Extended Play

Staying Safe with Browser Extensions

Time: 5 minutes

Points:

What is a Browser Extension?

Whether it's to stream your favorite show, buy yourself new shoes, or apply for your dream job, the internet – and the browsers we use to access it – are undoubtedly part of our everyday lives. But what if there were a way to make your everyday browser experience more efficient?

Browser extensions (also referred to as plug-ins) are small programs that can be added on to web browsers like Google Chrome, Firefox, Safari or Microsoft Edge to enhance the efficiency, usability, security and management of the web browser.

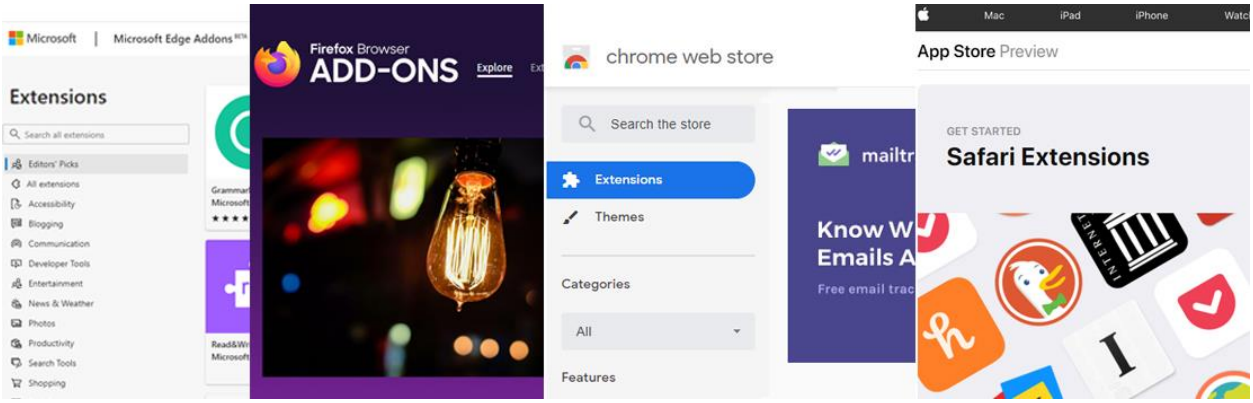
Similar to add-ons for a new car, extensions are an optional extension of a browser's base capabilities. While extensions are not required to use ("browse") the internet, they can be very helpful in enhancing a user's online experience. Among the more popular extensions are those used for:

- Translation
- Screen capturing
- Price comparisons
- Visual/Audio Accessibility
- Ad blocking
- Password managers
- Time tracking

With tens-of-thousands of browser extensions available, there's a long list to choose from when looking for an extension that suits your needs. But while these extensions may initially be approved for use by browser publishers like Google or Microsoft, it is possible that over time they become compromised and no longer safe to use.

How Can an Approved Extension Become Compromised?

In order to install most extensions into a browser, users must go to their browser's web store and download it from the secure website. Extensions offered through a browser's web store must first be reviewed and approved before becoming available for download. Once approved and placed on the market, cybercriminals are able to overtake control of these once-approved extensions.



How Do Cyber Criminals Steal an Extension?

A stolen extension is an approved and maintained extension that has since been illegally compromised by cybercriminals. While these extensions were originally safe and monitored by its developers, cybercriminals can hack or phish developers to gain the necessary access to compromise an extension.

Abandoned Extensions Can Occur, Too

An abandoned extension on the other hand is an extension that has been abandoned by its owner and taken by, or neglectfully sold to, cybercriminals. This typically occurs when an originally approved extension is no longer maintained by its owners and therefore the legal rights are left for the taking.

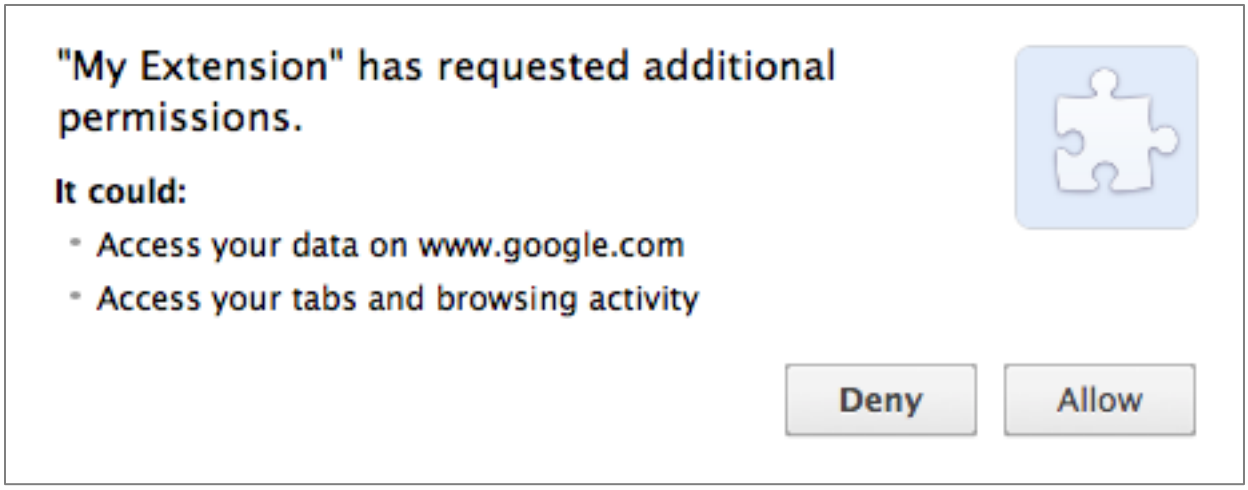
Staying Protected When Using Extensions

Browser extensions are meant to be helpful. But while these extensions are meant to make using a browser easier, that is not always the case. As we've learned, even extensions once deemed safe can potentially turn malicious. By following some quick and easy precautionary tips, you can significantly reduce the likelihood of becoming affected.

Watching Permissions

When installing an extension, permissions (such as permission to access your device's location) must be granted from the browser to the extension for proper functionality. The problem is, not all browsers ask users to grant these permissions— instead they allow permissions by default.

In order to monitor these permissions and to ensure that an extension is not requesting unnecessary or malicious permissions, consider using a browser like Google Chrome – currently the only web browser that asks users to first approve extension permissions before use.



Safe Source

Extensions should only be downloaded from a browser's official web store. Ignore messages claiming that a specific extension must be installed to access a website's content, as it is likely an attempt by cybercriminals to trick you into installing a malicious extension.

Like other online stores, customer reviews can be extremely valuable. Before installing an extension, take a moment to briefly research the extension online and read any reviews to ensure the extension or the extension's update has not affected others.

Only the Essentials

While browser extensions can bring luxury to your online interactions, too many under-utilized extensions can compromise the safety of these interactions. To stay protected, consider uninstalling any extensions that are no longer used. With less extensions, there comes a decreased likelihood of your extensions becoming stolen or abandoned.

Anti-virus/Anti-malware Software

Anti-virus software (like Norton and Malwarebytes that can be earned by reaching levels three, four and five in this platform) can be a great tool for staying protected. With the click of a button, anti-virus/anti-malware software can help ensure the safety and protection of your valuable digital information in the case of installing a stolen or abandoned extension.

With an ever-expanding online world for us to utilize and explore, extensions can make that experience a whole lot easier. And by taking the precautionary steps, you can enjoy all the benefits browser extensions have to offer without the worry of cybercriminals getting in your way.

References:

"Browser Extensions: Are They Worth the Risk?" Krebsonsecurity. Published: 9/18/2018. Accessed: 9/16/2019.

"Why you should be careful with browser extensions" Kaspersky Daily. Published: 1/30/2018. Accessed: 9/16/2019.

"Browser Extensions Are a Privacy Nightmare: Stop Using So Many of Them" How-to Geek. Published: 8/14/2017. Accessed: 9/18/2019.

Quiz Questions

Q1: True or False, browser extensions must be installed before you can use a web browser?

A1: True – This is actually False. Similar to add-ons for a new car, extensions are an optional extension of a browser's base capabilities. While extensions are not required to use, or "browse", the internet, they can be very helpful in enhancing a user's online experience.

*A2: False – Correct! Similar to add-ons for a new car, extensions are an optional extension of a browser's base capabilities. While extensions are not required to use, or "browse", the internet, they can be very helpful in enhancing a user's online experience.

Q2: Once an approved browser extension is downloaded from a browser's web store:

A1: It can never become compromised and will always remain safe to use. – A browser extension actually can become compromised. Extensions offered through a browser's web store must first be reviewed and approved before becoming available for download; but once approved and placed on the market, it is still possible for cybercriminals to take control of these once-approved extensions.

*A2: It is safe to use but can potentially become compromised in the future. – Correct! Extensions offered through a browser's web store must first be reviewed and approved before becoming available for download; but once approved and placed on the market, it is still possible for cybercriminals to take control of these once-approved extensions.

A3: It will immediately grant cybercriminals access to your personal information. – A browser extension actually can become compromised. Extensions offered through a browser's web store must first be reviewed and approved before becoming available for download; but once approved and placed on the market, it is still possible for cybercriminals to take control of these once-approved extensions.

Q3: _____ should only be granted by the user to ensure unnecessary or potentially malicious _____ are not granted.

A1: Extensions- Permissions should only be granted by the user. While many browsers automatically grant permissions to extensions, consider using a browser like Google Chrome that instead requires the user to grant permission to ensure unnecessary or potentially malicious permissions are not accidentally granted.

A2: Passwords- Permissions should only be granted by the user. While many browsers automatically grant permissions to extensions, consider using a browser like Google Chrome that instead requires the user to grant permission to ensure unnecessary or potentially malicious permissions are not accidentally granted.

*A3: Permissions- Correct! Permissions should only be granted by the user. While many browsers automatically grant permissions to extensions, consider using a browser like Google Chrome that instead requires the user to grant permission to ensure unnecessary or potentially malicious permissions are not accidentally granted.