# Windows 10 Security

## HOW TO SECURE A HACKER'S #1 TARGET


Browsers, such as Internet Explorer or Chrome™, are the #1 way we access the internet — which makes them the #1 target for hackers. These attacks typically come by way of an accidental or intentional click on a link that launches malicious code known as malware. There are a few simple steps you can take to significantly reduce the chances of a malware attack through your browser.

### USE A SECURE BROWSER.

Internet Explorer, Edge, and Chrome all offer strong security features with Windows. Edge and Internet Explorer 11, for example, use Microsoft SmartScreen to perform a reputation check on each site, and block any they suspect to be a phishing site. Additionally, on HP commercial PCs, Internet Explorer benefits from the additional security of HP Sure Click: whenever a tab is opened, HP Sure Click runs it in an isolated virtual machine. This means that any malicious code is trapped in the tab, and is destroyed when you close your browser.

### KEEP IT CURRENT.

Enable automatic browser updates through Settings.Doing so will ensure that all security updates are applied to your browser, making it much safer and increasing the chance that malware attacks will fail.

> *In Edge, updates are applied whenever Windows updates. However,to check whether you need an update to Edge, go to Start* **->** *Settings* **->** *Updates and Security* **->** *Windows Update* **->** *Check for updates.*

### HEED WARNINGS.

A secure browser should have a basic threshold for detecting malicious websites and will display a warning if they believe there to be a reasonable threat. Some also offer URL "autocorrect" features, to prevent navigating to a commonly-misspelled domain (where malicious software and sites are often hosted).

### RESTRICT CONTENT AND PLUG-INS.

Many of these browser add-ons (like Flash or JavaScript) are necessary for rich sites and web programs, but their increased access to your system also makes them a vulnerability. Microsoft Edge disables them by default, requiring a site to ask for permission to use them, and ensures only sites you opt to trust can use their features. You can replicate that security in other browsers, like Internet Explorer:

> *In IE, go to Tools (gear icon)* **->** *Internet Options* **->** *Security* **->** *Internet -> Custom level...* **->** *Scripting. You can disable JavaScript by simply selecting "Disable," or you can request IE ask before a site tries to use it by selecting "Prompt."*

For all the attention we give our online security habits, the importance of choosing a browser and configuring it properly is often overlooked. And that's exactly what makes them a hacker's favorite target. A good browser and proper use of it's settings can make the difference between an attack and merely an attempt.

*Be more secure from power on to power off.*

1HP Sure Click is available on most HP PCs and supports Microsoft® Internet Explorer and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode, when Microsoft Office or Adobe Acrobat are installed.