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

Modern Web browsers make it easy to access websites, search the Web, and do just about everything online. But by default, browsers might not have all the functionality you want. In these cases, many people will customize by installing a browser extension.

An extension is basically a piece of software that adds some custom function to your core browser. They can help you take notes, manage passwords, block ads, and more. But extensions can also introduce security risks.

At essence, Web browsers process information. Uploads from your computer, downloads from the Web, visiting websites…all this happens in your browser, with information constantly sent back and forth. Browser extensions modify this basic flow of information in some way.

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.

A guide to safely using browser extensions

Many extensions are safe and reputable, you just have to be careful when installing and using them. This guide covers the most important considerations when using extensions.

Check the source of an extension before you install

To validate the safety of any extension, start with a few quick checks:

Is it made by a reputable source?

Are you downloading from an “official” place like the Chrome Web Store?

When you search for the extension, do you find look-alike or “clone” versions? Are you sure you’re installing the right one?

Does the extension have lots of downloads and positive reviews? (Beware of a string of 5-star reviews, identical comments, or comments all published on the same date.)

Are there third-party reviews (e.g. in tech blogs) that vouch for the extension?

Does the extension have a privacy policy? Does that policy make sense?

Check the extension’s permissions—what does the extension have permissions to in your browser, and why?

By installing an extension, you’ll likely be enabling it to access any personal data that passes through your browser. So it’s best to know it comes from a reputable source and it has some social proof or third-party vetting. The questions above will help you determine the extension’s safety.

Stick with extensions from official sources

The Chrome Web Store is a useful resource to search for new Chrome extensions. But note that you can use those extensions for any browser that relies on Chromium, the open-source language that underpins the Chrome browser.

For example, the Brave browser will work with any Chrome browser extension since they share the Chromium code. There are other places to find extensions, including downloading them directly from the publisher’s website, but if you’re running a Chromium-based browser, the Chrome Web Store should be the first place you look.

Don’t overload your browser with extensions

Every extension you install adds a security risk and a performance burden to your browser. If you’ve got 15 extensions installed—and running—you’ll likely see a slowdown in browsing and even device processing speeds. Everything will just move slower, or your computer’s fan might even turn on more.

Know what extensions you have installed

It’s best practice to monitor the extensions you’ve installed, and which are still actively running in your browser or on your device. Then if you hear about a risky extension or a possible data leak, you know to take action.

Delete unused extensions

Finally, you should delete any extension you’re not regularly using. If it’s not in daily or weekly use, it’s probably not worth keeping on your browser. When you look at your list of installed extensions, you might find more there than you thought. If you’re unsure how an extension got installed or where it came from, delete it.

Extension compatibility across browsers and devices

Depending on your device and browser type, you'll have different extensions available, and different official resources to download from.

Firefox and Safari use fundamentally different source codes from Chrome and Brave (which both rely on the open-source Chromium codebase). This means that an extension for Firefox will require a separate version to work for Safari, or for Brave and Chrome. Both Brave and Chrome, however, are compatible with extensions found on the Chrome Web Store.

Extension compatibility on mobile devices

Mobile browsers generally offer three approaches to extensions:

Some don't allow extensions

Some are only compatible with native extensions from the browser maker

Some allow for third-party extensions

The desktop version of Chrome, for example, supports thousands of extensions, but the mobile version of Chrome supports none. Other mobile browsers like Opera offer only native extensions, which are built by the publisher and managed by the user. Safari on iOS enables users to download third-party extensions through Apple's App Store.

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.

Your browser is one of the easiest ways for malware to penetrate your network. Here are 10 ways to practice safe surfing in Google Chrome, Microsoft Edge, and Mozilla Firefox.

The web browser is an old piece of software, with lineages tracing back to the 1990s. It's your portal to the cloud, your interface with Salesforce, AWS, Azure and countless other cloud services.

It's also one of the most insecure apps you will ever use, with a whole manner of malicious attacks targeting the browser since Microsoft, Apple and various Linux vendors have effectively secured their respective operating systems.

Web browsers are not set up in the most secure means with the default configuration. They tend to be configured for maximum performance, and the performance and security don't always go together. This is true of both preloaded browsers with the computer and ones you may download.

Here are some setting suggestions, including how to enable or disable them in the three major browsers (Microsoft Edge, Google Chrome and Mozilla Firefox).

1. Get security browser extensions

We're going to start off contradicting ourselves, as suggestions #1 and #2 directly contradict each other. The call is yours to make. Browser extensions or add-ons are small plug-in applications to add functionality to your browser. All three have hundreds if not thousands of extensions for a variety of actions.

Among them are security and privacy extensions to protect your online privacy and security. They range from blocking access to known malicious websites to enabling HTTPS for everything to blocking cookies and IP addresses.

The Electronic Frontier Foundation (EFF), a nonprofit organization dedicated to protecting privacy and security recommends HTTPs Everywhere, in part because it created it. HTTPs Everywhere lives up to its name by forcing the browser to use HTTPS instead of the default, unsecured HTTP.

The EFF also makes Privacy Badger, which learns about and blocks secret trackers that track you across the web and even on different devices as you use your browser. It can be set to block all trackers, including cookies. Finally, the EFF makes and promotes uBlock Origin, an ad and tracking blocker. It stops ads on a page from loading so it makes the browser faster.

One last extension to consider is LastPass Password Manager, a password manager that lets you store all your passwords safely and gives you secure access from every computer and mobile device.

To access the plugins/extensions library of your browser:

- **In Chrome** – Select the Menu from the upper right (three dots), go down to the More Tools sub menu and select Extensions.
- **In Firefox** – Select the Menu from the upper right (three lines) and go down to Add-ons. You will be connected to the extension store.
- **In Edge** – Select the Menu from the upper right (three dots), go down to the Extensions option. You will see a link that says "Get extensions from Microsoft Store."

2. Disable extensions

Herein lies the contrarian advice. While many extensions come from reputable companies or developers and perform a useful function, some are written by unscrupulous developers and are designed to spy on you or outright hijack your web browser.

Google recently removed dozens of extensions from its stores involved in information theft. An extension can also be exploited by malware, and not just a poorly written one. JavaScript has many legitimate uses but a whole lot of exploits, too.

Universal banning of extensions isn't feasible. Some of your users will need extensions and there are plenty of good ones – there are more than 25 for Salesforce alone. But if you have some users who need maximum protection, a total ban is possible.

- **In Chrome** – Right click the icon, go to properties section and add --disable-extensions to the Target window.
- **In Firefox** – Like Chrome, add -safe-mode at the end of the link in the Target window. This disables everything.

- **In Edge** – Like Chrome, add –extoff to the Target window

3. Disable saved passwords

All of the web browsers offer some kind of built-in password manager to save your usernames and passwords. Given how many accounts we all have it's an obvious feature, but it also represents a danger, especially if the laptop is lost or stolen. Stored credentials on your PC can be stolen by malicious software because login/password information is not that well protected. That's why there are so many password managers out there.

- **In Chrome** – Open settings, select Passwords, and uncheck Offer to Save Passwords and Auto Sign-in.
- **In Firefox** -- Click the Menu button, then select Preferences. Select Privacy & Security on the left pane. Scroll down to Logins and Passwords and select the Saved Logins button.
- **In Edge** -- In Microsoft Edge, select Settings and select Passwords & Autofill, then use the toggle to turn off all three functions.

4. Use a strong antivirus

This should be obvious -- but all too often it isn't. The top antivirus products out there not only have a constantly updated database of known malware but also a database of known dangerous or malicious sites that try to inject malware into visitor's computers, and they will stop the page from even loading. Browser protection should be a mandatory checkmark for evaluating an antivirus product.

5. Disable autofill

Autofill is a feature that automatically fills out forms on web pages with your previously saved user information. It detects common fields like name, email address, physical address, and phone number. While it is convenient and time-saving to autofill all of your contact info without having to retype it there are very real risks. One developer has even published a simple phishing example on GitHub to show how easily your personal information can be exploited.

In Chrome -- Click Menu, then Settings, and select Autofill. Go into the Addresses and More section and toggle the setting to off.

In Firefox – Click Menu, Options, then Privacy & Security. Uncheck the box Forms and Autofill.

In Edge – Click Menu, Settings, and Profiles, then select Addresses and more. Turn it off from there.

6. Use a sandbox

A sandbox is an application that blocks software applications from accessing the hard disk. The entire app only exists in the memory space occupied by the sandbox and when the sandbox is closed, the app is wiped from memory without ever touching the disk. Some of these tools are simply virtual machines but they have the same effect of blocking disk writes.

Microsoft introduced a simple app called Windows Sandbox with the Windows 10 May 2019 Update but only for Windows 10 Pro or Enterprise. The Home edition does not have it. You enable it by going into Windows Features in the Control Panel and checking the box next to the name, then reboot. As a security measure, Windows Sandbox does not carry over any of the personalized features like favorites and themes, by design.

You have several choices for sandboxing/virtualization software.

- VirtualBox
- Sandboxie
- QEMU
- VMware Workstation Pro
- Parallels Desktop

7. Manage browser cookies

Browser cookies are a small piece of data a website stores on your web browser when you visit that website so it can remember you and your interactions. Cookies by themselves are not bad but can become a problem if you get infected with malware and the malware steals cookie information.

Cookie tracking can be reduced but not completely prevented. And because some websites need it to function properly, you may not and should not disable it entirely. But if you want to disable cookies completely:

- **In Chrome** – Click Menu, then Settings, then Advanced at the bottom of the page. Under "Privacy and security," click Site settings, then Cookies. Next to "Blocked," turn on the switch.
- **In Firefox** -- Go to Tools in the menu bar and click Options. In Options, under Enhanced Tracking Protection, select Custom, and in the Cookies pulldown menu you can block all cookies.
- **In Edge** -- Click on Menu, then Settings, then Site Permissions. Select off for “Allow sites to save and read cookie data” and turn on “Block third-party cookies.”

You also have the option of deleting certain cookies or blocking specific sites from these Option windows.

8. Update your browser. Or don’t

Browsers makers are always pushing out updates, but to make sure you get it, you should do a manual check. In all three browsers, go into their Menu and select Help or About. That forces a version check and then asks for a restart.

Caveat emptor: A browser update is usually an upgrade that comes with new/improved features, bug fixes and security patches. But the two most recent Firefox upgrades (versions 74 and 75) have been awful, introducing serious bugs and breaking features that previously worked. So it can’t hurt to wait before upgrading to see if there are problems.

9. Use a 64-bit web browser

64-bit programs have greater inherent protection against malware attacks because of something called address space layout randomization (ASLR). ASLR is a memory-protection process to protect against buffer-overflow attacks by randomizing the memory location where system executables are loaded into memory.

All three browsers now default to the 64-bit version, but it can’t hurt to double check. Go into the Menu and select Help or About, and the version number and 32/64-bit info will be displayed.

10. Consider alternatives to the big three

When you think browser, the automatic responses that come to mind are Chrome, Edge, Firefox and Safari for Mac users. But there are many more, owing to open-source browser engines.

The Brave browser is built on top of Chromium (an open-source version of the Chrome browser), but does none of the online activity collection Google engages in. And rather than rely on third-party privacy extensions, it does its own blocking of third-party and advertising cookies and uses HTTPS for all connections.

The Tor browser was designed to provide secure access to the Tor anonymity network and as such is heavily aimed at privacy and security. It is based on Firefox but with additional security features, such as built in HTTPS Everywhere and NoScript (which disables all scripts by default) plugins, it blocks other browser plugins such as Flash, RealPlayer and QuickTime and is always in private browsing mode, so it has tracking protection, no browsing history, no saved passwords, no search history, and no cookies or cached web content.

The Vivaldi browser is derived from the Chromium open-source project, but one key feature is it removes all of Google's usage tracking. It makes its money through other means than ad tracking. It has seamless syncing between the desktop and mobile versions, has an integrated notes app for writing down research as you are browsing, and in one of its most unique features, it lets you screenshot an entire webpage on a smaller screen, even if the contents of the page scroll down off screen.

The Opera browser made its name for being lightweight and easy on resources, but it also has a built-in ad blocker, uses Chrome extensions, has a battery saver mode for laptops that can reduce battery use by up to 50%, and has a built-in VPN, something the competition does not do.

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

Three main security protocols and their differences: Single Sign-On (SSO), Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA).

In today's world, security is of utmost importance. We want to protect our data, our accounts and our identities from malicious attackers. The three main protocols that you may come across when dealing with security are Single Sign-On (SSO), Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA).

While they share many similarities, each protocol serves a different purpose and has its own unique features. Understanding the difference between SSO, 2FA and MFA is essential for anyone looking to stay safe online. In this article, we will discuss the differences between these three protocols, how they work and why they are important for keeping your data secure.

Single Sign-On (SSO)

Single Sign-On (SSO) is an authentication process that allows users to access multiple applications or websites with one set of credentials. SSO creates a single, secure login portal for users to access all their applications, eliminating the need to remember multiple usernames and passwords.

One of the most popular examples of SSO is Google. Once you log in to Google, you can access multiple services like Gmail, YouTube, Maps, etc.

Key Points of SSO

- Requires only one set of credentials for authentication
- Allows for authentication across multiple applications and servers
- Usually requires a third-party authentication provider

- Credentials are securely stored in a centralized database
- Can be used to control access to multiple systems and applications

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) adds an additional layer of security to the authentication process by requiring users to input more than one type of authentication credential. Common types of 2FA include one-time passwords (OTPs), biometric authentication or hardware tokens.

Key Points of 2FA

- Requires two different forms of authentication such as knowledge-based (e.g., username/password) and something you have (e.g., a token or code sent via SMS)
- Provides an additional layer of security

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is an authentication process that requires users to provide two or more pieces of evidence to prove their identity. MFA combines two or more authentication methods, such as passwords, OTPs, biometrics, hardware tokens or other types of authentication. It is more secure than single-factor authentication because it makes it more difficult for a malicious actor to gain access to a user's account.

Key Points of MFA

- Requires two or more forms of authentication, such as a knowledge-based factor, something you have or something you are
- Provides an extra layer of security and is more secure than 2FA
- Can be used to protect accounts and data from unauthorized access
- Can help protect against phishing and other malicious attacks
- Can be used to control access to multiple systems and applications

SSO vs. 2FA vs. MFA

The three main security protocols have quirks, just like any technology. While they all aim to protect your data, data breaches and identity, they each have their own strengths and weaknesses. It's important to understand these differences in order to make informed decisions when it comes to protecting your data.

- **SSO –** This is the most commonly used authentication protocol. It's easy to use, convenient and saves time. It also helps create a unified digital experience by sending the same information to your device and server.

- **2FA –** This type of authentication is more secure than OTPs since it requires two different factors. Further, 2FA is generally more difficult to hack than 1FA, since it requires more than one method of authentication.

- **MFA** — This is similar to 2FA, but it uses more than one method to verify your identity. This can include a combination of different devices and technologies, such as a mobile app, a separate email address and a hardware key.

Cost

The cost of implementing SSO, 2FA and MFA will depend on the size and complexity of the organization. Generally, a small business can expect to pay anywhere from a few hundred to a few thousand dollars for the setup and maintenance of these security systems.

For larger organizations, the costs can increase significantly, especially if multiple systems need to be integrated or if custom solutions are required. Additionally, ongoing costs for the maintenance and support of these systems may need to be taken into consideration.

User Experience

The user experience of single sign-on (SSO), two-factor authentication (2FA) and multi-factor authentication (MFA) is a much smoother and more secure experience for users. SSO allows users to log in to multiple sites and applications with just one set of credentials. This makes logging in much easier and more secure than having a separate username and password for each site.

2FA and MFA add an extra layer of security by requiring users to authenticate using a second or multiple factors such as a one-time code sent via SMS or email, or biometric authentication. This additional security helps protect users from unauthorized access to their accounts, while still allowing them to conveniently access their accounts with minimal effort.

Implications for Businesses

SSO (Single Sign On), 2FA (Two-Factor Authentication) and MFA (Multi-Factor Authentication) are essential security measures for businesses to protect their data from unauthorized access. SSO simplifies the process of logging into multiple accounts or platforms with just one set of credentials, making it easier for employees to access the resources they need.

2FA and MFA provide an additional layer of security, ensuring that only authorized users have access to the data. The implications for businesses of these security measures are that they can provide a secure environment for their employees while also reducing the risk of data theft or data breaches. Additionally, the increased security can provide customers with confidence that their data is safe and secure.

Overall, SSO, 2FA and MFA all offer varying levels of security for online services and data. SSO is the simplest of the three, providing single sign-on access to multiple services with one set of credentials. 2FA requires a second form of authentication, usually in the form of a one-time code or biometric scan.

Finally, MFA requires multiple layers of authentication, allowing for the most secure and reliable authentication. All three technologies can be used together to create an even more secure authentication system.

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

Create, Remember, and Secure a Strong Password

Passwords have become a big part of our lives in the digital age. We use them so often that it is easy to overlook the importance of creating a strong one. Almost every bit of private information about us is stored behind a password. If that password were to fall into the wrong hands, it could

jeopardize our personal and financial livelihood. This article will provide helpful tips on how to create and remember a strong password—and more importantly, how to keep it secure.

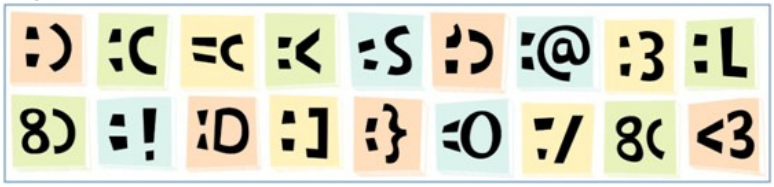
Create a Strong Password

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.

Remember a Strong Password

The secret to creating a hard-to-crack password that's unique and easy to remember is to focus on making it memorable and making it hard to guess. By learning a few simple skills, you can easily create a strong and memorable password with minimal effort. Plus, creating them can actually be fun - and your payoff in increased safety is huge.

USE A BIZARRE PASSPHRASE WITH SYMBOLS AND NUMBERS

Creating an an odd passphrase of words that typically don't go together is a good way to create the base of a long password. Some sites will even allow spaces. Add symbols and numbers to make it even stronger.

Example: 32 Seagulls deliver bologna sandwiches to Paris

Example: 32-Seagullsdeliver bologna5andwiches2Paris!

USE A PHRASE AND INCORPORATE SHORTCUTS OR ACRONYMS

Use phrases that mean something to you and shorten them by using shortcuts; or use the first digit in each word to create an acronym and add numbers and symbols throughout.

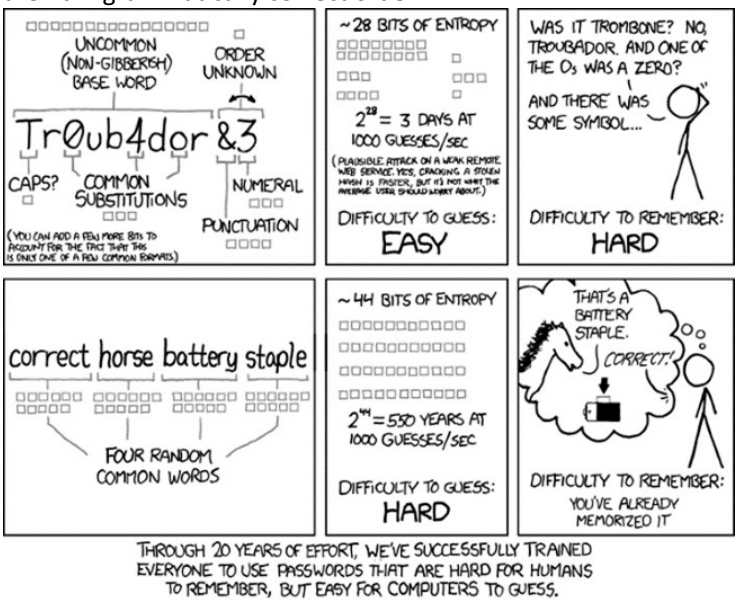
Shortcut Example: 2BorNot2B_ThatisThe? (To be or not to be, that is the question-Shakespeare)

Acronym Example: I go bowling every Friday night with 8 friends becomes **1gbeFnw8f:)**

USE RANDOM WORDS TO CREATE A PASSPHRASE

This method does not follow the traditional password advice of not using dictionary words. Instead, use four or five random words and string them together to create a passphrase that involves multiple words. The randomness of the word choice and length of the passphrase are what makes it strong.

The most important thing to remember is that the words need to be random. For example, "cat in the hat" would be a terrible combination because it is such a comon phrase and the words make sense together. But, something like "correct horse battery staple" doesn't make sense and the words aren't in grammatically correct order.



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

CMU has a free Two-Factor Authentication through DUO Security.

- ***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.

Password Manager

- Password managers are the ultimate solution for generating and storing passwords for multiple websites. Password managers can generate and store strong, unique passwords for each of your accounts. The password data is then encrypted and stored in the cloud or on your device meaning you do not need to memorize them.
- The only thing you need to remember is your login details for the password manager app. For more information on which password manager is best for you, check out the descriptions of approved Password Managers.

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

Point-of-Sale (PoS) systems are rapidly becoming the technology of choice for retail businesses as an all-in-one solution. Be it inventory information, stock handling, sharing customer data across stores, or managing business expenses, PoS systems have proven to be effective in providing a robust digital database for the retail sector. PoS systems have gained preference over cash for their ease of use, greater accuracy, detailed receipts, and error-free checkouts. However, the rapid growth of PoS transactions across the retail industry also raises some security concerns.

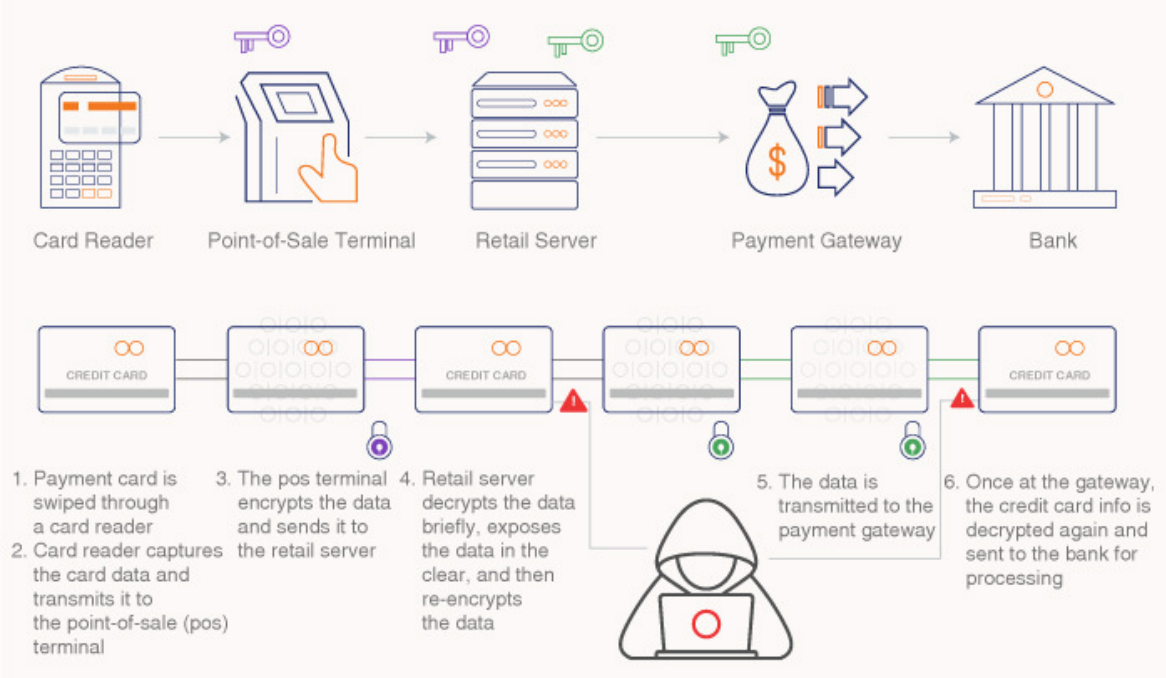
How Safe is the Payment Process over PoS?

According to the recent statistics, there are multiple attacks on PoS systems every minute in retail outlets, restaurants, and hospitality industries. With more technologies being used to process sales, there is a significant rise in threats like cyber-attacks and data thefts. Reported data breaches are growing drastically every year. However, several fraud detection breakthroughs in technologies have reduced the risks involved in using cards over PoS terminals.

What actually happens when you use your card to pay at a restaurant or supermarket?

When your card is swiped at the card reader, it captures the card data and transfers the information to the PoS terminal. The PoS terminal then encrypts the data and sends it to the retail server. The retail server decrypts the data, briefly exposing it, and further re-encrypts it to transmit to the payment gateway. Once at the gateway, the card information is re-decrypted and sent to the bank for processing.

Through the entire payment process, data is exposed several times, thereby making it vulnerable to cyber-crimes like hacking.



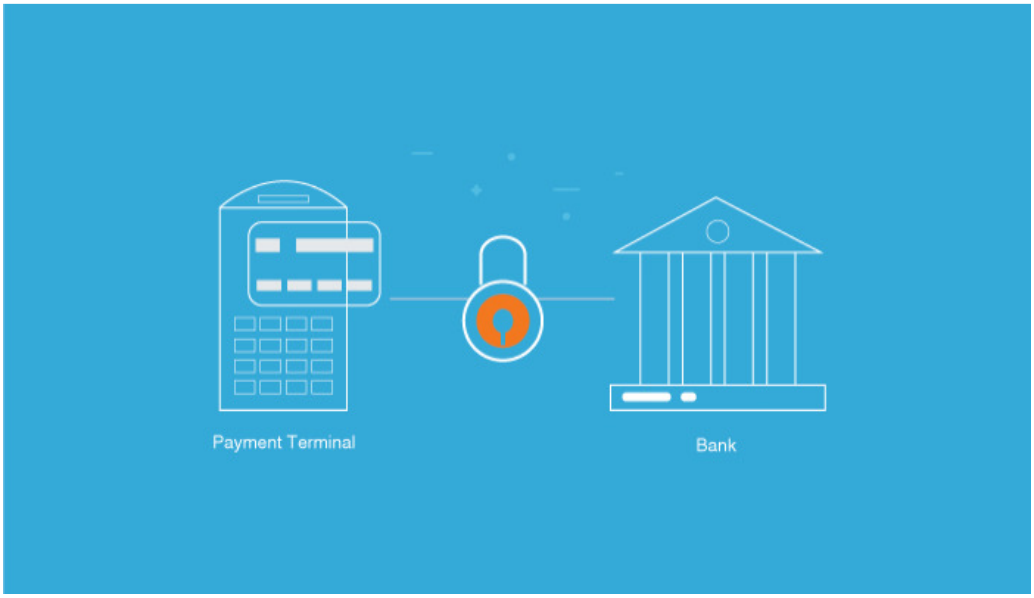
Hackers usually get credit card information by installing automated malware. This malware infiltrates networks, systems, and workstations, looking for unencrypted cardholder data. This data is, then, sold on the dark web.

So how can customers safeguard information?

Point-to-Point Encryption (P2PE) is regarded as one of the most standard payment security solutions, which instantly converts the confidential payment card data into indecipherable code, the moment the card is swiped at any PoS terminal. P2PE solutions minimize fraud and the potential invasion of malicious activities like hacking.

Encryption does not itself prevent interference, but denies access of the intelligible content to a would-be interceptor. Using encryption for card payments alters the payment card data into an indecipherable format and renders it unusable by hackers and cyberpunks, as they have no means to invert the data back to its original form. The PCI-validated P2PE solutions provide not only P2P encryption, but also validated hardware, software, and solution provider processes and environment. Hence, one of the most secure ways to safeguard the valuable cardholder data in PoS systems is the PCI (Payment Card Industry) validated P2PE solutions.

Let's look at how the P2PE works in a PoS system.



When you swipe your card on a P2PE secure PoS system, the devices or readers used are already integrated and PCI-compliant, which means they all have a key in them even before the merchant can see it. When the card information is swiped through these peripherals, it is encrypted immediately. Therefore, P2PE protects payment card data from the point of capture until the secure decryption endpoint. The card information remains in the encrypted form as it is transmitted to the point of sale terminal, then to the retail server, and further to the payment gateway. This one-time key is highly secure and is destroyed after every use. The decryption keys are stored in a Hardware Security Module (HSM) at the payment gateway. Once the data is decrypted at the payment gateway, it is sent to the acquirer for approval

we'll look at the four most common point-of-sale security issues.

1. Unauthorized access to point-of-sale application

Fraudsters exploit mobile point-of-sale apps to steal personal and sensitive information such as credit or debit card information. They then use these to make fraudulent purchases, which results in both financial losses and damaged credit standings for unsuspecting customers.

It's a fact that customers are more likely to buy from retailers that they believe protect their information. Compromised retailers suffer far-reaching consequences from point-of-sale hacks, as their customers may switch to other retailers. That's not to mention enduring a burden of a potential lawsuit, which could leave the company substantially out of pocket.

Combating this fraud is therefore of crucial importance to point-of-sale vendors because it can threaten the very existence of the business itself, and has a devastating impact on retailers, the core customer of point-of-sale vendors.

It is vital for point of sale vendors to improve the security of point of sale applications and to make it easier to identify suspicious and fraudulent POS transactions and act on them to protect shoppers' sensitive data.

2. Malware targeting point-of-sale application

Mobile malware is quickly becoming one of the main ways that cybercriminals steal payment card details. Malware is used to obtain sensitive information, and in some cases to even steal money directly from bank accounts. Retailers are vulnerable to point-of-sale malware attacks and remain so until they implement the right security technology to strengthen their point-of-sale applications.

An effective application security technology should be able to detect malware, tampering, rooted/jailbroken point of sale devices, and more, so that point-of-sales providers can act before it's too late. The right application security technology needs to include a feature that alert retailers and POS providers when it is not safe to use mobile POS devices for making payments or performing other electronic transactions.

3. Cyberattacks against the point-of-sale application backend system

A point-of-sale application running on a smartphone, a tablet or a mobile device is only a single component in a full, intricate point-of-sale system. The majority of business transactions are processed on the server's side. That means most cyberattackers use the entry point from the point-of-sale application to the server to begin their attack on internal business systems.

Once the cyberattackers get inside the data center of POS vendors or retailers, not only can they access the compromised POS application, but also all other POS applications used by the retailer in other locations. Attacking the entry point at the backend is a common attacking method, and countless large-scale security breaches have been caused by this method.

Therefore, it is essential that this entry point is kept secure and protected. Point-of-sale application backend systems and other business systems hosted in the data center need to be shielded from direct internet exposure. Otherwise, hackers could easily exploit a single weakness to access numerous POS retail apps.

For retailers to trust a mobile point of sale application, they need to feel comfortable operating mobile POS apps without the risk of having their internal business systems hacked and risk being sued by affected customers.

4. Business disruption due to poor unavailability of point-of-sale applications

Retailers not only want their business and customer data to be kept safe, but also expect that there will be no disruption to their business caused by cyberattacks or technical downtime with their point of sale applications. Retailers want to operate point of sale applications in a secure, reliable way, and prevent attacks before they even happen. For this to happen, the ideal point of sale application needs to not only boast strong POS security technology but also feature a reliable security monitoring and incident response service. This service should alert IT personnel- either in-house or outsourced to a third-party outsource- when there is a breach, and also monitor POS application-related activities, detect and flag up threats, and provide real-time responses to any problems.

Having a reliable POS security monitoring and incident response service in place help POS providers to assure their retailer customers, and give them a peace of mind as they process countless of data transactions via point-of-sale applications.

If you are a provider and operator of POS application, you want to pay attention to these four common security issues affecting point-of-sale applications. If you make sure that each of them is covered, then you can rest assured that your POS application is secure, and you putting yourself at unnecessary risk of cyberattacks.