Topics/Content

Password security

Option 2:

To keep your online accounts safe, you must create and use strong passwords. Combining capital and lowercase letters, numbers, and symbols, a strong password should be at least 12–14 characters long and should not contain dictionary words or first names. It must be distinct and not duplicated between accounts. You can create and save secure passwords with Microsoft Edge. Never exchange passwords, use a password manager for several accounts, and turn on multi-factor authentication (MFA) for an additional degree of security. Keep passwords secure if you write them down or use hints. Watch out for phishing schemes; never give out passwords over the phone or by email and always double-check website URLs before entering login information. *(Microsoft, 2024)*

Option 3:

Strong credentials are crucial for safeguarding personal information since hackers can take advantage of weak passwords. Important extra insights consist of:

- Avoid Personal Information: Since hackers frequently start with easily discovered information, such as names, addresses, or birthdays, you should never utilise it.
- Length Is Important: Longer passwords (10+ characters) are much more secure, even if six characters is the minimum.
- Uniqueness Per Account: Using the same password for many accounts increases the danger since if one is compromised, others are at risk.
- Randomness Over Patterns: words from dictionaries or basic keyboard patterns (like "123abccba321") are straightforward to figure out. It's best to use randomness or a password generator.
- Mnemonic Devices: Make memory aids for complicated generated passwords (for example, linking "H=jNp2#" to a phrase such as "HARRY = jessica NORTH paris 2 #").
- Password managers: By securely storing passwords, programs like LastPass or Chrome's built-in manager remove the need to commit them to memory.

(*GCFGlobal.org, n.d.)*

Security Software

Option 2:

A proactive strategy for defending systems against vulnerabilities, data breaches, and cyberattacks is software security. It entails incorporating safeguards at every stage of the software development process to guarantee that systems are safe against cyberattacks. This is important since software is used in many different industries, and even one flaw can have disastrous results. By "shifting left," companies may implement security early and prevent expensive retrofits, resulting in more resilient systems. To put it briefly, software security aims to prevent issues in the first place rather than only address them. In a world that is becoming more digital, a well-secured system safeguards data, fosters trust, and guarantees dependability. *(IEEE Computer Society, n.d.)*

Option 3:

An organized method for reducing dangers in digital systems is software security. Software security guarantees that systems secure data and operate as intended—without unauthorized access or interruptions—much like a financial audit ensures that funds are handled appropriately. *(IEEE Computer Society, n.d.)*

What makes it so important?

- Confidentiality: Private information, such as financial or medical records, must remain confidential.
- Integrity: Malicious alteration of information is never acceptable.
- Availability: Even in the face of an attack, systems must continue to function.

Software security is ultimately about controlling risk before it becomes an emergency. In a time when digital safety is a must, companies who put it first not only protect their resources but also gain the trust of their people. *(IEEE Computer Society, n.d.)*

Update software

Option 2:

Consider software upgrades as the armor of your device; if you don't do them on a regular basis, cracks will form, and you'll be at risk of cyberattacks. Hackers are always looking for flaws in out-of-date software so they may install malware, steal data, or take over networks. Updates fix these flaws, strengthening your armor before combat like a blacksmith. *(University of Idaho, 2023)*

But there are other benefits besides security. Updates also:

But security isn’t the only perk. Updates also:

- Boost performance: Improve speed, add features, and fix errors to increase performance.
- Assure compatibility: Maintain the seamless operation of apps on various devices and software.
- Avoid scams: You may be tricked into installing malware by fake update pop-ups. Update via official settings only—never at random website prompts. *(University of Idaho, 2023)*

Option 3:

Software upgrades are essential for cybersecurity, not just best practice. They are required by institutions such as the University of Idaho because unpatched software is a major point of entry for cybercriminals. This is why updates are important:

1. Security Patches = Risk Reduction

As vulnerabilities are found, developers address them. Delaying updates exposes systems to network attacks, ransomware, and data breaches. For instance, a single unfixed bug in Office 365 or Zoom might reveal private university information.

2. Compliance Requirements

Patches must be implemented within 30 days, for example, and many institutions enforce update policies. Until they are upgraded, non-compliant devices risk losing their network connectivity.

3. Avoiding Fake Update Scams

To disseminate malware, cybercriminals imitate legitimate update notices. Red flags include strange download links, poor grammar, and pressure to take action right away.

(University of Idaho, 2023)

Phishing

Option 2:

Consider a professional scammer who poses as a tech support representative, bank teller, or even a coworker in order to fool you into giving them your wallet. Phishing operates similarly, whereby fraudsters impersonate reliable organizations (such as Microsoft, Amazon, or your bank) to obtain credit card information, passwords, or even take over your computer. *(Cisco, 2025)*

How the Scam Works:

1. The bait is an urgent SMS or email that says, "Your account has been locked! To repair it, click here.
2. The hook is that the link leads to a phony login page that appears authentic.
3. The Catch: The hacker gains access to your accounts as soon as you input your password.

(Cisco, 2025)

Why It’s So Dangerous:

- AI increases the fear of scams Phishing emails now resemble your boss's writing style and contain flawless language and personal information.
- A phishing link can transmit malware, lock company files (ransomware), or drain bank accounts with just one click.
- Hackers send thousands of emails to everyone in the hopes that a few may fall for it.

(Cisco, 2025)

Option 3:

Phishing is a type of cyberattack in which hackers pose as trustworthy organizations (banks, employers, IT businesses) in order to trick victims into downloading malware or disclosing personal information. It circumvents technical defenses by making use of human psychology, specifically trust, anxiety, and urgency. *(Cisco, 2025)*

Key Tactics:

- Spoofed Communication: Phishing emails and messages imitate legitimate companies, such as Microsoft and PayPal.
- Malicious Links & Attachments: These can install malware or reroute users to fake websites.
- "Update now or lose access!" is an example of a social engineering message that demands action.

(Cisco, 2025)

How to Spot & Stop Phishing:

- Verify the sender addresses to see if they are associated with @amazon.com or @amaz0n-support.ru.
- Hover before clicking: To view the actual URL on a desktop, move your cursor over links.
- Avoid clicking in a panic. Urgency is used by phishing ("Your account will be deleted!").
- Employ multi-factor authentication (MFA) to prevent hackers from logging in without your phone, even if they manage to steal your password.

(Cisco, 2025)

Practice safe browsing

Option 2:

Consider safe browsing to be similar to developing internet street smarts. Safe browsing teaches you how to use the internet without stumbling into cybercriminals' traps, much like you wouldn't give your wallet to a stranger or stroll down a dark alley at night.

Why It Matters:

- Although socializing, working, and banking all depend on the internet, hackers use it as a playground.
- There are threats everywhere: phishing emails, malicious downloads, fake websites, and even "harmless" cookies can steal your data or spy on you.

Your Safe Browsing Toolkit:

- Your Padlock = HTTPS A padlock icon and "https://" should always be visible in your browser bar before entering credit card numbers or passwords.
- Prior to clicking, consider your options. Untrustworthy links in pop-ups or emails? Avoid falling for the trick. To view the actual destination, hover over links.
- All software should be updated since outdated software is like an opened door. To prevent new dangers, keep your operating system, browser, and antivirus software patched.
- Antivirus = Your Personal Protector Although it's not infallible, it's an essential backup to detect spyware that you might unintentionally welcome in.

Option 3:

The user-facing aspect of cybersecurity is safe browsing, which consists of a collection of practices and resources that reduce vulnerability to online dangers such as malware, data theft, and scams. Networks are protected by firewalls and IT standards, but human behaviour is frequently the weakest link.

Because fraudsters frequently construct harmful sites that imitate legal ones, being vigilant about websites is the first step towards safe browsing. Modern browsers display padlock images for websites that support HTTPS, ensuring secure data transmission. Additionally, users should be on the lookout for typos, bad design, and misleading claims.

Because of phishing, a prevalent cyberthreat, email skepticism is essential. Attackers craft persuasive communications that compel users to open attachments or click links without question. Verifying sender addresses, evaluating links, and avoiding unexpected file downloads are all part of safe browsing.

In the end, safe browsing helps to close the gap between everyday behaviour and cybersecurity theory. It enables people to confidently traverse the digital world by converting intangible hazards into preventative measures. These guidelines provide a crucial foundation for security in a connected world, whether one is using them to check one's bank account, shop online, or just browse social media. People and organisations can significantly lower their exposure to the constantly changing range of online risks by making safe practices second nature.

Reference list

- Microsoft (2024). *Create and Use Strong Passwords*. [online] support.microsoft.com. Available at: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb. (Microsoft, 2024)
- GCFGlobal.org. (n.d.). *Tech Savvy Tips and Tricks: Password Tips*. [online] Available at: https://edu.gcfglobal.org/en/techsavvy/password-tips/1/. (GCFGlobal.org, n.d.)
- IEEE Computer Society (n.d.). *What is software security and why is it important?* [online] IEEE Computer Society. Available at: https://www.computer.org/resources/software-security.
- University of Idaho (2023). *Why Keeping Your Software Up to Date is Important for Cybersecurity*. [online] University of Idaho - Knowledge Base. Available at: https://support.uidaho.edu/TDClient/40/Portal/KB/ArticleDet?ID=2770.
- Cisco (2025). *The Future of Ransomware: inside Cisco Talos Threat Hunters*. [online] Cisco. Available at: https://www.cisco.com/site/us/en/learn/topics/security/what-is-phishing.html.
- Reasonlabs.com. (2023). *What is Safe Browsing? The Importance of Secure Browsing in Cybersecurity*. [online] Available at: https://cyberpedia.reasonlabs.com/EN/safe%20browsing.html.