Assignment -4

1. ***Web Browser Extensions: How risky are extensions & how can you choose safe ones?***

ANS:

An extension is a small piece of software you can install to customize your browser's appearance or function. Some extensions come from the makers of a browser, but more often, they come from third-party developers trying to add some new functionality that a browser doesn't already have.

Extensions can do almost anything. They might enable email encryption, ad blocking, one-click password storage, spell-checking, and more. Extensions are like specialized agents working with the flow of information through your browser. They might organize your notes, protect you from hackers, or just transform how that information appears in the browser window (e.g. dark mode).

But in order to function, extensions usually need broad-sweeping permissions over your browser. Some require access to almost everything your browser sees. Everything from the sites you visit, keystrokes, even your passwords. This means a bad extension (or a poorly secured browser) can expose you and your data, and introduce major privacy and security risks.

Security and privacy risks with browser extensions

Many browser extensions are safe, but there's always some degree of inherent risk. Installing an extension introduces new software to your browser—software which could potentially have security weaknesses (or be downright malicious).

Third-party extensions might secretly include malware, or have security flaws that hackers can exploit. And it's very common for attackers to "spoof" legitimate browser extensions, creating fraudulent versions to trick and defraud users (e.g. the numerous MetaMask fakes on the market).

There's even a risk in downloading from trusted channels like the Chrome Web Store—sometimes Google will accidentally remove the authentic version of an extension and leave a fake one behind. It's also possible for a legitimate extension to make it onto the Web Store, and then be sold to a different publisher who changes the code and introduces malware. And, with broad permissions over your browser, malicious extensions can cause all kinds of harm. For example, malicious extensions have been found to secretly use the browser to click on pay-per-click ads, collect user data, intercept messages from Gmail, and—most recently—hijack Facebook accounts using a fake ChatGPT extension.

The Brave browser: safe by default, safer for extensions

To use browser extensions safely, use them sparingly, and follow the best practices discussed in this article. But of course, the safest way to use extensions…is to not use them at all. Consider the purpose of the extension you're looking at, and see if there's a browser with that functionality out-of-the-box. For example, Brave has ad-blocking, a VPN, and even a crypto wallet, all built right into the browser. No extensions required.

And if you do need to use an extension, it's best to do so in a private browser that doesn't collect or store data about you. The more data that's sitting in your browser, the more an extension might have access to.

2. ***Securing Your Browser: Best methods & their trade-offs for a safer browsing experience***.

1. **Keep Your Web Browser Updated**

Popular web browsers like Microsoft Edge, Mozilla Firefox, Apple's Safari, or Google Chrome receive updates on a regular basis to fix bugs, add new functionality, and, most importantly, patch security vulnerabilities.

2. **Use as Few Extensions as Possible**

Every now and then, a large number of users become compromised after installing a malicious web browser extension.

In 2020, for instance, security firm Avast discovered 28 extensions that contained code capable of performing several malicious operations. These extensions were installed by over three million users, exposing them to threats such as phishing, malware, and data theft.

As useful as web browser extensions are, you should install as few of them as possible because any developer can become compromised. If multiple extensions that do the same thing are available, always pick the one that has been around for a while and has received many positive reviews.

3. **Enable HTTPS-Only Mode**

HTTPS (Hypertext Transfer Protocol Secure) is a web protocol used for secure communication over a computer network, typically the internet.

Virtually all reputable websites these days use HTTPS to encrypt data in transit, and major web browsers make it possible to enable HTTPS-only mode to help users avoid unsecured sites.

4. **Install a Reliable Adblocker**

If there's one web browser extension that you should definitely install, it's an adblocker like uBlock Origin, which is available for Chrome, Chromium, Edge, Firefox, Opera, and Pale Moon.

Adblockers are the most controversial web browser extensions because many people install them to disable ads on websites to enjoy a more comfortable reading or viewing experience.

However, adblockers don't block only legitimate ads that websites use to earn money. They also block malicious ads, various annoyances, privacy threats, trackers, and more.

The best adblockers let you customize exactly what you want to block, so it's up to you to decide which websites you want to support by allowing ads to be displayed on them.

5. **Block Pop-Up Windows**

Pop-up windows are not only annoying, but they're also very dangerous because they often lead to malicious websites and are designed to appear right under the mouse cursor.

Luckily for you, popular web browsers can block pop-ups without a third-party extension:

6. **Delete Unwanted Cookies**

Cookies are small blocks of data where websites save information about each user's session to offer personalized experiences. Some websites also use a special type of cookie, called tracking cookie, to track users' web browsing habits.

To prevent cookies from tracking you and compromising your privacy, you should delete all cookies except for those that are associated with websites you regularly visit and trust. An extension like Click & Clean makes this easy, but all major web browsers come with a cookie manager, so you don't really need a third-party extension.

7**. Use a Password Manager Extension**

In recent years, all popular web browsers have gained password management capabilities, allowing their users to securely save commonly used passwords for faster authentication.

As useful as native password management capabilities can be, they pale in comparison with password manager extensions like Bitwarden, LastPass, or 1Password.

These and other similar extensions make it easy to access saved passwords across all devices and platforms, and they offer superior password protection thanks to

8. **Disable the Autofill Feature**

The purpose of the Autofill feature is to make your life easier by automatically populating form fields with previously-entered information, such as addresses, passwords, and credit card data.

While useful, the Autofill feature is a double-edged sword because it makes it way too easy to fill in sensitive information in a form created by a cybercriminal. What's more, the saved information can be retrieved by anyone with access to your computer.

9. **Take Advantage of Private Browsing**

Private browsing, also known as incognito mode, is a misunderstood feature because many people believe that its purpose is to hide their online activity. That's not the case at all, however.

Instead, private browsing deletes all information about your browsing session, including your history, downloads, and cookies, when you close the private window. Some web browsers also enforce strict tracking prevention when private browsing is enabled.

10. **Use a Virtual Private Network (VPN)**

When you use your web browser to visit a website, your activity is visible to your internet service provider, the person responsible for the local network you're connected to, and, if the network is unsecured, potentially even malicious strangers.

To prevent all these third parties from seeing what you do online, you should tunnel your web browser traffic through a virtual private network, an encrypted web browsing connection that enables data to be securely transferred over the public internet.

3. ***Two-Step Authentication: Compare methods, strengths, weaknesses & choose the right one.***

ANS:

Two-factor authentication (2FA), sometimes referred to as *two-step verification* or *dual-factor authentication*, is a security process in which users provide two different authentication factors to verify themselves.

2FA is implemented to better protect both a user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically, a password or passcode. Two-factor authentication methods rely on a user providing a password as the first factor and a second, different factor -- usually either a security token or a biometric factor, such as a fingerprint or facial scan.

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

Two-factor authentication has long been used to control access to sensitive systems and data. Online service providers are increasingly using 2FA to protect their users' credentials from being used by hackers who stole a password database or used phishing campaigns to obtain user passwords.

here are several ways in which someone can be authenticated using more than one authentication method. Currently, most authentication methods rely on knowledge factors, such as a traditional password, while two-factor authentication methods add either a possession factor or an inherence factor.

Authentication factors, listed in approximate order of adoption for computing, include the following:

- A **knowledge factor** is something the user knows, such as a password, a personal identification number (PIN) or some other type of shared secret.
- A **possession factor** is something the user has, such as an ID card, a security token, a cellphone, a mobile device or a smartphone app, to approve authentication requests.
- A **biometric factor**, also known as an **inherence factor**, is something inherent in the user's physical self. These may be personal attributes mapped from physical characteristics, such as fingerprints authenticated through a fingerprint reader. Other commonly used inherence factors include facial and voice recognition or behavioral biometrics, such as keystroke dynamics, gait or speech patterns.
- A **location factor** is usually denoted by the location from which an authentication attempt is being made. This can be enforced by limiting authentication attempts to specific devices in a particular location or by tracking the geographic source of an authentication attempt based on the source Internet Protocol address or some other geolocation information, such as Global Positioning System (GPS) data, derived from the user's mobile phone or other device.
- A **time factor** restricts user authentication to a specific time window in which logging on is permitted and restricts access to the system outside of that window.

The vast majority of two-factor authentication methods rely on the first three authentication factors, though systems requiring greater security may use them to implement multifactor authentication (MFA), which can rely on two or more independent credentials for more secure authentication.

4. *Strong Passwords: What makes them weak, how attackers exploit them & how to create secure, memorable ones.*

ANS:

What is a strong password?

A strong password is one you can't guess or crack using a brute force attack. Progress in the technological sphere leads to improvements in malicious hacker's arsenals, too. Therefore, strong passwords consist of a combination of uppercase and lowercase letters, numbers, and special symbols, such as punctuation. They should be at least 12 characters long or even lengthier.

Here are the main characteristics of a secure and strong password:

- At least 12 characters long or more
- Combination of uppercase and lowercase letters, numbers, and symbols
- Not a familiar name, person, character, or product
- Is not based on your personal information
- Passwords are unique for each account you have
- Significantly different from your previously used passwords

How to Create a Strong Password
MAKE IT LONG

- Use a Minimum of at Least 10-Characters: CMU requires all users to have a minimum password of at least 8-characters, however when did CMU ever settle for the bare minimum? The longer the password the more secure it becomes.

ADD VARIETY

- Include Numbers, Symbols, Capital and Lower-Case Letters: The more you mix up letters, numbers, and symbols, the more potent your password becomes making it harder for a brute force attack to crack it.
- Add Emoticons: While some websites limit the types of symbols you can use, most allow a wide range. Make your symbols memorable by turning them into smiley faces to instantly boost your password strength.

MAKE IT UNIQUE

- Don't use Personal Information: Be sure your passwords do not contain any personal information that can be publically accessible such as your birth date, pet's name, car model, phone number, or street name and address.
- Don't use Dictionary Words: Any word on its own is bad. Any combination of a few words, especially if they grammatically go together isn't great either. For example "mouse" is a terrible password. "small brown mouse" is also very bad.
- Avoid Common Substitutions: Password crackers are familiar with the usual substitutions. "M0use" isn't strong just because the o was replaced with a 0.

How to Secure a Strong Password :

- **Don't Reuse it:** Having various passwords makes it harder for a cybercriminal to compromise your accounts. In the case that someone got a hold of your passwords, you can rest assured your other accounts are safe. Using a password manager will help you generate new unique passwords for each site you visit.
- **Use Two-Factor Authentication:** Two-factor authentication adds another layer of defense for your information. This technology enables you to provide multiple pieces of information as authentication, in any combination of:
  - Something you know-Your Password
  - Something you have- One-Time-Passcode or Generated Key
  - Something you are: Your Fingerprint, Voice, or Iris

  - **Don't Share it:** Someone who has your password can impersonate you, change or delete your financial information, make purchases as you, or damage your reputation. The results are lost time, money, and embarrassment.
  - **Secure your Security Questions:** Beware of the "security questions" that websites use to confirm your identity. Honest answers to these questions are

often publicly discoverable facts that a determined adversary can easily find and use to bypass your password entirely. Instead, give fictional answers that no one knows but you.

- **Don't Store it Online:** If you were to lose your laptop or have it stolen, the bad actor would have easy access to your accounts. Instead, use a password manager to store your passwords.

5. ***POS Security Threats: Identify vulnerabilities & suggest solutions for malware, breaches & theft.***

   ANS:

4 POS System Security Risks (POINT OF SALE)

1.Network and Software Weaknesses

The most common POS problems come from a network that isn't secure. Hackers can infiltrate these weak setups and steal valuable information, such as customer credit card numbers and business account data. Your POS technology should be kept on a separate, password-protected network if possible. Additionally, you should change passwords at least once every 90 days to reduce the chance of infiltration.

Keeping your software up-to-date is vital too. Software companies are always releasing patches and improvements for their operating systems. Staying current means having access to the latest security measures, giving you the peace of mind you need.

2.Device Faults

Even if the network is protected, your devices need to be secure too. Guarding your computers and tablets with passcodes is a fantastic first step. Train employees to always log out of your POS system when stepping away from it, and to never share passwords or other information. Choose technology products that have inherent security measures. For example, Apple's iPads won't compromise other apps if one program is infiltrated.

3.Phishing

Phishing is a relatively new hacking technique, where hackers trick employees into opening malicious links through email. After clicking a link, hackers can gain access to both your system and data. To prevent this, train employees never to open any out-of-the-ordinary emails or links that get sent to them. Install a good antivirus system that can automatically block these types of malware. Avoid this problem altogether by training and monitoring employees on their POS device

usage, so that they are never checking their personal email or browsing the web on company-owned devices.

4.Skimming

Everyone has heard about credit card skimmers placed on gas pumps, and unfortunately retail is becoming a target for skimming as well. These small devices are discretely attached to POS system hardware to collect and access customer credit card information and compromise it. Even though skimmers aren't prominent at many types of retailers, it's perfectly possible and should be on your radar. Thieves can slide on a device in just seconds, so it's important to check your hardware routinely for anything suspicious—and to contact authorities if you find anything.

Network and Software Vulnerabilities

An unsecured network causes the most common POS problems. Hackers can infiltrate these weak installations and steal valuable information such as customer credit card numbers and business account data. If possible, your POS technology should be kept on a separate, password-protected network. It's also a good idea to change passwords at least once every 90 days to avoid data leaks.

It's also critical to keep your software up to date. Software companies release patches and improvements for their operating systems all the time. Using up-to-date software means having access to the latest security measures and giving you the peace of mind you need.

Business interruptions due to inadequate point-of-sale applications

Retailers not only want business and customer data to be kept secure but also expect their point-of-sale applications to be free from disruption to their business due to cyber attacks or technical downtime.

Retailers want to run point-of-sale applications securely and prevent attacks before they happen. For this to happen, the ideal point-of-sale application must have

reliable security monitoring and incident response services, as well as powerful POS security technology.

The security monitoring and incident response service should alert IT staff, whether in-house or outsourced, when a breach occurs, monitor POS application-related activities, detect and flag threats, and provide real-time responses to any issues.

As they manage countless data transactions through point-of-sale applications, POS providers may comfort their retail customers and give them peace of mind by using a dependable POS security monitoring and incident response solution.

4 Ways to Prevent a Data Breach

1. Vulnerability Assessments

Organizations should regularly assess their systems to identify vulnerabilities and associated risks. These assessments help determine if the established security policies require updates, strengthening the overall security strategy.

2. Implementing Least Privilege

When implementing an Identity and Access Management (IAM) system, organizations should apply the principle of least privilege to ensure that each user only has the necessary access permissions. Maintaining least privilege access can be complicated, especially if the organization has many users with constantly changing roles. However, this security control is essential for ensuring that malicious actors (internal or external) cannot access sensitive data.

3. Data Backup and Recovery

Organizations should regularly back up their data and establish a recovery plan to restore their data after a breach. A backup and recovery plan helps ensure a faster response to minimize damage and prevent downtime. Administrators should regularly review the risk management, backup, and recovery policies to prevent attackers or ransomware from accessing backup data.

4. Penetration Testing

Penetration tests are simulated attacks that allow ethical hackers to identify vulnerabilities in computer systems, networks, or applications. Organizations may use third-party or in-house penetration testers to mimic an attacker's techniques and determine how easily they can hack the system.

Penetration tests are also useful for evaluating compliance with security regulations. Organizations use regular pentesting to identify vulnerabilities proactively before an attacker can exploit them.

----------00000----------