GetApp®

# 10 Best Practices for Safe Internet Browsing

## Here are ten tips to help you stay safe as you browse online.

1. **Update browser and OS software regularly:** Running older versions of your browser or operating system (OS) leaves you vulnerable to new forms of malware. Ensure that you update your software tools as soon as possible every time a new patch is offered.

2. **Check for HTTPS and the padlock sign:** An HTTPS connection encrypts your connection with the third-party websites you browse. This becomes particularly important when you are sharing confidential information such as financial details when making an online payment. Only submit confidential details on websites that have the HTTPS certificate.

> **You must also ensure that your own business website is protected using an HTTPS certificate to strengthen its security and to prevent hacks.**

3. **Scan file downloads:** Cybercriminals try to trick you into downloading malicious files laced with malware. Never download files from unknown websites. Install antivirus software that can help detect whether the files you're about to download are potentially harmful.

4. **Use a VPN to connect to the office network when working remotely:** Virtual private networks (VPNs) help to secure your connection with your office or business network even when you're logging in from a public network. It secures and encrypts communications with your business network, ensuring that data transmission is safe.

5. **Use multiple strong passwords:** Eighty-one percent of hacking incidents took advantage of stolen or weak passwords because hackers can easily break into accounts that use weak passwords. Using the same password across multiple websites also makes it easier for hackers to break into all your different accounts. Use a password manager tool to store multiple passwords securely.

6. **Update and run antivirus software regularly**: Antivirus software solutions detect malicious files and alert you. It is important that you update your antivirus software regularly so it can detect all the latest forms of malware and spyware. Also, condition your employees to break the habit of delaying scheduled scans to ensure improved security posture at all times.

7. **Check URLs and webpage content for phishing:** Double-check all URLs to ensure authenticity. You should also roll your mouse over the hyperlinked text in a document to see where it leads. Be wary of websites that offer free games, ask for money, want you to recruit others, etc. since they could be harmful websites or phishing attempts. Always, when in doubt, seek help from a supervisor or IT team.

8. **Optimize privacy settings:** Keep your privacy settings turned "ON." This helps you keep your digital footprint less exposed. Otherwise, hackers and spammers will try to get a hold of your personal information.

9. **Optimize cookie storage:** Cookies are temporary files in your browser's cache that store details such as usernames and passwords. While this makes browsing convenient, it is a juicy target for hackers to steal your credentials. Manage your cookies using the various options provided within the browser, including deleting them on a weekly or monthly basis, depending on the sensitivity of information and the frequency of its use.

10. **Post judiciously on social media:** People can go overboard with what they post on social media websites. Posting personal or professional details that would ideally stay confidential will only get hackers one step closer to you.