1)

Extension:

A browser extension is essentially a small piece of software that performs a function or adds a feature to a browser client. Since extensions are given special authorizations within the browser, they are attractive targets for attackers.

## How to use extensions (more) safely

Even though extensions can be risky, if used correctly, they can be extremely beneficial. It’s **especially** important to research extensions if you are using an application that accesses [P4 protected data](https://security.berkeley.edu/data-classification-standard#plclassification).

#### ****Before Installing an Extension:****

* Check out the developer’s website to see if it’s a legitimate extension and not a one-off by an unvetted source.
* Read the description. Look for things that may be questionable, like tracking info or data sharing.
* Check out the reviews. Look for users complaining of oddities happening, speculating on their data being taken, or for anything that strikes you as odd.

**When Installing an Extension:**

* Be picky. The more extensions installed, the bigger the attack surface you open up to attackers. Only pick the most useful and delete the ones you don’t need.
* Only install through trusted sources. While not guaranteed safe, security technicians review extensions for malicious content.
* Review permissions. Review extension permissions closely. If an extension installed suddenly requests new permissions, be wary. If you can’t find a reason for the permission change, it’s probably better to uninstall.
* Use antivirus protection. Install and run [SCEP(link is external)](https://software.berkeley.edu/system-center-endpoint-protection-scep-0) to detect and neutralize malicious code in browser extensions.

If you really want to dig into an extension, look it up on [https://crxcavator.io/(link is external)](https://crxcavator.io/). CRXcavator is a Chrome Extension security assessment automation tool designed to help security analysts have better insight into Chrome Extensions.

## How to see extensions already installed

* Google Chrome users click the three dots to the right of the address bar, selecting “More tools”, then “Extensions.”
* Firefox users click the three horizontal bars next to the address bar, then “Add-ons,” then “Extensions.”
* Safari users click Preferences, then on the Extensions tab. All extensions enabled will have a checkmark in the box to the left of the icon in the sidebar.
* Internet Explorer users click the gear menu at the top-right corner and select Manage add-ons. Browser plug-ins are displayed under the Toolbars and Extensions category, along with any browser toolbars and other types of ActiveX add-ons installed.

2)

The browsing the web, there’s a lot of people who know exactly what you’re doing, from your ISP (Internet Service Provider) to advertisers, governments, and social media companies. And while your approach might be the common “I have nothing to hide”, that’s not necessarily the case…

Your internet browsing actually gives away a great deal about you, from political beliefs and sexual preferences to shopping habits or health concerns. With this information in the wrong hands, you can find yourself being targeted with ads and subjected to price discrimination. So while you have nothing to hide per se, your browsing habits can be of great interest to others.

Which is why we thought we’ve come up with 5 easy tips on how you can browse the web more safely.

## 1. Stay updated

This one is pretty much a given, but you’d be surprised how often it falls by the wayside. [Virus threats](https://www.avg.com/en/signal/what-is-a-computer-virus) can be found even in the most [reputable of websites](https://www.avg.com/en/signal/website-safety), and it’s now more important than ever to keep your wits about you. Hackers are always on the lookout for new vulnerabilities and ways to get their hands on your sweet data, and the current global situation means that more people than ever are online.

Ensuring you have an updated browser (most browsers will do this automatically for you) and [antivirus software](https://www.avg.com/internet-security) will go a long way in guaranteeing your security. Remember, you don’t need to spend a lot of money on an antivirus — a free one from a reputable source is all you need. In fact, we might be able to help with that.

## 2. Get an ad blocker

Not only can an ad-blocker stop pesky ads and pop-ups from following you around the internet, but it can also make your browsing experience that little bit faster too. Many ad blockers will still allow a certain amount of ‘safe’ ads to allow websites to continue collecting revenue from them. You can also whitelist your favorite sites if you want to keep seeing certain targeted advertisements.

As an alternative, you can also consider a browser with built-in ad-blocking. Many of the [best browsers for security and privacy](https://www.avg.com/en/signal/best-browsers-most-security-privacy) offer this feature.

## 3. Vary your passwords

We know, we know, we go on about this one **a lot**. But it’s super important to vary your passwords. It’s oh so easy to reuse the same password for all your accounts, especially if you have one [super secure password](https://www.avg.com/en/signal/how-to-create-a-strong-password-that-you-wont-forget). But, all it takes is one leak for all your accounts to then be at risk — no matter how secure that password seemed.

Using a wide, unique selection of secure passwords means that if your info is leaked it’s not going to put all your online accounts at risk. Remembering 350 passwords that look like 3CX-6HG-IU8 can be pretty tricky, which is where a [password manager](https://www.avg.com/en/signal/why-you-need-a-password-manager) can come in handy.

## 4. Clear those cookies

[Deleting your cookies](https://www.avg.com/en/signal/delete-browser-cookies) — that would be the little bits of data a website has saved on your browser — and clearing your cache can reduce how many ads are following you around the internet and targeting you. It's a short-term solution, but it’ll refresh your browser, and clear out saved data-like passwords that could be stolen easily. Remember to whitelist the pages you want to keep login details for though.

Another little tip to reduce your [cookies](https://www.avg.com/en/signal/what-are-cookies) is to turn on any private browsing options your browser may have. It’s really not as private as the name suggests — your ISP can still see everything you do — but it does limit how many cookies you get and [hides your browsing history](https://www.avg.com/en/signal/how-to-clear-your-browsing-and-search-history), which can be useful on a shared device.

## 5. Use a VPN

Using a [VPN](https://www.avg.com/en/signal/what-is-a-vpn-and-why-should-you-use-one), or virtual private network, encrypts your data while it travels from one place to another on the internet. Using a VPN when you’re online allows you to browse websites privately and securely, as well as [gain access to restricted websites](https://www.avg.com/en/signal/how-to-unblock-websites) and overcome censorship blocks. Which comes in handy, especially right now when we have more time on our hands than ever, and a greater need for global content access.

It’s important to remember that a VPN only [hides your IP address](https://www.avg.com/en/signal/hide-your-ip-address), location, and data as it is transmitted. In order to ensure a completely secure browsing experience you need to combine using one with a secure browser. Which leads us nicely onto the next step.

## 6.Stay safe online with a secure and private browser

Of course your ideal solution here is a browser that does as many of these things for you as possible. Now, we wouldn't normally push our products on you here so excuse the little plug, but it*is*free, so we thought that might help.

[AVG Secure Browser](https://www.avg.com/secure-browser) comes with built-in adblock and anti-track software. The desktop version works with our VPN and the mobile version has one built-in. So, if you're in the market for a safer browsing experience then give it a go. It works on [Windows](https://www.avg.com/secure-browser#pc), [Mac](https://www.avg.com/secure-browser#mac), and [Android](https://play.google.com/store/apps/details?id=com.avg.android.secure.browser&hl=en&referrer=utm_source%3Davg%26utm_medium%3Dblog-post%26lang%3Den)!

3)

# Two Factor Authentication (2FA):

Two-factor authentication (2FA), a type of multi-factor authentication (MFA), is a security process that cross-verifies users with two different forms of identification, most commonly knowledge of an email address and proof of ownership of a mobile phone.

Used on top of the regular username/password verification, 2FA bolsters security by making it more difficult for intruders to gain unauthorized access, even if a perpetrator gets past the first authentication step (e.g., brute forces a username and password).

Today, 2FA is commonly employed in online banking websites, social media platforms and e-commerce sites as a way to harden [access controls to the more sensitive areas of a web application](https://www.imperva.com/learn/application-security/broken-object-level-authorization-bola/)(e.g., admin panels or areas that store credit details and/or personal data).

Two-factor authentication also enables businesses and public institutions to be more productive and efficient, allowing employees to perform remote tasks with far less security concerns.

## Multi-factor authentication methods

MFA identification can be categorized into three types:

* **Knowledge factors** (something the user knows) – Common examples are email addresses, username-password combinations, answers to security questions, and the CVV on the back of a credit card.
* **Possession factors** (something the user owns) – Examples of this authentication type include a mobile phone, USB token and a card reader.
* **Inherence factors** (something the user is/has) – This authentication type pertains to unique physical attributes that are inherent to a single person, such as fingerprint readers, retinal scans and voice recognition.2FA example using a mobile device.

Typically, the 2FA method verifies the user’s identity against a knowledge factor alongside one of the remaining two factor types. Going to the ATM is a good example, as the bank requires that you provide both your credit card (possession factor) and your personal identification number (knowledge factor) to take out money.

## Potential downsides to two-factor authentication

2FA, and multi-factor authentication as a whole, is a reliable and effective system for blocking unauthorized access. It still, however, has some downsides. These include:

* **Increased login time** – Users must go through an extra step to login into an application, adding time to the login process.
* **Integration** – 2FA usually depends on services or hardware provided by third parties, e.g., a mobile service provider issuing verification codes via text message. This creates a dependency issue, as the enterprise has no means of controlling these external services should a malfunction occur.
* **Maintenance** – Ongoing maintenance of a 2FA system might prove to be a chore in the absence of an efficient way of managing a database of users and various authentication methods.

## Web application security and 2FA

Two-factor authentication can play an important role in securing your website by blocking a number of application-based attacks.

These include brute force and dictionary attacks, in which perpetrators use automated software to generate massive amounts of username/password combinations in an attempt to guess a user’s credentials.

With 2FA enabled, these attacks are fruitless—even if perpetrators are able to discover a user’s password, they still lack the second form of identification needed to login to the application.

Additionally, two-factor authentication can help applications counter social engineering attacks, e.g., [phishing](https://www.imperva.com/learn/application-security/phishing-attack-scam/) and [spear phishing](https://www.imperva.com/learn/application-security/spear-phishing/), which attempt to dupe a user into revealing sensitive data, including their username and password. Even in the event of a successful attack, a perpetrator would still need the additional form of identification required by a 2FA solution.

As such, the [Payment Card Industry (PCI) Data Security Standards (DSS)](https://www.imperva.com/learn/data-security/pci-dss-certification/), which is used to [secure](https://www.imperva.com/learn/application-security/application-security/) credit and debit card transactions against data theft and fraud, requires 2FA as a fundamental prerequisite for receiving certification.

4)

### Creating strong passwords:

we need to **create a password**to do just about everything on the Web, from checking your email to online banking. And while it's simpler to use a short, easy-to-remember password, this can also pose **serious risks** to your online security. To protect yourself and your information, you'll want to use passwords that are **long**,**strong**,**and difficult for someone else to guess** while still keeping them relatively **easy for you to remember**.

A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

* **Never use personal information** such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.
* **Use a longer password**. Your password should be **at least six characters long**, although for extra security it should be even longer.
* **Don't use the same password for each account**. If someone discovers your password for one account, all of your other accounts will be vulnerable.
* Try to include **numbers, symbols**, and both **uppercase**and**lowercase letters**.
* Avoid using words that can be**found in the dictionary**. For example, **swimming1** would be a weak password.
* **Random passwords are the strongest**. If you're having trouble creating one, you can use a [**password generator**](http://strongpasswordgenerator.com/) instead.

#### Common password mistakes

Some of the most commonly used passwords are based on **family names**, **hobbies**, or just a **simple pattern**. While these types of passwords are easy to remember, they're also some of the least secure. Let's take a look at some of the most common password mistakes and how to fix them.

**Problem**: This password uses too much personal information, along with common words that could be found in the dictionary.

**Solution**: A stronger version of this password would use symbols, uppercase letters, and a more random order. And rather than using family names, we could combine a character from a movie with a type of food. For example, Chewbacca and pizza could become **chEwbAccAp!ZZa**.

**Problem**: While patterns like this are easy to remember, they're also some of the first things a hacker might guess when attempting to access your account.

**Solution**: Remember that **random passwords** are much stronger than simple patterns. If you're having trouble creating a new password, try using a [**password generator**](http://strongpasswordgenerator.com/) instead. Here's an example of a generated password: **#eV$pIg&qf**.

If you use a password generator, you may also want to create a **mnemonic device** to make the password easier to remember. For example, **H=jNp2#** could be remembered as **HARRY = jessica NORTH paris 2 #**. This may still feel pretty random, but with a bit of practice it becomes relatively easy to memorize.

#### Using password managers

Instead of writing your passwords on paper where someone might find them, you can use a**password manager** to store them securely online. Password managers can remember and enter your password on different websites, which means you won't have to remember longer passwords. Examples of password managers include **[LastPass](https://lastpass.com/" \t "_blank)**, [**1Password**](https://1password.com/), and [**Google Chrome's password manager**](http://support.google.com/chrome/bin/answer.py?hl=en&answer=95606).

This is a great example of a **strong password**. It's strong, long, and difficult for someone else to guess. It uses **more than 10 characters** with letters (both **uppercase** and **lowercase**), **numbers**, and **symbols**, and includes no obvious personal information or common words. This password might even be a bit too complicated to remember **without a password manager**, which underscores why they're so helpful when creating a strong password.

Remember to use these tips whenever you create a password to keep your online information safe and secure.

5)

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.

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.

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.

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.

While the attacks against PoS systems are decreasing, it does not mean they will completely disappear. Cybercriminals will continue to target vulnerable and compromised PoS systems as long as there is a market for stolen credit cards. However, with the retailers switching over to secure EMV (Europay Mastercard and Visa) cards, P2PE and tokenization, scam activities have dropped considerably.

An all-inclusive payment security solutions, including encryption, have become mandatory for businesses to avoid data breaches and secure transactions. Some of the PoS security practices include the exclusive use of PCI-compliant devices, constant surveillance of physical devices to prevent tampering of wires, placing hidden cameras, and avoiding the connection of PoS to any external networks. While data breach risks are still real, security technologies are changing rapidly to protect card holders at PoS systems.