How to improve your online safety with Chrome

4 important security steps you can take now

01 How do I protect myself from malware and phishing attacks?
Turn on enhanced protection. It helps guard against phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or extensions. You can activate it under Settings > Privacy and security > Security.

02 How do I know if any of my passwords have been stolen?
One of the simplest things you can do is go to your Settings and run a Safety Check. With just a few clicks, this all-in-one tool monitors passwords, updates, extensions and Safe Browsing.
- How Chrome protects your passwords
- Read the blog post on the future of password safety

03 How do I know if a site’s connection is secure?
Chrome will alert you if you can’t visit the site safely or privately by labeling the site “Not Secure” to the left of the URL.

Safe Browsing resources
- How to find Safety Check
- Here’s an overview video of Safety Check
- Watch the video on 4 ways to stay safe in Chrome
- Hear what our security experts say about Enhanced Safe Browsing
- How to interpret site security symbols

04 How do Chrome updates affect me?
While you’re working, Chrome automatically checks for updates in the background. Every time you close and relaunch the browser, it applies any potential new features and security fixes. Occasionally, your company admin may remind you to relaunch; or notify you of a scheduled automatic relaunch. The sooner you relaunch, the safer your browsing experience will be.

Updates resources
- Learn more about Chrome updates in the Chrome Help Center

For the latest Chrome security tips, follow us on Twitter.

Please note that some of these settings may be managed by your administrator, which may limit your ability to make adjustments.