly failing to receive your regular bills or other mail can be a sign that an identity thief has submitted a change of address form to divert your mail and hide their tracks.
- **IRS Notices:** Receiving a notice from the IRS stating that more than one tax return was filed in your name or that you have income from an employer you don't work for.
- **Errors on Your Credit Report:** Finding accounts or addresses you don't recognize on your credit report.

Recognizing these signs promptly allows a victim to begin the recovery process sooner, potentially limiting the extent of the financial and administrative damage.

Part II: The SAFE Framework: Your Blueprint for Online Security

Understanding the threat landscape is the first step. The second, more crucial step is to build a robust defense. This section transitions from theory to practice, introducing the **SAFE** framework—a structured, four-part approach to personal cybersecurity. By systematically implementing the principles of Securing your assets, maintaining Awareness, Fortifying your privacy, and knowing the Emergency response, anyone can build a formidable defense against the vast majority of online threats.

Chapter 4: S – Secure Your Accounts and Devices

The foundation of any strong cybersecurity posture rests on a set of core technical controls. These are the digital locks, alarms, and reinforcements that protect your most valuable assets. This chapter covers the essential, non-negotiable actions required to secure your accounts, devices, and networks.

Sub-section 4.1: Passwords Reimagined: The New Rules of Strength

For decades, the conventional wisdom on passwords was clear: create a short, complex string of characters, like P@ssw0rd1!, and change it every 90 days. However, extensive research has shown that this advice is not only ineffective but often counterproductive. Humans struggle to remember complex, arbitrary strings, leading them to create weak, predictable patterns (like changing P@ssw0rd1! to P@ssw0rd2!) or writing them down on sticky notes, ultimately undermining security.[35]

In response, the National Institute of Standards and Technology (NIST), a leading authority on cybersecurity standards, has revolutionized password guidance. The new philosophy, backed by extensive data, is simple and far more effective: **length trumps complexity**.[35]

Modern Password Best Practices

Adopting modern password practices is one of the most impactful security changes an individual can make.

- **Length is Key:** A password's strength against brute-force cracking attempts is exponentially related to its length. The minimum acceptable length is now considered to be 12-15 characters, with 16 or more being strongly recommended for critical accounts.[37]
- **Embrace the Passphrase:** Instead of struggling to create and remember a complex string like 8#k$zP!vQ@4f, it is far more secure and practical to use a **passphrase**. A passphrase is a sequence of several unrelated words, such as CorrectHorseBatteryStaple or HorsePurpleHatRunBayLifting. These phrases are easy for a human to remember but are exceptionally difficult for computers to guess or brute-force due to their significant length.[39]
- **Uniqueness is Non-Negotiable:** This is the most critical rule of password hygiene. A completely different, unique password must be used for every single online account.[41] The reason is simple: data breaches are inevitable. When a website you use is breached, criminals will take your email and password from that breach and try them on other popular sites like your bank, email provider, and social media accounts. This is known as a "credential stuffing attack," and it is one of the most common ways accounts are

compromised.[11] If you reuse passwords, a breach at one minor, insecure website can lead to the takeover of all your most important accounts.

- **Use a Password Manager:** It is humanly impossible to create and memorize dozens of unique, long, and random passwords for every online service. A **password manager** is an essential, modern security tool that solves this problem. These applications generate highly secure, random passwords for each of your accounts, store them in an encrypted vault, and can automatically fill them in when you log in to websites and apps. The user only needs to remember one, very strong master password to unlock the vault itself.[35] This is the single most effective way to implement the rule of password uniqueness.
- **Stop Forced Password Changes:** The old practice of forcing password changes every 60 or 90 days is no longer recommended by NIST. Research shows this practice encourages users to create weaker, more memorable passwords and make only minor, predictable changes each time.[35] A password should only be changed if there is evidence or suspicion that it has been compromised.

To clarify this fundamental shift in best practices, the following table contrasts the outdated advice with modern, expert-backed guidance.

Feature	Old Advice (Often Ineffective)	Modern NIST & Expert Guidance (More Secure)
Length	8 characters was often the minimum.	Minimum 15 characters; longer is better.[36]
Complexity	Must contain uppercase, lowercase, number, and symbol.	Length is more important. Arbitrary complexity is not required.[35]
Composition	P@ssw0rd1!	Horse Purple Hat Run Bay Lifting (passphrase).[42]
Rotation	Change every 60-90 days.	Only change if a breach is suspected.[35]
Uniqueness	Often ignored, leading to password reuse.	Use a unique password for every single account.[41]
Tools	Memorization was key.	Use a password manager to generate and store unique passwords.[35]

Sub-section 4.2: Multi-Factor Authentication (MFA): Your Digital Deadbolt

While a strong, unique password is a critical first line of defense, even the strongest password can be stolen in a data breach or phished by a clever attacker. This is why the single most important security step anyone can take is to enable **Multi-Factor Authentication (MFA)**. According to CISA, simply enabling MFA makes your accounts **99% less likely to be**

hacked.[49]
MFA, also known as two-factor authentication (2FA) or two-step verification, is a layered security approach that requires more than just a password to log in. It verifies your identity by asking for a combination of two or more "factors" [47]:

- **Something you know:** Your password.
- **Something you have:** A physical object like your smartphone or a security key.
- **Something you are:** A biometric characteristic like your fingerprint or face.

Even if a criminal steals your password, they cannot access your account because they do not possess the second factor.

Types of MFA, from Good to Best

Not all MFA methods offer the same level of security. While any MFA is better than no MFA, it is important to understand the hierarchy of protection.

- **SMS/Email Codes (Fairly Secure):** This is the most common and accessible form of MFA. After entering your password, a one-time code is sent via text message to your phone or to your email address, which you then enter to complete the login.[43]
  Weakness: This method is vulnerable to "SIM swap" attacks, where a criminal tricks a mobile carrier into transferring your phone number to their device, allowing them to intercept your codes. It is also vulnerable to phishing, as a user could be tricked into entering the code on a fake website.[54]
- **Authenticator Apps (Strong):** Applications like Google Authenticator, Microsoft Authenticator, or Authy generate a new, time-sensitive six-digit code on your smartphone every 30-60 seconds.[51] This is significantly more secure than SMS because the code is generated locally on your device and is not transmitted over the vulnerable mobile network.
- **Biometrics (Strong):** This method uses your unique biological traits, such as a fingerprint or facial scan, to verify your identity.[51] It is convenient and tied to your physical device.
- **Phishing-Resistant MFA (Very Strong):** This is the gold standard of authentication security. It uses cryptographic verification that is immune to phishing. The two main types are:
  - **Physical Security Keys:** Small hardware devices (like a YubiKey) that plug into your computer's USB port or connect via NFC/Bluetooth. To log in, you must physically touch the key, proving your presence.[57]
  - **Platform Authenticators (Passkeys):** This technology, built on the FIDO/WebAuthn standard, turns your device (computer or smartphone) into a security key. It uses the device's built-in biometrics (like Windows Hello or Apple's Face ID/Touch ID) to create a unique cryptographic key pair for each website. When you log in, the authentication is bound to the legitimate website, making it impossible for a phishing site to intercept it.[52]

How to Enable MFA (Step-by-Step Guide)

Enabling MFA is a simple process that typically takes only a few minutes.

1. **Navigate to Security Settings:** Log in to the account you wish to secure (e.g., Google, Apple, Microsoft, Facebook, your bank). Go to the account settings, and look for a section labeled "Security," "Sign-In & Security," or "Password and Security".[51]
2. **Find and Turn On MFA:** Within the security section, locate the option for "Two-Factor Authentication," "2-Step Verification," or "Multi-Factor Authentication" and select the option to turn it on.[51]
3. **Choose and Configure Your Method:** The service will guide you through setting up your preferred MFA method. This may involve:
   - Entering your phone number to receive SMS codes.
   - Scanning a QR code with an authenticator app to link it to your account.
   - Registering a physical security key by inserting it and touching it.[55]
4. **Save Recovery Codes:** Most services will provide you with a set of one-time recovery codes. Print these out and store them in a safe, physical location. These codes will allow you to access your account if you lose your primary MFA device.
5. **Prioritize Critical Accounts:** Enable MFA on all of your most important accounts immediately, including your primary email, all financial and banking accounts, social media accounts, and especially your password manager.[42]

Sub-section 4.3: Your Digital Immune System: Updates, Antivirus, and Firewalls

Just as the human body relies on an immune system to fight off infections, your digital life depends on a set of automated defenses to protect against constant threats. Keeping this digital immune system strong through software updates, antivirus protection, and firewalls is a fundamental aspect of cyber hygiene.

The Critical Role of Software Updates

Software is not static; it is constantly evolving. Developers release updates not just to add new features or improve performance, but to patch security vulnerabilities that have been discovered.[60] These vulnerabilities are holes in the software's defenses that hackers can exploit to gain access to your device and data. In fact, unpatched software was identified as the cause of 60% of data breaches, highlighting how critical updates are to security.[62]

When a notification for a software update appears, it is tempting to click "Remind Me Later." This is a dangerous habit. Cybercriminals actively scan the internet for devices running outdated software with known vulnerabilities, making those who delay updates easy targets.[60]

Best Practice: The most effective strategy is to enable **automatic updates** for your operating system (Windows, macOS, iOS, Android), your web browsers, and all of your applications whenever the option is available. This ensures you receive critical security patches as soon as they are released, without having to remember to do it manually.[48]

Antivirus Software: Your Digital Guardian

Antivirus software (also known as anti-malware) is a program designed to detect, quarantine, and remove malicious software from your devices.[63] It acts as a real-time scanner and a proactive defense against known threats.

- **How it Works:** Antivirus software employs several detection methods:
  - **Signature-Based Detection:** This is the traditional method. The software maintains a vast database of "signatures"—unique digital fingerprints of known malware. It scans files on your computer and compares them against this database. A match indicates an infection.[65]
  - **Heuristic and Behavior-Based Detection:** Since signature-based detection can't catch brand-new malware, modern antivirus programs also use behavioral analysis. They monitor programs for suspicious actions—like trying to modify critical system files, encrypting large numbers of files rapidly, or attempting to capture keystrokes. This allows them to detect and block new, unknown threats based on their malicious behavior.[65]

Best Practice: Install a reputable antivirus solution on all of your computers and mobile devices. Many high-quality options are available, including free versions from well-known companies. Crucially, ensure that the software is set to **update its virus definitions automatically** to protect against the latest threats.[64]

Firewalls: Your Network's Border Control

A firewall is a network security system that acts as a barrier between a trusted internal network (like your home or office network) and an untrusted external network (the internet).[69] It monitors all incoming and outgoing network traffic and, based on a set of predefined security rules, decides whether to allow or block specific data packets, preventing malicious connections from reaching your devices.[72]

- **Types of Firewalls:** You interact with two main types of firewalls, and both are important:
  - **Hardware Firewalls:** These are physical devices, and the most common example is the firewall built into your home Wi-Fi router. It sits between the internet and all the devices on your home network, providing a first line of defense.[73]
  - **Software Firewalls:** These are programs that run on your individual computer or device. Modern operating systems like Windows and macOS include powerful,

built-in software firewalls.[73]

Best Practice: Ensure that both the firewall on your computer's operating system and the firewall on your home Wi-Fi router are enabled. For most users, the default settings are sufficient, but it is wise to confirm they are active.[73]

Sub-section 4.4: Fortifying Your Home Base: Securing Your Wi-Fi Router

Your home Wi-Fi router is the gateway to your entire digital life. It connects every device in your home—computers, smartphones, tablets, smart TVs, security cameras, and more—to the internet. If an attacker compromises your router, they can potentially monitor all your internet traffic, redirect you to malicious websites, and attack every other device on your network.[75] Securing this single piece of hardware is therefore one of the most high-impact actions you can take to protect your digital home.

The security of individual accounts and devices is fundamentally intertwined with the security of the network they connect to. A user can implement the world's strongest passwords and use phishing-resistant MFA, but if their home Wi-Fi is unprotected, their efforts can be undermined. An attacker who gains control of an insecure router could execute a Man-in-the-Middle (MitM) attack, intercepting all traffic passing through it.[21] This could allow them to capture passwords, hijack active login sessions, and inject malware into downloads. Furthermore, a compromised router gives an attacker a foothold inside the "trusted" home network, from which they can launch attacks against other, less-secure devices like smart home gadgets or older computers.[26] Therefore, securing the router is not just another item on a checklist; it is the foundational layer upon which all other personal security rests.

Essential Router Security Checklist

Follow these steps to transform your router from a security liability into a digital fortress. You will typically need to log in to your router's administrative interface via a web browser to change these settings; consult your router's manual or the manufacturer's website for specific instructions.

1. **Change the Default Administrator Credentials:** Every router ships with a default administrator username and password (e.g., "admin" and "password"). These are public knowledge and are the first thing an attacker will try. Change them immediately to a strong, unique password.[48]
2. **Change the Network Name (SSID):** The Service Set Identifier (SSID) is the name of your Wi-Fi network that appears in the list of available networks. The default SSID often reveals the router's manufacturer and model number, giving hackers valuable clues about potential vulnerabilities. Change it to something unique that does not reveal any personal information about you or your family (e.g., avoid "The Smiths Wi-Fi").[77]
3. **Use Strong Encryption (WPA3):** Encryption scrambles the data transmitted over your

Wi-Fi network, making it unreadable to eavesdroppers. You must enable the strongest encryption protocol your router supports.
   - **WPA3** is the current, most secure standard. Use it if available.
   - **WPA2-AES** is the next-best option and is still considered secure.
   - **Avoid WEP and WPA (version 1)** at all costs. These older protocols are critically flawed and offer no real security.[48] If your router only supports these, it is dangerously outdated and must be replaced.
4. **Create a Strong and Unique Wi-Fi Password:** The password used to connect to your Wi-Fi network should be treated with the same care as your other critical passwords. Use a long (16+ characters) and unique passphrase that is easy for you to remember but hard for others to guess.[77]
5. **Keep the Router's Firmware Updated:** Router firmware, like any software, contains vulnerabilities that manufacturers patch with updates. Regularly check the manufacturer's website for the latest firmware version and install it. If your router has an option for automatic updates, enable it.[75]
6. **Disable Risky and Unnecessary Features:** Many routers come with features designed for convenience that can introduce security risks. It is best to disable them unless you have a specific need for them:
   - **Wi-Fi Protected Setup (WPS):** This feature allows devices to connect by pressing a button instead of entering a password, but it has known vulnerabilities that can be exploited by attackers.[75]
   - **Universal Plug and Play (UPnP):** UPnP allows devices on your network to automatically open ports in your firewall, which can be convenient for gaming or media sharing but can also be exploited by malware to open your network to the internet.[75]
   - **Remote Management/Administration:** This feature allows you to access your router's settings from anywhere on the internet. It is a major security risk and should be disabled. You should only manage your router from a device that is physically connected to your home network.[75]
7. **Enable and Use the Guest Network:** Most modern routers allow you to create a separate "guest" Wi-Fi network with its own name and password. This is a powerful security feature. Provide the guest network password to visitors. This isolates their devices from your primary network, so if a guest's device is infected with malware, it cannot spread to your personal computers, file servers, or other sensitive devices.[75]
8. **Enable the Built-in Firewall:** Confirm that your router's network firewall is turned on. This provides a critical layer of protection by blocking unsolicited incoming traffic from the internet.[75]

Chapter 5: A – Awareness and Spotting Threats

Technical controls like strong passwords and firewalls are essential, but they are only part of the solution. An equally critical layer of defense is the "human firewall"—a well-informed and vigilant user who can recognize and avoid threats before they have a chance to cause harm. This chapter focuses on developing that awareness, providing the knowledge needed to spot malicious communications, navigate the web safely, and adopt responsible online habits.

Sub-section 5.1: Think Before You Click: Recognizing Malicious Communications

Email remains the primary delivery vehicle for phishing attacks, malware, and other scams. Learning to dissect a suspicious message is a fundamental cybersecurity skill. While attackers are becoming more sophisticated, many phishing attempts still contain tell-tale signs for those who know what to look for.[15]

Anatomy of a Phishing Email

- **Verify the Sender's Address:** This is the first and most important check. Attackers are skilled at making the "From" name look legitimate (e.g., "PayPal Support"), but they cannot perfectly fake the email address. Hover your mouse cursor over the sender's name to reveal the actual email address it came from. Be highly suspicious of addresses that use a public domain (like @gmail.com) for an official communication, or that contain subtle misspellings and alterations of a legitimate domain (e.g., support@amazan.com or service@microsoft.co).[15]
- **Look for Generic Greetings:** Legitimate companies with whom you have an account will almost always address you by your name. Be wary of generic salutations like "Dear Valued Customer," "Dear Account Holder," or "Sir/Ma'am".[15] This often indicates a bulk phishing campaign sent to thousands of addresses.
- **Hover, Don't Click:** Never blindly click on links in an email, especially if the message is unexpected. Before clicking, hover your mouse over the link to preview the actual destination URL. This preview typically appears in the bottom-left corner of your browser or email client. If the destination URL looks suspicious, is a string of random characters, or does not match the website described in the link text, do not click it.[25] For example, a link that says
  Click here to log in to your bank might reveal a destination URL of
  http://123.45.67.89/login or www.yourbanc-secure.com.
- **Identify Pressure Tactics and Urgency:** A hallmark of phishing is the creation of a false sense of urgency or fear. Messages often use threatening language or emotional appeals to pressure you into acting quickly without thinking. Common tactics include threats of account closure ("Your account will be suspended in 24 hours"), legal action, or claims of a prize that must be redeemed immediately.[15]
- **Be Cautious with Unexpected Attachments:** Treat all unexpected email attachments with extreme caution, even if they appear to come from someone you know (as their

account could be hacked). Never open attachments with executable file extensions like .exe, .scr, .bat, or .com from an email. Be aware that attackers often disguise these files within .zip archives to bypass email filters.[83]

It is important to note that the reliability of some traditional red flags is decreasing. For instance, while poor grammar and spelling were once a dead giveaway of a phishing attempt, the rise of Generative AI now allows criminals to craft perfectly written, grammatically correct phishing emails, making them much more convincing.[84] This shift makes the technical verification of sender addresses and link destinations more critical than ever.

Finally, if you receive a suspicious email, the correct action is to delete it. Never reply to the message, even to ask to be removed from their list. Replying confirms to the spammers that your email address is active and monitored, which will likely lead to a significant increase in spam and future phishing attempts.[86]

Sub-section 5.2: Safe Surfing: How to Identify Suspicious Websites

Just as with emails, criminals create malicious websites designed to steal information or deliver malware. These sites are often designed to be near-perfect clones of legitimate ones.

Checking a URL for Security and Authenticity

- **Look for HTTPS and the Padlock:** The first thing to check in a website's address bar is the presence of https:// at the beginning of the URL and a corresponding padlock icon. The "S" stands for "secure" and indicates that the connection between your browser and the website is encrypted with an SSL/TLS certificate, making it difficult for third parties to intercept the data you send.[93]

  However, this is not a guarantee of legitimacy. In recent years, it has become easy and free for anyone, including scammers, to obtain a basic SSL certificate. Therefore, while the *absence* of HTTPS is a major red flag for any site asking for information, its *presence* does not automatically mean the site is trustworthy.[96]
- **Scrutinize the Domain Name:** This is the most critical part of verifying a website. The true domain name is the part of the URL immediately to the left of the .com, .org, .net, etc..[98] Attackers use several tricks to make fake domains look real:
  - **Typosquatting:** Using subtle misspellings of a popular brand (e.g., BankoffAmerica.com with two 'f's, or Walmart.com using a capital 'i' instead of an 'l').[97]
  - **Subdomain Tricks:** Adding the legitimate brand name as a subdomain to a malicious domain (e.g., paypal.com.secure-site.com). In this case, the actual domain is secure-site.com, not paypal.com.[97] Always identify the core domain.
- **Avoid Shortened URLs and IP Addresses:** Be very cautious with links that have been shortened using services like bit.ly or tinyurl, as they completely mask the final

destination. You have no way of knowing where the link will take you.[98] Similarly, avoid clicking on links that are just a numerical IP address (e.g., http://101.10.1.101) unless you are a technical user who knows exactly what it is.[98]

Assessing Site Quality and Content

Beyond the URL, the website itself can offer clues to its legitimacy. Professional organizations invest in high-quality websites. Phishing sites, while often good copies, may have flaws.[96]

- **Look for poor quality:** Spelling mistakes, grammatical errors, broken English, and low-resolution or pixelated logos and images are red flags.
- **Check for contact information:** A legitimate business will have a "Contact Us" or "About Us" page with a physical address, a customer service phone number, and an email address. The absence of this information is highly suspicious.
- **Beware of excessive pop-ups and ads:** While many sites have ads, a site that bombards you with aggressive pop-ups and intrusive advertisements may be malicious.

Using Website Checkers and Safe Browsing Tools

For an extra layer of verification, you can use free online tools like the Google Transparency Report or URLVoid. These services will scan a URL you provide and check it against databases of known malicious and phishing websites.[97] Additionally, all modern web browsers (Chrome, Firefox, Edge, Safari) have built-in safe browsing features. They automatically check the sites you visit against constantly updated lists of dangerous sites and will display a full-page warning before allowing you to proceed to a known malicious site. It is critical to heed these warnings.[100]

Sub-section 5.3: Responsible Practices: Safe Downloading and Scam Avoidance

Awareness extends beyond just identifying threats; it also involves adopting safe habits in your day-to-day online activities.

Safe Downloading Hygiene

Downloading files from the internet is a common activity, but it carries inherent risks, as files can be bundled with malware.

- **Download Only from Trusted Sources:** The cardinal rule of safe downloading is to only get files from official and reputable sources. For software, this means downloading directly from the developer's official website. For mobile apps, use only the official Apple App Store or Google Play Store.[100] Avoid third-party app stores and websites that offer "free" versions of paid software, as these are often laden with malware.

- **Scan Everything:** Use your antivirus software to scan all files you download before you open or run them. This also applies to files transferred via external media, such as USB drives or external hard drives.[64]
- **Enable Browser Security:** Modern browsers have settings to help block potentially dangerous downloads. Ensure these features are enabled in your browser's security settings.[105]

Recognizing and Avoiding Common Scams

While scams come in many forms, the Federal Trade Commission (FTC) notes that most rely on a few core psychological tactics.[88] Recognizing these patterns is key to avoidance.

- **The Impersonation:** Scammers pretend to be from an organization you know and trust, such as the IRS, Microsoft, your bank, or a local utility company.
- **The Fake Problem or Prize:** They invent a pretext to get your attention. This could be a problem (you owe back taxes, your computer has a virus, a family member is in trouble) or a prize (you've won a lottery or sweepstakes).
- **The Pressure to Act Fast:** They create a sense of urgency to prevent you from having time to think, research their claims, or talk to someone you trust.
- **The Specific Payment Method:** This is often the most definitive red flag. Scammers will insist on payment through methods that are difficult to trace and nearly impossible to reverse. If anyone demands payment via **wire transfer (like Western Union or MoneyGram), gift cards (like Apple, Google Play, or Target), or cryptocurrency (like Bitcoin)**, it is a scam. No legitimate business or government agency will ever demand payment in this way.[88]

The golden rule of scam avoidance remains timeless: if an offer sounds too good to be true, it almost certainly is.[16] The best response to a high-pressure situation is to stop, take a breath, and talk to a trusted friend, family member, or colleague before taking any action.[88] A moment of consultation can often be enough to break the spell of the scammer's urgency.

Ultimately, user awareness is a critical but fallible line of defense. The increasing sophistication of AI-generated phishing emails, flawless website clones using valid HTTPS certificates, and the sheer volume of attacks create a state of "alert fatigue" where even the most vigilant user can eventually make a mistake. This reality underscores the importance of a multi-layered defense. While the awareness skills in this chapter are vital, they must be backed by the robust technical controls from Chapter 4. When a user's ability to "spot the fake" fails, it is the presence of MFA, up-to-date software, and a properly configured firewall that prevents a single errant click from escalating into a catastrophic security incident. This reinforces the necessity of the holistic, defense-in-depth approach advocated by the SAFE framework.

Chapter 6: F – Fortify Your Privacy

In the digital economy, personal data is the most valuable currency. Every action taken online contributes to a vast and permanent record known as a digital footprint. This data is collected, aggregated, and often sold by advertisers, data brokers, and, unfortunately, criminals. Fortifying your privacy involves understanding this footprint and taking deliberate steps to control your personal information, thereby reducing your visibility and making you a harder target.

Sub-section 6.1: Understanding Your Digital Footprint

Your digital footprint is the complete trail of data you create and leave behind as you use the internet. It is a detailed, living record of your online life that can be accessed, shared, and analyzed by others, often without your knowledge.[30] This footprint is composed of two distinct types of data:

- **Active Digital Footprint:** This consists of the data you share intentionally and knowingly. It includes social media posts, comments on blogs, emails you send, photos you upload, and information you voluntarily submit in online forms.[30]
- **Passive Digital Footprint:** This is the data collected about you in the background, often without your direct action or awareness. It is generated when websites use cookies to track your browsing habits across the web, when mobile apps log your precise geolocation, or when your IP address is recorded by the servers you visit.[30]

Managing this footprint is critically important for several reasons. It directly impacts your **online reputation**, as potential employers, universities, and even romantic partners may search for you online to form an opinion.[111] It is central to your **privacy**, as an unmanaged footprint can expose intimate details of your life to the public. Most critically, it is a matter of **security**. The more information that is publicly available about you, the easier it is for criminals to commit identity theft or craft highly convincing, personalized spear-phishing attacks.[30] This data is the raw material for data brokers, who compile detailed profiles on individuals and sell them to advertisers, businesses, and virtually anyone else willing to pay.[114]

Sub-section 6.2: Minimizing Your Exposure: How to Reduce Your Footprint

While it is impossible to completely erase your digital footprint, you can take concrete steps to significantly reduce it and regain control over your personal information.

- **Audit Your Online Presence:** The first step is to understand what is already out there. Conduct a thorough search for your own name on multiple search engines like Google and Bing. You may be surprised by what you find.[117] To stay informed about new mentions, set up a Google Alert for your name, which will notify you whenever new content about you appears online.[117]

- **Delete Old and Unused Accounts:** One of the most effective ways to shrink your footprint is to get rid of accounts you no longer use. That old MySpace profile, the email account you haven't logged into for a decade, or the online retail account you created for a single purchase are all repositories of your personal data, often protected by old, weak passwords. Deleting these accounts removes that data from circulation and reduces your attack surface.[114]
- **Manage Mobile App Permissions:** Modern mobile apps often request access to a wide range of data on your phone, including your contacts, location, photos, microphone, and camera. Audit the permissions for every app on your device. Follow the principle of "least privilege": grant an app only the permissions it absolutely needs to perform its core function. For example, a map application needs your location, but a simple game or a news app likely does not. Deny any permissions that seem excessive or unnecessary.[115]
- **Use Privacy-Enhancing Tools:**
    - **Virtual Private Network (VPN):** A VPN is an essential privacy tool. It creates an encrypted tunnel for your internet traffic, hiding your online activities from your Internet Service Provider (ISP) and others on the network. It also masks your IP address, making it much more difficult for websites to track your location. Using a VPN is especially critical when connecting to public Wi-Fi networks, which are notoriously insecure.[114]
    - **Privacy-Focused Browsers and Search Engines:** Standard web browsers and search engines are designed to track your activity for advertising purposes. Consider switching to privacy-focused alternatives. Browsers like Brave or Firefox with enhanced tracking protection can block many online trackers by default. Search engines like DuckDuckGo do not track your search history or build a profile on you.[119]
- **Limit Ad Tracking:** Your mobile device and computer have a unique Advertising ID (Ad ID) that allows advertisers to track your activity across different apps and websites to build a detailed profile for targeted ads. You can limit this tracking by resetting or disabling the Ad ID in your device's privacy settings on iOS, Android, and Windows.[115]
- **Opt-Out of Data Brokers:** Data broker and people-search websites collect and sell your personal information. While the process can be tedious, you have the right to request that these companies remove your data from their databases. There are also paid services that can automate this opt-out process on your behalf.[114]

Sub-section 6.3: The Perils of Oversharing: Responsible Information Sharing

The information you actively choose to share is a significant part of your digital footprint. Practicing responsible sharing means thinking critically about the potential long-term consequences of a post before you click "share".[126] A simple rule of thumb is to ask yourself: "Would I be comfortable with a stranger, a future employer, or a criminal seeing this information?" If the answer is no, don't post it.[20]

Oversharing creates specific and tangible risks:

- **Physical Security Risks:** Posting real-time updates about your vacation, including photos geotagged with your location, is like putting a sign on your front door that says "My house is empty." Criminals have been known to monitor social media for just this kind of information.[17]
- **Fuel for Identity Theft:** Sharing seemingly innocuous personal details can be dangerous. Posting your full date of birth, your mother's maiden name, the name of your first pet, or your high school mascot can give criminals the exact answers they need to bypass the security questions on your bank or email accounts.[17]
- **Reputation Damage:** Inappropriate photos, angry rants, or controversial comments can remain online forever and can have serious consequences for your personal and professional reputation. A growing number of employers and college admissions officers review candidates' social media profiles as part of their screening process.[20]
- **Targeting for Sophisticated Attacks:** Sharing details about your job, such as your title, projects you are working on, or even that you hold a security clearance, can make you a prime target for highly sophisticated spear-phishing attacks from criminals or even foreign intelligence services.[19]
- **"Sharenting" and Children's Privacy:** Parents who frequently post photos and detailed stories about their children are creating a massive, permanent digital footprint for them without their consent. This practice, sometimes called "sharenting," can lead to future embarrassment, cyberbullying, or even "digital kidnapping," where a stranger uses a child's photos to create a fake profile. It can also expose children to identity theft before they are even old enough to have a credit card.[130] Always get consent before posting photos or personal information about other people, including your children.[126]

Sub-section 6.4: Platform-Specific Privacy Guides

The default settings on most social media and online platforms are designed to maximize data collection, not to protect your privacy. This is a direct consequence of their business model, which relies on user data to fuel targeted advertising.[131] This means users must be proactive and manually adjust their settings to fortify their privacy. Fortunately, most major platforms offer "Privacy Checkup" tools to make this process easier.

Google Privacy Checkup

Google services are deeply integrated into many people's lives. Taking control of your Google privacy settings is essential.

1. **Navigate to Your Google Account:** Go to myaccount.google.com.
2. **Use the Privacy Checkup Tool:** From the main account page, select the **Privacy Checkup** tool (or go directly to privacycheckup.google.com). This guided tool will walk you through your most important settings.[135]
3. **Manage Activity Controls:** Decide what activity is saved to your account. Key settings to review are:
   - **Web & App Activity:** This saves your search history and activity on Google sites and apps.
   - **Location History:** This creates a timeline of where you go with your devices.
   - YouTube History: This saves your watch and search history on YouTube.
     You can pause the collection of this data or, more practically, set it to auto-delete after a chosen period, such as 3, 18, or 36 months. This is a powerful feature that automatically purges your old data.131
4. **Manage Ad Settings:** Go to "My Ad Center" to limit how Google uses your information to personalize the ads you see across the web.[131]

Facebook Privacy Checkup

Facebook collects a vast amount of data about its users. A regular privacy checkup is crucial.

1. **Navigate to the Privacy Checkup:** Log in to Facebook, click your profile picture, and go to **Settings & Privacy > Privacy Checkup**.[132]
2. **Review "Who can see what you share":**
   - Go through your profile information (hometown, work, education, relationship status) and set the audience for each item to "Friends" or "Only Me" instead of "Public."
   - Set the **default audience for future posts** to "Friends".[132]
3. **Review "How people can find you on Facebook":**
   - Limit who can find your profile using your email address or phone number.
   - Decide whether you want your profile to be discoverable by search engines like Google. It is recommended to turn this off.[132]
4. **Review "Your data settings on Facebook":**
   - This section shows you which third-party apps and websites you have logged into using your Facebook account. **Remove any apps you no longer use or trust.**
   - Crucially, manage your **Off-Facebook Activity**. This is data that other businesses and organizations share with Facebook about your interactions with them. You can clear your existing history and disable future tracking.[132]
5. **Review "Your ad preferences on Facebook":** Control which profile details can be used to target ads to you and limit whether your social interactions (e.g., likes) can be used in ads shown to your friends.[132]

X (formerly Twitter) Privacy and Safety Settings

X provides several key settings to enhance privacy and control your experience.

1. **Navigate to Privacy and Safety:** Click on **More > Settings and privacy > Privacy and safety**.[143]
2. **Manage "Audience, media and tagging":**
   - ○ Check the box for **"Protect your posts"** to make your account private. This means only your approved followers will be able to see your posts, and they cannot be retweeted. New followers will require your approval.[143]
   - ○ Manage **Photo tagging** to control who can tag you in photos ("Anyone," "Only people you follow," or "Off").[143]
3. **Manage "Content you see":** This section allows you to filter out potentially sensitive content from your feed.[133]
4. **Manage "Mute and block":** Use these tools to curate your experience by muting specific words, phrases, or accounts, or by blocking users entirely.[143]
5. **Manage "Discoverability and contacts":** Disable the options that allow others to find your account by searching for your email address or phone number.[143]
6. **Manage "Data sharing and personalization":** Turn off location information and inferred identity to limit how X tracks you and personalizes your experience.[133]

The need for users to manually perform these checkups reveals a fundamental tension at the heart of the modern internet. The business model of most "free" platforms is predicated on collecting vast amounts of user data for targeted advertising. This creates a system where the default settings are inherently permissive and favor data collection. Proposed legislation like the Kids Online Safety Act (KOSA), which would mandate that platforms enable the strongest privacy settings for minors *by default*, highlights this systemic issue.[148] Until such regulations are widespread, the responsibility falls on the individual user to be proactive. Understanding that the system is designed for data extraction empowers users to see these privacy checkups not as a chore, but as a necessary act of digital self-defense against a system that is not built with their best interests at heart.

Chapter 7: E – Emergency Response and Recovery

Even with the best preventative measures, security incidents can still happen. A sophisticated phishing attack, a zero-day vulnerability, or a simple human error can lead to a compromised account or stolen identity. In these moments, having a clear, actionable plan is critical to minimizing the damage and beginning the recovery process. This chapter provides step-by-step playbooks for responding to the most common cybersecurity emergencies.

Sub-section 7.1: Account Takeover Playbook: Hacked Email or Social Media

Discovering that your email or social media account has been hacked can be alarming. You might be locked out, or friends may report receiving strange messages from you containing suspicious links or pleas for money. Acting quickly is essential to regain control and limit the fallout.[149]

Immediate Steps to Regain Control

1. **Attempt to Log In and Change Your Password:** If you can still access your account, your first move is to change the password immediately. Make the new password long, unique, and strong.[150]
2. **Use the Account Recovery Process:** If the hacker has already changed your password and locked you out, use the platform's official "Forgot my password" or account recovery link. This process will typically send a reset link or code to your designated recovery email address or phone number.[152] Be persistent, as it can sometimes be difficult to get a response from social media platforms.[152]
3. **Report the Hack to the Platform:** Inform the service provider (Facebook, Google, X, etc.) that your account has been compromised. Most platforms have a specific portal or help page for reporting hacked accounts. This creates an official record and can aid in recovery.[151]
4. **Scan Your Devices for Malware:** Before and after regaining access, run a full scan of your computer and mobile devices with up-to-date antivirus software. The hacker may have gained your password by installing malware on your device, and you need to ensure it is removed to prevent them from simply stealing your new password.[149]

Post-Recovery Damage Control

Once you have regained access to your account, the work is not over. You must now assess the damage and secure your digital life.

1. **Enable Multi-Factor Authentication (MFA):** If you did not have MFA enabled before, turn it on immediately. This is the single best step to prevent the hacker from getting back in, even if they somehow obtain your new password.[149]
2. **Secure All Related Accounts:** If you reused the compromised password on any other websites, change those passwords immediately. A password manager is invaluable for this task.[151] Also, change the password for your recovery email account to ensure the hacker cannot use it to regain access.
3. **Review All Account Settings:** Carefully check your account settings for any changes the hacker may have made. Look for:
   - **Email Forwarding Rules:** In your email settings, check for any forwarding rules you didn't create that could be sending copies of your messages to the attacker's

address.[149]

- **Profile and Personal Information:** Check for any changes to your name, profile picture, or contact information.
- **Connected Apps:** Review the list of third-party applications that have permission to access your account and revoke access for any you don't recognize or trust.[153]
- **Sent Messages and Posts:** Check your sent messages, posts, and deleted items folders to see what the hacker did while they had control of your account.[149]

4. **Warn Your Contacts:** Send a message to your friends, family, and followers letting them know your account was hacked. This alerts them to disregard any strange messages they may have received from "you" and prevents them from falling victim to scams propagated through your account.[149]
5. **Review for Compromised Data:** Consider what sensitive information was stored in the account. If credit card numbers were saved, contact your bank to monitor for fraud or cancel the card. If private messages were exposed, be aware of the potential for blackmail or further social engineering attacks.[152]

Sub-section 7.2: Identity Theft Recovery: The Official FTC Process

If you suspect your identity has been stolen—for example, you see unauthorized accounts on your credit report or receive bills for things you didn't buy—it is crucial to follow a structured recovery process. The U.S. federal government's official, centralized resource for victims is the Federal Trade Commission's website, **IdentityTheft.gov**.[33]

Step-by-Step Recovery Plan

1. **Report the Theft to the FTC at IdentityTheft.gov:** This is the first and most important step. Go to the website and provide as many details as you can about the situation. The site will use this information to generate a personalized, step-by-step recovery plan and an official **FTC Identity Theft Report**. This report is a critical legal document that serves as proof of the crime and will be necessary for the subsequent steps.[155]
2. **Contact the Companies Where Fraud Occurred:** Use your FTC report to contact the fraud departments of the banks, credit card companies, utility providers, or any other businesses where the thief opened fraudulent accounts. Explain that you are a victim of identity theft and ask them to close or freeze the accounts and remove the fraudulent charges.[154]
3. **Place a Fraud Alert on Your Credit Reports:** Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion) and ask to place an initial fraud alert on your file. By law, the bureau you contact must notify the other two. This alert is free and lasts for one year. It signals to potential creditors that they must take extra steps to verify your identity before issuing new credit in your name.[34] Placing an alert also entitles you

to free copies of your credit reports from all three bureaus.

4. **File a Report with Your Local Police Department:** Take your FTC Identity Theft Report, a government-issued photo ID, and proof of your address to your local police station to file an official police report. While the police may not be able to investigate every case, the police report adds significant weight to your claim when dealing with creditors and credit bureaus.[154]

The Ultimate Protection: The Credit Freeze

While a fraud alert is a good first step, a **credit freeze** (also known as a security freeze) is the most powerful tool available to prevent new account identity theft.

- **What it Does:** A credit freeze restricts all access to your credit report. Since most lenders will not issue new credit without first checking an applicant's credit report, a freeze effectively stops an identity thief from opening new accounts in your name.[34]
- **How to Place a Freeze:** Unlike a fraud alert, you must contact **each of the three credit bureaus separately** to place a freeze. It is free to place, temporarily lift (if you need to apply for credit yourself), and permanently remove a freeze.[34]

Sub-section 7.3: Data Breach Protocol: What to Do When Your Info is Leaked

Data breaches are now a common occurrence. If you receive a notification that your personal information was exposed in a data breach at a company you do business with, you must act proactively, even if you don't see immediate signs of fraud.

Who to Contact After a Breach

- **The Breached Company:** Follow the instructions in the breach notification letter. Contact the company to understand exactly what information was exposed. Take advantage of any free credit monitoring or identity theft protection services they offer to victims.[165]
- **Law Enforcement:** For large-scale breaches, you can file a complaint with the FBI's Internet Crime Complaint Center (IC3) at ic3.gov to aid in broader investigations.[167]
- **Financial Institutions:** If financial information was exposed, notify your bank and credit card companies so they can monitor your accounts for fraudulent activity.[166]
- **The Credit Bureaus:** Proactively place a fraud alert or, for maximum protection, a credit freeze on your reports.[162]

Your Personal Action Plan

1. **Change Your Password Immediately:** Change the password for your account with the breached company. If you have reused that password anywhere else, change it on all those accounts as well.[165]
2. **Enable MFA:** If you haven't already, enable multi-factor authentication on the breached account and other critical accounts.[165]
3. **Monitor Your Accounts and Credit:** Be extra vigilant in the months following a breach. Regularly review your bank statements, credit card statements, and credit reports for any suspicious activity.[162]
4. **Be on High Alert for Phishing:** Criminals use the information stolen in data breaches to launch highly targeted and convincing spear-phishing attacks. Be extremely suspicious of any unsolicited emails, texts, or calls that reference the breach, as they may be scams designed to steal even more of your information.

The complexity of this emergency response process reveals a significant challenge within the current cybersecurity ecosystem. The burden of recovery from a hack, data breach, or identity theft falls almost entirely on the individual victim. They are forced to navigate a fragmented and often frustrating web of interactions with private companies (banks, tech companies, credit bureaus) and multiple government agencies (FTC, local police, FBI).[154] The very existence of a "one-stop resource" like IdentityTheft.gov is a testament to how convoluted the process is.[155]

This reactive and burdensome recovery model underscores a critical, systemic truth: prevention is exponentially easier, cheaper, and less stressful than recovery. The difficulty of cleaning up the mess after an incident is the strongest possible argument for diligently applying the proactive principles outlined in the "Secure," "Aware," and "Fortify" sections of this guide. This chapter serves not only as a practical "how-to" for emergencies but also as a powerful cautionary tale, reinforcing the immense value of the preventative measures that came before it.

Part III: Special Considerations for Our Communities

While the principles of online safety are universal, certain demographics face unique risks and require tailored guidance. This section provides specific advice for protecting two often-targeted groups: children and teens, who are navigating the digital world for the first time, and seniors, who may be less familiar with the nuances of online threats.

Chapter 8: Protecting Our Children and Teens Online

For children and teenagers, the internet is an integral part of their social and educational lives. It offers incredible opportunities for learning, creativity, and connection. However, it also exposes them to a unique set of risks that they may not be emotionally or developmentally equipped to handle on their own.[169]

Unique Risks for Youth

- **Cyberbullying:** This is one of the most prevalent dangers, involving harassment, spreading rumors, social exclusion, or posting humiliating photos or messages on social media or in online gaming environments. Unlike traditional bullying, cyberbullying can be relentless, following a child 24/7 into their own home.[169]
- **Online Predators:** Malicious adults may pose as children or teens on social media, gaming platforms, or chat apps to gain a child's trust. They may then attempt to solicit personal information, pressure the child into sending explicit images (a prelude to sextortion), or even try to arrange a dangerous in-person meeting.[169]
- **Inappropriate Content:** The internet contains a vast amount of content that is unsuitable for children, including real or simulated violence, pornography, hateful ideologies, and user-generated content that promotes dangerous activities like drug use or self-harm.[170]
- **Sexting and Sextortion:** "Sexting" refers to the sending of sexually explicit messages or photos. While sometimes consensual between teens, these images can be shared without consent, leading to widespread humiliation and bullying. This also opens the door to "sextortion," a form of blackmail where an attacker threatens to release the explicit images unless the victim pays them or provides more images.[170]

Guidance for Parents and Guardians

Protecting children online requires a combination of open communication, clear rules, and the use of technical tools.

- **Foster Open Communication:** This is the most important protective measure. Create a family environment where your child feels safe and comfortable talking to you about their online experiences, both good and bad. Reassure them that they can come to you without fear of punishment if they encounter anything scary or uncomfortable online. An open dialogue is more effective than any filter.[169]
- **Establish Clear Rules and Boundaries:** Work with your child to create a family media plan that outlines clear rules for device usage. This can include screen-time limits, screen-free zones (like the dinner table or bedrooms), and guidelines for appropriate online behavior. For younger children, keeping the computer in a common area of the house allows for easier supervision.[169]
- **Teach Digital Citizenship and Safety Basics:** Just as you teach them to look both ways before crossing the street, teach them the rules of the digital road:
  - **Protect Personal Information:** Emphasize that they should never share personal details like their full name, address, phone number, or school name with strangers online.[169]

    - **The Internet is Permanent:** Teach them to "think before you post." Explain that anything they share online—photos, comments, messages—can be copied and shared, and may exist forever, potentially impacting future college or job applications.[176]
    - **Strangers are Strangers:** Remind them that people online may not be who they say they are. They should treat online contacts as strangers and never agree to meet someone in person without your approval and supervision.[169]
- **Utilize Technical Tools:**
    - **Privacy Settings:** Sit down with your child and review the privacy settings on all their social media accounts, apps, and gaming platforms. Ensure their profiles are set to "private" or "friends only," not "public".[170]
    - **Parental Controls:** Use the parental control options provided by your Internet Service Provider (ISP) or built into devices and operating systems. These tools can help filter inappropriate content and limit screen time.[169]

Key Resources for Parents

Several organizations provide excellent, free resources to help parents navigate these challenges.

- **National Center for Missing & Exploited Children (NCMEC):** This is a critical resource for child safety.
    - **NetSmartz:** NCMEC's online safety education program offers free, age-appropriate videos, presentations, games, and activities for children from kindergarten through high school, as well as for parents and educators.[175]
    - **CyberTipline:** This is the nation's centralized reporting system for any suspected instance of online child sexual exploitation. If you or your child encounter such material, it should be reported to the CyberTipline immediately.[169]
    - **Take It Down:** This service helps victims get their nude or explicit images removed from the internet.[175]
- **Federal Trade Commission (FTC):** The FTC plays a key role in protecting children's privacy online.
    - **Children's Online Privacy Protection Act (COPPA):** This federal law requires websites and online services to obtain verifiable parental consent before collecting, using, or disclosing personal information from children under the age of 13.[134]
    - **Kids Online Safety Act (KOSA):** This proposed bipartisan legislation aims to strengthen protections by requiring platforms to make their features safer for minors and provide parents with more robust controls, including making the strongest privacy settings the default for young users.[148]

Chapter 9: Empowering Seniors in the Digital Age

Older adults have embraced the digital world to connect with family, manage their health, and access services. However, they are often specifically and relentlessly targeted by cybercriminals. Fraudsters perceive seniors as being more trusting, more likely to have significant savings or assets, and potentially less familiar with the fast-evolving landscape of digital technology and scams.[3] The statistics are alarming: in 2023, the FBI reported that individuals over the age of 60 lost a staggering $3.4 billion to internet crimes.[189]

Common Scams Targeting Seniors

While seniors can be victims of any type of scam, criminals often tailor their lures to this demographic.

- **Tech Support Scams:** This is a very common tactic. A victim receives an unsolicited phone call or sees an alarming pop-up on their computer screen that claims to be from a major tech company like Microsoft, Apple, or Geek Squad. The message warns of a non-existent virus or security issue and urges the victim to call a support number. If they call, the scammer will pressure them into granting remote access to their computer and then demand payment to "fix" the fake problem.[3]
- **Impersonation Scams (Government and Grandparent):** Scammers frequently impersonate official agencies. They may call or email pretending to be from the IRS, the Social Security Administration, or Medicare, claiming the victim owes money or that their benefits are at risk, in an attempt to steal personal information or solicit payment.[186] A particularly cruel variation is the "grandparent scam," where a criminal calls an older person, pretends to be their grandchild in a state of emergency (e.g., arrested, in a car accident), and desperately pleads for money to be wired immediately.[192]
- **Romance Scams:** Predators create fake profiles on dating sites and social media to target lonely or isolated seniors. They invest time in building a trusting, emotional relationship before inventing a sudden crisis—a medical emergency, a business problem, a travel issue—and asking for money.[3]
- **Phishing and Fake Websites:** Seniors are often targeted with phishing emails and fake websites that offer deals on prescription medications, low-cost health insurance, or pretend to be official bank notices to steal login credentials.[109]

Essential Safety Tips for Seniors

Empowerment comes from knowledge and the adoption of a few key, cautious habits.

- **Slow Down and Resist Pressure:** The number one tool of a scammer is creating a sense of urgency. They want you to act emotionally before you have time to think. If any call, text, or email feels rushed, threatening, or too good to be true, the best response is to **stop**. Hang up the phone. Delete the email. Do not respond immediately. Take a moment to breathe and think.[108]

- **Verify, Verify, Verify:** Never trust contact information provided in an unsolicited message. If you get a call that claims to be from your bank, hang up and call the official phone number printed on the back of your debit card or on your bank statement. If you get a suspicious email, do not click any links. Instead, open a new browser window and type the company's official website address yourself.[87]
- **Protect Your Accounts:** Secure all important online accounts with strong, unique passphrases and enable multi-factor authentication (MFA) wherever it is offered. A password manager can be an invaluable tool to help create and remember these secure credentials without having to write them down.[3]
- **Recognize Payment Scams:** This is a critical red flag. If anyone ever insists that you must pay them using a **gift card, a wire transfer service (like Western Union), or cryptocurrency**, it is **always a scam**. Legitimate businesses and government agencies will never demand payment through these untraceable methods. End the conversation immediately.[108]
- **Share With Care:** Be mindful of what you share on social media. Avoid posting your full birthdate, home address, or real-time vacation plans. The more personal information criminals can find about you online, the easier it is for them to target you.[108]
- **Ask for Help:** There is no shame in being targeted by these sophisticated scams. Talk to a trusted family member, friend, or neighbor if something feels off. A second opinion can often spot a scam that you might have missed. Acting quickly and talking to someone can help you get help and fix what happened.[108]

Key Resources for Seniors

- **Cybersecurity and Infrastructure Security Agency (CISA):** CISA's "Secure Our World" campaign provides easy-to-understand tip sheets and guidance specifically for older adults, focusing on the four basic steps of using strong passwords, enabling MFA, recognizing phishing, and updating software.[47]
- **AARP:** AARP is a leading advocate for senior safety and provides a wealth of resources. The **AARP Fraud Watch Network** offers up-to-date information on the latest scams, a scam-tracking map, and a helpline for victims. They also provide online safety games, videos, and articles covering everything from device protection to privacy settings.[87]
- **Federal Trade Commission (FTC):** The FTC's **Pass It On** campaign specifically enlists older adults to help each other learn how to recognize and report fraud and scams within their communities.[196]

Conclusion: A Lifelong Commitment to Digital Safety

The digital world is a landscape of immense opportunity and evolving risk. Navigating it safely is not about achieving a single, static state of "perfect security," but rather about adopting a lifelong commitment to a set of principles and practices that build resilience. This guide has been structured around the **SAFE** framework to provide a clear, actionable, and memorable path toward that resilience.

- **S – Secure Your Accounts and Devices:** This is the foundation. By using long, unique passphrases managed by a password manager, enabling multi-factor authentication on all critical accounts, keeping software and antivirus programs automatically updated, and properly securing your home Wi-Fi router, you build a formidable technical barrier against the majority of automated and opportunistic attacks.
- **A – Be Aware of the Threats:** Technology alone is not enough. A vigilant and informed user is a powerful "human firewall." By learning to recognize the signs of phishing, spot malicious websites, and understand the psychology of common scams, you can avoid the traps that criminals set to bypass technical defenses.
- **F – Fortify Your Privacy:** In the digital age, your personal data is a valuable commodity. By actively managing your digital footprint, being mindful of what you share online, and using platform privacy settings and tools like VPNs, you reduce your visibility to criminals and data brokers, making yourself a much harder target for the sophisticated, personalized attacks that are becoming increasingly common.
- **E – Know the Emergency Response:** In the event that a security incident does occur, knowing the correct steps to take can dramatically limit the damage. Having a clear plan to recover a hacked account, report identity theft to the FTC, and respond to a data breach allows you to act decisively and effectively in a stressful situation.

The threat landscape will continue to evolve. New challenges, driven by the increasing sophistication of Artificial Intelligence, the potential for deepfakes to erode trust, and the proliferation of Internet of Things (IoT) devices, will constantly emerge.[4] Cybersecurity is therefore not a destination, but a continuous journey of learning and adaptation.

The ultimate message of this guide is one of empowerment. While the risks of the digital world are real, they are manageable. By embracing the principles of the SAFE framework not as a one-time checklist but as a set of ongoing habits—a commitment to digital hygiene—you can navigate the online world with confidence, harnessing its incredible benefits while skillfully mitigating its dangers.

Appendix: Quick Reference Guide & Glossary

One-Page Quick Reference Guide: Five Critical Security Actions

This guide provides a printable summary of the five most critical, high-impact security actions every user should take. These practices form the core of strong personal cyber hygiene.

1. **Use Strong, Unique Passwords & a Password Manager**
   - **Action:** Stop reusing passwords. Use a different, unique password for every single online account. Make passwords long (16+ characters) by using a memorable passphrase of several unrelated words.
   - **Why:** This prevents a "credential stuffing" attack, where a password stolen from one site is used to break into your other, more important accounts.[11]
   - **Tool:** Use a reputable password manager to generate, store, and fill in your passwords. You only need to remember one strong master password.[35]
2. **Turn On Multi-Factor Authentication (MFA)**
   - **Action:** Enable MFA on all critical accounts, especially email, banking, and social media. Use an authenticator app or a physical security key for the best protection.
   - **Why:** MFA makes you 99% less likely to be hacked. Even if a criminal steals your password, they cannot log in without the second factor.[49]
   - **How:** Go to the "Security" settings of your accounts and look for the "Two-Factor Authentication" or "2-Step Verification" option.[51]
3. **Recognize & Report Phishing**
   - **Action:** Be suspicious of unexpected emails, texts, or messages that create urgency or fear. Hover over links to check their true destination before clicking. Verify the sender's email address.
   - **Why:** Phishing is the number one way criminals steal credentials and deliver malware. Learning to spot the signs is a critical defense.[14]
   - **Response:** If an email looks suspicious, delete it. Do not click any links or open attachments. Report it as spam or phishing within your email client.[47]
4. **Keep Your Software Updated**
   - **Action:** Enable automatic updates for your operating system (Windows, macOS), web browser, and all applications. Do not click "Remind Me Later" on update prompts.
   - **Why:** Software updates contain essential security patches that fix vulnerabilities. Unpatched software is a primary target for hackers.[60]
   - **Tool:** Ensure reputable antivirus software is installed and also set to update automatically.[64]
5. **Secure Your Home Wi-Fi Router**
   - **Action:** Log in to your router and change the default administrator password and network name (SSID). Enable WPA3 (or WPA2) encryption and set a strong, unique Wi-Fi password. Keep the router's firmware updated.
   - **Why:** Your router is the gateway to your entire home network. An unsecured router can be compromised, putting every device connected to it at risk.[75]
   - **Bonus:** Enable the guest network for visitors to keep their devices separate from your main network.[75]

Glossary of Terms

- **Adware:** Software that automatically displays or downloads advertising material (often unwanted) when a user is online.[21]
- **Antivirus Software:** A program designed to detect, prevent, and remove malicious software (malware) from computers and devices.[64]
- **Botnet:** A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam or launch DDoS attacks.[21]
- **Credential Stuffing:** An automated attack where criminals use stolen usernames and passwords from one data breach to try and log in to many other services, exploiting password reuse.[11]
- **Cyber Hygiene:** A set of routine practices that users can follow to improve their online security and maintain system health.[10]
- **Data Breach:** An incident where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.[5]
- **Deepfake:** Synthetic media (video or audio) in which a person's likeness has been replaced with someone else's, created using artificial intelligence techniques.[6]
- **Digital Footprint:** The trail of data an individual creates while using the internet, including both active (intentional posts) and passive (browsing history, IP address) data.[30]
- **Encryption:** The process of converting information or data into a code, especially to prevent unauthorized access. WPA3 is a strong encryption standard for Wi-Fi.[48]
- **Firewall:** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules, acting as a barrier between a trusted network and an untrusted network.[69]
- **Identity Theft:** The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.[31]
- **Malware:** Short for "malicious software," it is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, or deprive users access to their information.[21]
- **Multi-Factor Authentication (MFA):** A security process that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.[47]
- **NIST (National Institute of Standards and Technology):** A U.S. government agency that develops standards and guidelines for technology and cybersecurity, including influential password guidance.[38]
- **Passphrase:** A sequence of words or other text used to control access to a computer system, program, or data. Recommended as a more secure and memorable alternative

to traditional passwords.[42]

- **Password Manager:** A software application designed to store and manage online credentials. They generate strong, unique passwords for different sites and store them in an encrypted vault.[42]
- **Phishing:** A type of social engineering attack where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information or to deploy malicious software on the victim's infrastructure.[15]
- **Ransomware:** A type of malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.[22]
- **Social Engineering:** The use of psychological manipulation to trick users into making security mistakes or giving away sensitive information.[12]
- **Spyware:** Malware that secretly observes the user's activities on their computer without their permission and reports it to the software's author.[26]
- **Trojan (or Trojan Horse):** A type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.[26]
- **VPN (Virtual Private Network):** A service that creates a secure, encrypted connection over a less secure network, such as the public internet. It masks the user's IP address and encrypts their traffic.[114]
- **Worm:** A standalone malware computer program that replicates itself in order to spread to other computers, often using a computer network to spread itself.[26]

Works cited

1. www.nationwide.com, accessed June 16, 2025, https://www.nationwide.com/lc/resources/personal-finance/articles/how-malware-works#:~:text=The%20term%20%22malware%22%20refers%20to,an%20electronic%20device's%20normal%20operation.&text=Malware%20can%20infect%20personal%20computers,any%20device%20with%20computing%20capabilities.
2. 5 Steps to Protect Your Digital Home - CISA, accessed June 16, 2025, https://www.cisa.gov/sites/default/files/publications/NCSAM_YourDigitalHome_2020.pdf
3. Internet Safety for Seniors: Essential Tips You Need to Know, accessed June 16, 2025, https://chandlerplace.seniorlivingnearme.com/blogs/internet-safety-for-seniors-essential-tips-you-need-to-know
4. 10 Cyber Security Trends For 2025 - SentinelOne, accessed June 16, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/
5. Key Cyber Security Statistics for 2025 - SentinelOne, accessed June 16, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/
6. Top Cybersecurity Threats [2025] - University of San Diego Online Degrees,

accessed June 16, 2025, https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

7. The cyber threats to watch in 2025, and other cybersecurity news to know this month - The World Economic Forum, accessed June 16, 2025, https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/
8. IBM X-Force 2025 Threat Intelligence Index, accessed June 16, 2025, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
9. Shields Up - CISA, accessed June 16, 2025, https://www.cisa.gov/shields-up
10. Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA, accessed June 16, 2025, https://www.cisa.gov/topics/cybersecurity-best-practices
11. What is Phishing & How does it work? - Huntress, accessed June 16, 2025, https://www.huntress.com/defenders-handbooks/defenders-handbook-phishing
12. www.cmu.edu, accessed June 16, 2025, https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html#:~:text=Social%20engineering%20is%20the%20tactic,or%20giving%20away%20sensitive%20information.
13. What is Social Engineering | Attack Techniques & Prevention Methods - Imperva, accessed June 16, 2025, https://www.imperva.com/learn/application-security/social-engineering-attack/
14. What Is Social Engineering? - Definition, Types & More | Proofpoint US, accessed June 16, 2025, https://www.proofpoint.com/us/threat-reference/social-engineering
15. What is Phishing? Techniques and Prevention | CrowdStrike, accessed June 16, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/phishing-attack/
16. Social Engineering - Information Security Office - Computing ..., accessed June 16, 2025, https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html
17. The dangers of oversharing - Microsoft Support, accessed June 16, 2025, https://support.microsoft.com/en-us/topic/the-dangers-of-oversharing-79330a32-4ee1-433a-812e-fe4bb3d34511
18. How oversharing on social media could put your personal information at risk, accessed June 16, 2025, https://its.uky.edu/news/how-oversharing-on-social-media-could-put-your-personal-information-risk
19. How Oversharing Online Creates Serious Cybersecurity Risks for Organizations - Everfox, accessed June 16, 2025, https://www.everfox.com/blog/techhub/online-oversharing-cybersecurity-risks
20. The Risks of Oversharing: What You Need to Know About Social Media Privacy | First Bank & Trust Company, accessed June 16, 2025, https://www.firstbank.com/resources/learning-center/the-risks-of-oversharing-what-you-need-to-know-about-social-media-privacy/

21. What Is Malware? - Palo Alto Networks, accessed June 16, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-malware
22. What Is Ransomware? Definition & Prevention | Proofpoint US, accessed June 16, 2025, https://www.proofpoint.com/us/threat-reference/ransomware
23. www.itgovernance.co.uk, accessed June 16, 2025, https://www.itgovernance.co.uk/phishing#:~:text=Phishing%20works%20by%20sending%20messages,as%20their%20credit%20card%20number.
24. What is phishing | Attack techniques & scam examples - Imperva, accessed June 16, 2025, https://www.imperva.com/learn/application-security/phishing-attack-scam/
25. The Dos and Don'ts of Clicking Links for Better Email Security ..., accessed June 16, 2025, https://www.resultstechnology.com/blog/the-dos-and-donts-of-clicking-links-for-email-security/
26. What is Malware and How Does it Work - Nationwide, accessed June 16, 2025, https://www.nationwide.com/lc/resources/personal-finance/articles/how-malware-works
27. www.ncsc.gov.uk, accessed June 16, 2025, https://www.ncsc.gov.uk/ransomware/home#:~:text=What%20is%20ransomware%3F-,Ransomware%20is%20a%20type%20of%20malware%20which%20prevents%20you%20from,be%20encrypted%2C%20stolen%20or%20deleted.
28. Ransomware | Cyber.gov.au, accessed June 16, 2025, https://www.cyber.gov.au/threats/types-threats/ransomware
29. A guide to ransomware - NCSC.GOV.UK, accessed June 16, 2025, https://www.ncsc.gov.uk/ransomware/home
30. Digital footprint (ITSAP.00.133) - Canadian Centre for Cyber Security, accessed June 16, 2025, https://www.cyber.gc.ca/en/guidance/digital-footprint-itsap00133
31. www.texasattorneygeneral.gov, accessed June 16, 2025, https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/what-identity-theft#:~:text=Identity%20theft%20happens%20when%20someone,accounts%2C%20or%20obtain%20medical%20services.
32. What is Identity Theft? | Office of the Attorney General, accessed June 16, 2025, https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/what-identity-theft
33. Identity Theft and Your Social Security Number - SSA, accessed June 16, 2025, https://www.ssa.gov/pubs/EN-05-10064.pdf
34. What To Know About Identity Theft | Consumer Advice, accessed June 16, 2025, https://consumer.ftc.gov/articles/what-know-about-identity-theft
35. NIST Password Guidelines: What You Need to Know - 1Password Blog, accessed June 16, 2025, https://blog.1password.com/nist-password-guidelines-update/
36. 2024 NIST Password Guidelines: What You Need to Know - Descope, accessed June 16, 2025, https://www.descope.com/blog/post/2024-nist-password-guidelines
37. 2025 NIST Password Guidelines: Enhancing Security Practices, accessed June 16, 2025,

https://securityboulevard.com/2024/09/2024-nist-password-guidelines-enhancing-security-practices/
38. linfordco.com, accessed June 16, 2025, https://linfordco.com/blog/nist-password-policy-guidelines/#:~:text=Password%20length%3A%20The%20absolute%20minimum,of%20at%20least%2064%20characters.
39. NIST Password Policy Guidelines 2024: What You Need to Know - Linford & Company LLP, accessed June 16, 2025, https://linfordco.com/blog/nist-password-policy-guidelines/
40. NIST's September 2024 Update to Password Guidelines: Improved User Experience., accessed June 16, 2025, https://www.authsignal.com/blog/articles/nists-september-2024-update-to-password-guidelines-improved-user-experience
41. Create and use strong passwords - Microsoft Support, accessed June 16, 2025, https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
42. Use Strong Passwords | CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world/use-strong-passwords
43. Protect Your Personal Information From Hackers and Scammers ..., accessed June 16, 2025, https://consumer.ftc.gov/articles/protect-your-personal-information-hackers-and-scammers
44. Create a strong password & a more secure account - Google Help, accessed June 16, 2025, https://support.google.com/accounts/answer/32040?hl=en
45. Password Best Practices | UC Santa Barbara Information Technology, accessed June 16, 2025, https://www.it.ucsb.edu/general-security-resources/password-best-practices
46. Tips for Creating a Strong Password - LastPass, accessed June 16, 2025, https://www.lastpass.com/features/password-generator/tips-for-creating-strong-passwords
47. Secure Our World - CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world
48. Cybersecurity Basics | Federal Trade Commission, accessed June 16, 2025, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics
49. Multifactor Authentication | Cybersecurity and Infrastructure Security Agency CISA, accessed June 16, 2025, https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication
50. Secure Yourself & Your Family - CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world/secure-yourself-your-family
51. Turn On MFA | CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world/turn-mfa
52. More than a Password - CISA, accessed June 16, 2025, https://www.cisa.gov/MFA
53. Getting started with multi-factor authentication (MFA) - ID.me Help Center, accessed June 16, 2025,

https://help.id.me/hc/en-us/articles/360018113053-Getting-started-with-multi-factor-authentication-MFA

54. CISA Publishes Multi-Factor Authentication Guidelines to Tackle Phishing, accessed June 16, 2025, https://www.infosecurity-magazine.com/news/cisa-mfa-guidelines-to-tackle/
55. Set up your Microsoft 365 sign-in for multi-factor authentication, accessed June 16, 2025, https://support.microsoft.com/en-us/office/set-up-your-microsoft-365-sign-in-for-multi-factor-authentication-ace1d096-61e5-449b-a875-58eb3d74de14
56. Turn on 2-Step Verification - Computer - Google Account Help, accessed June 16, 2025, https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DDesktop
57. Require Multifactor Authentication - CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world/require-multifactor-authentication
58. CISA Guidance: Numbers Matching and Phishing-Resistant MFA, accessed June 16, 2025, https://fairviewinvest.com/news/cisa-guidance-phishing-mfa/
59. Two-factor authentication for Apple Account, accessed June 16, 2025, https://support.apple.com/en-us/102660
60. Update Software | CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world/update-software
61. Why keeping your software up to date is important for cybersecurity? - University of Idaho, accessed June 16, 2025, https://support.uidaho.edu/TDClient/40/Portal/KB/ArticleDet?ID=2770
62. Why Software Updates Are Critical for Cybersecurity in 2025: Protect Your Business from Emerging Threats | Superior IT Perth, accessed June 16, 2025, https://www.superiorit.com.au/blog-posts/why-software-updates-are-critical-for-cybersecurity-in-2025-protect-your-business-from-emerging-threats
63. www.ericom.com, accessed June 16, 2025, https://www.ericom.com/glossary/what-is-antivirus-software/#:~:text=Antivirus%20software%20safeguards%20your%20devices,phishing%20attempts%2C%20and%20other%20cyberattacks.
64. What is an antivirus product? Do I need one? - NCSC.GOV.UK, accessed June 16, 2025, https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product
65. What Is Antivirus Software? - Sophos, accessed June 16, 2025, https://www.sophos.com/en-us/cybersecurity-explained/antivirus
66. Understanding Anti-Virus Software | CISA, accessed June 16, 2025, https://www.cisa.gov/news-events/news/understanding-anti-virus-software
67. Understanding Antivirus Software, accessed June 16, 2025, https://www.ericom.com/glossary/what-is-antivirus-software/
68. Home Network Security - CISA, accessed June 16, 2025, https://www.cisa.gov/news-events/news/home-network-security
69. www.paloaltonetworks.com, accessed June 16, 2025, https://www.paloaltonetworks.com/cyberpedia/what-are-the-benefits-of-a-firewall#:~:text=A%20firewall%20is%20a%20system,threats%20and%20controlling%2

0data%20flow.

70. What Is Firewall Security? How to Protect Your Infrastructure - F5, accessed June 16, 2025, https://www.f5.com/glossary/firewall-security
71. Firewalls for Network Security: Importance, Types & Best Practices - Exabeam, accessed June 16, 2025, https://www.exabeam.com/explainers/network-security/firewalls-for-network-security-importance-types-and-best-practices/
72. What is a Firewall? Types, history, methods & importance - NordLayer, accessed June 16, 2025, https://nordlayer.com/learn/firewall/what-is-firewall/
73. Understanding Firewalls for Home and Small Office Use | CISA, accessed June 16, 2025, https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use
74. Firewalls: how important are they? - BCS365, accessed June 16, 2025, https://bcs365.com/insights/firewalls-how-important-are-they
75. How To Secure Your Home Wi-Fi Network | Consumer Advice, accessed June 16, 2025, https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network
76. Best Practices for Securing Your Home Network - Department of Defense, accessed June 16, 2025, https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF
77. Module 5: Securing Your Home Wi-Fi - CISA, accessed June 16, 2025, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module5
78. Wi-Fi Security Settings: 10 Steps to Secure Your WiFi Router | TP-Link Philippines, accessed June 16, 2025, https://www.tp-link.com/ph/blog/1778/wi-fi-security-settings-10-steps-to-secure-your-wifi-router/
79. Router Security, accessed June 16, 2025, https://routersecurity.org/
80. How to Secure Your Wi-Fi in 7 Simple Steps | Norton, accessed June 16, 2025, https://us.norton.com/blog/iot/keep-your-home-wifi-safe
81. Recommended settings for Wi-Fi routers and access points - Apple Support, accessed June 16, 2025, https://support.apple.com/en-us/102766
82. 5 simple ways to avoid malicious emails - Alliance InfoSystems, accessed June 16, 2025, https://www.ainfosys.com/blog/5-simple-ways-to-avoid-malicious-emails/
83. Handling Unexpected or Suspicious Email Attachments | Division of Information Technology, accessed June 16, 2025, https://it.stonybrook.edu/help/kb/handling-unexpected-or-suspicious-email-attachments
84. Recognize and Report Phishing - CISA, accessed June 16, 2025, https://www.cisa.gov/secure-our-world/recognize-and-report-phishing
85. Avoiding Social Engineering and Phishing Attacks | CISA, accessed June 16, 2025, https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
86. Email Security Best Practices – The Dos And Don'ts - GSC IT Solutions, accessed June 16, 2025,

https://gscitsolutions.com/news/email-security-best-practices-the-dos-and-donts/
87. Re: Tips for Staying Safe & Secure Online - AARP Online Community, accessed June 16, 2025, https://community.aarp.org/t5/Computer-Questions-Tips/Tips-for-Staying-Safe-amp-Secure-Online/m-p/2388445
88. How To Avoid a Scam | Consumer Advice, accessed June 16, 2025, https://consumer.ftc.gov/articles/how-avoid-scam
89. How Can You Protect Yourself Against Malicious Software in Attachments?, accessed June 16, 2025, https://guardiandigital.com/resources/faq/why-are-email-attachments-dangerous
90. Do's & Dont's of Cybersecurity - Zane State College, accessed June 16, 2025, https://www.zanestate.edu/dos-donts-of-cybersecurity/
91. Using Caution with Email Attachments - CISA, accessed June 16, 2025, https://www.cisa.gov/news-events/news/using-caution-email-attachments
92. 9 Email Security Best Practices (Ultimate Guide 2025) - Hoxhunt, accessed June 16, 2025, https://hoxhunt.com/blog/email-security-best-practices
93. Computer Security Tips | Consumer Advice, accessed June 16, 2025, https://consumer.ftc.gov/media/79887
94. Online Shopping - Security Tips | Consumer Advice - Federal Trade Commission, accessed June 16, 2025, https://consumer.ftc.gov/media/79929
95. Identifying and Understanding Malicious Websites | NordLayer, accessed June 16, 2025, https://nordlayer.com/blog/what-are-malicious-websites/
96. 5 Ways to Identify a Phishing Website - MetaCompliance, accessed June 16, 2025, https://www.metacompliance.com/blog/phishing-and-ransomware/5-ways-to-identify-a-phishing-website
97. How To Identify Fake Websites: 11 Warning Signs To Know - Aura, accessed June 16, 2025, https://www.aura.com/learn/how-to-identify-fake-websites
98. 5 URL Warning Signs to Watch For | INFORMATION TECHNOLOGY, accessed June 16, 2025, https://www.du.edu/it/services/security/5-url-warning-signs
99. 7 Ways to Quickly Detect Malicious Websites | Memcyco, accessed June 16, 2025, https://www.memcyco.com/7-ways-to-quickly-detect-malicious-websites/
100. How to Update Your Software - National Cybersecurity Alliance, accessed June 16, 2025, https://www.staysafeonline.org/articles/software-updates
101. nordlayer.com, accessed June 16, 2025, https://nordlayer.com/blog/safe-file-download-tips/#:~:text=Verify%20the%20source%20before%20downloading%20files&text=Only%20download%20from%20trusted%20websites,%3A%2F%2F)%20and%20clear%20sender%20addresses.
102. How to Download on The Internet Safely - Fortec US, accessed June 16, 2025, https://fortec.us/blog/how-to-download-on-the-internet-safely/
103. Maximizing Security: Best Practices for Managing Your Downloads on This Computer, accessed June 16, 2025, https://www.ask.com/news/maximizing-security-best-practices-managing-downloads-computer

104. Malware: How To Protect Against, Detect, and Remove It | Consumer Advice, accessed June 16, 2025, https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it
105. Is this download safe? Cybersecurity tips for businesses - NordLayer, accessed June 16, 2025, https://nordlayer.com/blog/safe-file-download-tips/
106. Scams and Your Small Business: A Guide for Business | Federal Trade Commission, accessed June 16, 2025, https://www.ftc.gov/business-guidance/resources/scams-your-small-business-guide-business
107. How To Avoid Scams After Weather Emergencies and Natural Disasters | Consumer Advice, accessed June 16, 2025, https://consumer.ftc.gov/articles/how-avoid-scams-after-weather-emergencies-and-natural-disasters
108. Secure-Our-World-Online-Safety-for-Older-Adults-Tip-Sheet.pdf - CISA, accessed June 16, 2025, https://www.cisa.gov/sites/default/files/2025-01/Secure-Our-World-Online-Safety-for-Older-Adults-Tip-Sheet.pdf
109. CYBERSECURITY AND OLDER AMERICANS - CISA, accessed June 16, 2025, https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Older%2520Americans.pdf
110. www.nsw.gov.au, accessed June 16, 2025, https://www.nsw.gov.au/education-and-training/digital-citizenship/healthy-online-habits/digital-footprint#:~:text=Every%20time%20you're%20online,access%20and%20share%20this%20information.
111. Leaving a digital footprint | NSW Government, accessed June 16, 2025, https://www.nsw.gov.au/education-and-training/digital-citizenship/healthy-online-habits/digital-footprint
112. What Is a Digital Footprint and Why Is It Important? - Dashlane, accessed June 16, 2025, https://www.dashlane.com/blog/what-is-a-digital-footprint
113. Teaching About Digital Footprints to K-12 Students - Learning.com, accessed June 16, 2025, https://www.learning.com/blog/digital-footprints/
114. Best Ways to Reduce Your Digital Footprint Now - LevelBlue, accessed June 16, 2025, https://levelblue.com/blogs/security-essentials/best-ways-to-reduce-your-digital-footprint-now
115. Limit Your Digital Footprint | CISA, accessed June 16, 2025, https://www.cisa.gov/resources-tools/training/limit-your-digital-footprint
116. Protecting Your Digital Footprint: Tips from CISA | Align Wealth Strategies, accessed June 16, 2025, https://alignretire.com/resources/digital-footprint/
117. Protect Your Digital Footprint | Morgan Stanley, accessed June 16, 2025, https://www.morganstanley.com/articles/digital-footprint-protection-strategies
118. How To Manage Your Digital Footprint for 2025: 20 Tips for Students | Research.com, accessed June 16, 2025, https://research.com/education/how-to-manage-digital-footprint

119. 10 Ways to Minimize Your Digital Footprint, accessed June 16, 2025, https://febabenefits.org/blog/10-ways-to-minimize-your-digital-footprint/
120. TPT: Digital footprint: what is it? How to check and delete it? : r/TechnologyProTips - Reddit, accessed June 16, 2025, https://www.reddit.com/r/TechnologyProTips/comments/198szv2/tpt_digital_footprint_what_is_it_how_to_check_and/
121. Manage Application Permissions for Privacy and Security | CISA, accessed June 16, 2025, https://www.cisa.gov/resources-tools/training/manage-application-permissions-privacy-and-security
122. The Dangers of Oversharing Online | Digital4Good - ICanHelp, accessed June 16, 2025, https://www.icanhelp.net/blog/the-dangers-of-oversharing-online
123. Tips for Staying Safe and Secure Online - AARP, accessed June 16, 2025, https://www.aarp.org/personal-technology/privacy-for-seniors/
124. 5 Easy Ways to Protect Yourself From Web Hackers and Eavesdroppers - AARP, accessed June 16, 2025, https://www.aarp.org/personal-technology/protect-your-devices/
125. Older Adults Wary About Their Privacy Online - AARP, accessed June 16, 2025, https://www.aarp.org/personal-technology/companies-address-online-privacy-concerns/
126. Digital citizenship: pre-teens and teens being responsible online, accessed June 16, 2025, https://raisingchildren.net.au/pre-teens/entertainment-technology/digital-life/digital-citizenship
127. Why Digital Responsibility Matters: The Unspoken Rules of Online Behavior - NameSilo, accessed June 16, 2025, https://www.namesilo.com/blog/en/privacy-security/why-digital-responsibility-matters-the-unspoken-rules-of-online-behavior
128. Responsible sharing - (Media Literacy) - Vocab, Definition, Explanations | Fiveable, accessed June 16, 2025, https://library.fiveable.me/key-terms/media-literacy/responsible-sharing
129. How To Keep Seniors Safe in the Digital Age: A Social Media Guide | All About Cookies, accessed June 16, 2025, https://allaboutcookies.org/social-media-safety-for-seniors
130. What is Sharenting? The Risks and Dangers of Oversharing Online - A Healthier Michigan, accessed June 16, 2025, https://www.ahealthiermichigan.org/stories/health-and-wellness/what-is-sharenting-the-risks-and-dangers-of-oversharing-online
131. Privacy Settings - Google Play Community, accessed June 16, 2025, https://support.google.com/googleplay/thread/311424709/privacy-settings?hl=en
132. The Ultimate Facebook Privacy Settings Guide - IPVanish, accessed June 16, 2025, https://www.ipvanish.com/blog/facebook-privacy-settings/
133. How to Change Privacy Settings on Twitter Fast | VeePN Blog, accessed June 16, 2025, https://veepn.com/blog/how-to-change-privacy-settings-on-twitter/
134. FTC forum highlights the road to improving children's online safety - IAPP,

accessed June 16, 2025, https://iapp.org/news/a/ftc-forum-highlights-the-road-to-improving-childrens-online-safety

135. Privacy Checkup - Google, accessed June 16, 2025, https://myaccount.google.com/intro/privacycheckup
136. Data Privacy Settings, Controls & Tools - Google Safety Center, accessed June 16, 2025, https://safety.google/intl/en_us/settings/privacy-settings
137. Data Privacy Settings, Controls & Tools - Google Safety Center, accessed June 16, 2025, https://safety.google/privacy/privacy-controls/
138. www.cyber.nj.gov, accessed June 16, 2025, https://www.cyber.nj.gov/guidance-and-best-practices/social-media-security/guide-to-accessing-facebook-s-security-privacy-settings#:~:text=To%20access%20your%20Settings%2C%20click,can%20find%20and%20contact%20you.
139. Manage Facebook Privacy Settings: A Complete Guide - wikiHow, accessed June 16, 2025, https://www.wikihow.com/Manage-Facebook-Privacy-Settings
140. Facebook: Adjusting Your Privacy Settings - GCFGlobal, accessed June 16, 2025, https://edu.gcfglobal.org/en/facebook101/adjusting-your-privacy-settings/1/
141. How to Change Your Privacy Settings on Facebook - Avast, accessed June 16, 2025, https://www.avast.com/c-change-facebook-privacy-settings
142. Guide to Accessing Facebook's Security & Privacy Settings - NJCCIC - NJ.gov, accessed June 16, 2025, https://www.cyber.nj.gov/guidance-and-best-practices/social-media-security/guide-to-accessing-facebook-s-security-privacy-settings
143. Controlling your X privacy settings | Learning Module | Introduction to Twitter Online Course, accessed June 16, 2025, https://beconnected.esafety.gov.au/topic-library/social-media-apps/introduction-to-twitter/controlling-your-x-privacy-settings
144. The Ultimate Twitter Privacy Settings Guide - IPVanish, accessed June 16, 2025, https://www.ipvanish.com/blog/x-twitter-privacy-settings/
145. X: How to change your privacy settings - Android Police, accessed June 16, 2025, https://www.androidpolice.com/how-to-change-privacy-safety-settings-x/
146. beconnected.esafety.gov.au, accessed June 16, 2025, https://beconnected.esafety.gov.au/topic-library/social-media-apps/introduction-to-twitter/controlling-your-x-privacy-settings#:~:text=At%20the%20top%20of%20the,X%20users%20who%20follow%20you.
147. X (Twitter) parental controls - Internet Matters, accessed June 16, 2025, https://www.internetmatters.org/parental-controls/social-media/twitter/
148. Kids Online Safety Act | U.S. Senator Richard Blumenthal, accessed June 16, 2025, https://www.blumenthal.senate.gov/about/issues/kids-online-safety-act
149. How To Recover Your Hacked Email or Social Media Account ..., accessed June 16, 2025, https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account
150. What do you do if your Facebook account is hacked? I can't log in, can't get

any feedback about what to do or how long it will take. - Quora, accessed June 16, 2025, https://www.quora.com/What-do-you-do-if-your-Facebook-account-is-hacked-I-cant-log-in-cant-get-any-feedback-about-what-to-do-or-how-long-it-will-take

151. Your social media account has been hijacked. Now what? - LifeLock, accessed June 16, 2025, https://lifelock.norton.com/learn/internet-security/social-media-hackers

152. How to Take Back Control of a Social Media Account - National Cybersecurity Alliance, accessed June 16, 2025, https://www.staysafeonline.org/articles/how-to-take-back-control-of-a-social-media-account

153. Hacked social media guide and free expert help - The Cyber Helpline, accessed June 16, 2025, https://www.thecyberhelpline.com/guides/hacked-social-account

154. What to Do If Your Identity Is Stolen | Office of the Attorney General, accessed June 16, 2025, https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/what-do-if-your-identity-stolen

155. IdentityTheft.gov, accessed June 16, 2025, https://www.identitytheft.gov/

156. Identity theft | USAGov, accessed June 16, 2025, https://www.usa.gov/identity-theft

157. Report Identity Theft | Federal Trade Commission, accessed June 16, 2025, https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft

158. IdentityTheft.gov Recovery Checklist, accessed June 16, 2025, https://www.bulkorder.ftc.gov/system/files/publications/pdf-0204_identitytheftwhat_to_do_right_away_0.pdf

159. Identity Theft: A Recovery Plan - Bulkorder.ftc.gov - Federal Trade Commission, accessed June 16, 2025, https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf

160. What to Do Next - IdentityTheft.gov, accessed June 16, 2025, https://www.identitytheft.gov/Steps?scroll=true

161. What do I do if I've been a victim of identity theft? | Consumer Financial Protection Bureau, accessed June 16, 2025, https://www.consumerfinance.gov/ask-cfpb/what-do-i-do-if-i-think-i-have-been-a-victim-of-identity-theft-en-31/

162. What to Do After a Data Breach - Kansas State University, accessed June 16, 2025, https://support.ksu.edu/TDClient/30/Portal/KB/ArticleDet?ID=1259

163. FTC Identity Theft Guide: How to Recover | Pinnacle Financial Partners, accessed June 16, 2025, https://pnfp.com/learning-center/fraud-and-security/safe-online-practices-for-consumers/ftc-identity-theft-guide-how-to-recover/

164. what to do if your identity is stolen - Department of Justice, accessed June 16, 2025, https://www.justice.gov/usao-wdmi/file/764151/dl?inline

165. 7 steps to take if your personal data has been compromised online | Fulton Bank, accessed June 16, 2025, https://www.fultonbank.com/Education-Center/Privacy-and-Security/personal-data-breach-tips
166. Here's What To Do After a Data Breach - Equifax, accessed June 16, 2025, https://www.equifax.com/personal/education/cybersecurity/articles/-/learn/after-data-breach/
167. Data Breach - Internet Crime Complaint Center (IC3), accessed June 16, 2025, https://www.ic3.gov/CrimeInfo/DataBreach
168. www.ftc.gov, accessed June 16, 2025, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
169. Online Safety | Nemours KidsHealth, accessed June 16, 2025, https://kidshealth.org/en/parents/net-safety.html
170. Online safety for teenagers | Raising Children Network, accessed June 16, 2025, https://raisingchildren.net.au/teens/entertainment-technology/cyberbullying-online-safety/internet-safety-teens
171. Internet Risks | Cottage Grove Oregon, accessed June 16, 2025, https://www.cottagegroveor.gov/police/page/internet-risks
172. Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online, accessed June 16, 2025, https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online
173. Child and Youth Safety Online - the United Nations, accessed June 16, 2025, https://www.un.org/en/global-issues/child-and-youth-safety-online
174. Online Safety Tips for Teens | NCDIT - NC.gov, accessed June 16, 2025, https://it.nc.gov/resources/online-safety-privacy/tips-guidance/online-safety-tips-teens
175. NetSmartz Home - MissingKids.org, accessed June 16, 2025, https://www.missingkids.org/netsmartz/home
176. How to keep your child safe online | UNICEF Parenting, accessed June 16, 2025, https://www.unicef.org/parenting/child-care/keep-your-child-safe-online
177. 10 Internet Safety Tips for Kids - Create & Learn, accessed June 16, 2025, https://www.create-learn.us/blog/internet-safety-tips-for-kids/
178. Resources - MissingKids.org, accessed June 16, 2025, https://www.missingkids.org/netsmartz/resources
179. CyberTipline - MissingKids.org, accessed June 16, 2025, https://www.missingkids.org/gethelpnow/cybertipline
180. National Center for Missing & Exploited Children, accessed June 16, 2025, https://www.missingkids.org/home
181. Children's Privacy | Federal Trade Commission, accessed June 16, 2025, https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy
182. The FTC takes on kids online safety - POLITICO, accessed June 16, 2025, https://www.politico.com/newsletters/future-pulse/2025/06/05/the-ftc-takes-on-

kids-online-safety-00388839

183. Protecting Your Child's Privacy Online | Consumer Advice - Federal Trade Commission, accessed June 16, 2025, https://consumer.ftc.gov/articles/protecting-your-childs-privacy-online

184. Online Safety for Seniors - CyberInsureOne, accessed June 16, 2025, https://cyberinsureone.com/online-safety-seniors/

185. Online Safety for Seniors: A Complete Guide | Poper Blocker, accessed June 16, 2025, https://poperblocker.com/online-safety-for-seniors/

186. Internet Safety for Seniors | Washington State, accessed June 16, 2025, https://www.atg.wa.gov/internet-safety-seniors

187. Online Safety For Seniors - LCB Senior Living, accessed June 16, 2025, https://www.lcbseniorliving.com/blog/online-safety-for-seniors/

188. Cybersecurity Awareness: Internet Safety Tips for Seniors, accessed June 16, 2025, https://springpointsl.org/blog/cybersecurity-awareness-internet-safety-tips-for-seniors/

189. AT&T and AARP Join Forces for Senior Cyber Safety with Tech Kits for Nonprofits - Dallas Innovates, accessed June 16, 2025, https://dallasinnovates.com/att-and-aarp-join-forces-for-senior-cyber-safety-with-tech-kits-for-nonprofits/

190. Internet Safety Tips for Older Adults - Braven Health, accessed June 16, 2025, https://bravenhealth.com/blog/detail/internet-safety-tips-older-adults

191. Cybersecurity Guide for Seniors: A 2025 Update, accessed June 16, 2025, https://floridaseniorconsulting.com/cybersecurity-guide-for-seniors-2025/

192. Cybersecurity for Seniors: A Guide for Loved Ones | Morgan Stanley, accessed June 16, 2025, https://www.morganstanley.com/articles/cybersecurity-for-seniors

193. How to Improve Your Personal Cyber Security - The National Council on Aging (NCOA), accessed June 16, 2025, https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security/

194. How can technology help protect older adults online? | Google Public Policy, accessed June 16, 2025, https://publicpolicy.google/article/how-can-tech-protect-adults-online/

195. Seniors - Security in Depth, accessed June 16, 2025, https://securityindepth.com.au/seniors-1

196. OLDER AMERICANS - CISA, accessed June 16, 2025, https://www.cisa.gov/sites/default/files/publications/Older%2520Americans%2520Presentation.pdf

197. Seniors Online Safety Tips - Enterprise Technology Services, accessed June 16, 2025, https://ets.wyo.gov/cybersecurity/specific-audience/seniors-online-safety-tips

198. Digital Essentials: Online Safety - YouTube, accessed June 16, 2025, https://www.youtube.com/watch?v=6TNLawXHQwk

199. Staying Safe on Social Media Game - AARP eLearn, accessed June 16, 2025, https://elearn.aarp.org/URL/StayingSafeOnSocial

200. Online Safety Basics - AARP, accessed June 16, 2025, https://www.aarp.org/videos/personal-technology/3948774377001/
201. Staying Safe Online - AARP States, accessed June 16, 2025, https://states.aarp.org/pennsylvania/staying-safe-online
202. The Importance of Regular Software Updates in Cybersecurity | Lucidum, accessed June 16, 2025, https://lucidum.io/blog/the-importance-of-regular-software-updates-in-cybersecurity/
203. Understanding the NIST cybersecurity framework - Federal Trade Commission, accessed June 16, 2025, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework