



20 Tips to Stay Protected Online

GENERAL SECURITY TIPS

1. Always keep your security software working and up-to-date. Especially if you use a laptop on unprotected wireless networks in airports, cafes and other locations.
2. Install products and solutions that protect you whether you're surfing the Internet or downloading files directly to your computer.
3. Ensure that Web protection software extends beyond email protection to encompass peer-to-peer networks and the entire range of home computing applications, and can provide warnings about traffic that is incoming and outgoing from your computer in real-time.
4. Employ the latest technologies, such as Web reputation, which can measure the trustworthiness and safety of a Website before you visit it. Use Web reputation technology combined with existing URL filtering and content scanning technologies.
5. Use the latest Web browser version and install security patches when available.
6. Use a web browser that has a no-script plug-in.
7. Check with your Internet Service Provider to see what kind of protection is offered by their network.
8. If you use the Microsoft Windows operating system, enable the "Automatic Update" feature and apply new updates as soon as they are available.
9. Always install, update, and maintain firewalls and intrusion detection software, including those that provide malware/spyware security.
10. Make sure that your security software solution is up to date.

FOR EMAIL

11. Always make sure you are using an anti-spam product for each email address you have.
12. Beware of unexpected or strange-looking emails, regardless of who the sender is. Never open attachments or click on links in these emails.
13. Report suspicious emails to the appropriate authorities.
14. If you trust the sender of the email, scan their email attachments with a security solution before opening them. If they send you a URL and it is short enough, type the URL in your web browser instead of clicking on it from the email.
15. Be alert when receiving emails that request account details (financial institutions almost never request financial details in emails).
16. Never email financial information to anyone.

FOR WEB SURFING AND DOWNLOADING ONLINE PROGRAMS

17. Use a Web reputation service to make sure the website you are going to visit is safe from web threats.

18. Beware of Web pages that require software installation. Scan all programs downloaded from the Internet with an up-to-date security solution.
19. Always read the End User License Agreement and cancel the installation process if other “programs” are going to be installed in addition to the desired program.
20. Do not provide personal information to unsolicited requests for information. Only provide personal information on sites that display a lock icon at the bottom of your browser.

