



grassmarket
community project

Internet Safety Rules & What Not to Do Online

1. Keep Personal Information Professional and Limited

Most people do not need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to contact you. You would not hand purely personal information out to strangers individually—do not hand it out to millions of people online.

2. Keep Your Privacy Settings On

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. You can take charge of your information. Both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy setting and keep them enabled.

3. Practice Safe Browsing

Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you do not even give the hackers a chance.

4. Make Sure Your Internet Connection is Secure

When you go online in a public place, for example by using a public Wi-Fi connection, you have no direct control over its security. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you can connect to a secure Wi-Fi network) before providing information such as your bank account number.

5. Be Careful What You Download

Cybercriminals want to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. do not download apps that look suspicious or come from a site you do not trust.

6. Choose Strong Passwords

Passwords are one of the biggest weak spots in the whole Internet security structure, but there is currently no way around them. The problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to

demystify. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers, and special characters.

7. Make Online Purchases from Secure Sites

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. You can identify secure sites by looking for an address that starts with *https*: (the S stands for *secure*) rather than simply *http*: They may also be marked by a padlock icon next to the address bar.

8. Be Careful What You Post

The Internet does not have a delete key, any comment or image you post online may stay online forever because removing the original (say, from Twitter, Facebook, or Instagram) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you had not made or get rid of that embarrassing selfie you took at a party. Do not put anything online that you would not want anyone to see.

9. Be Careful Who You Meet Online

People you meet online are not always who they claim to be. Indeed, they may not even be real. fake social media profiles are a current way for hackers to cosy up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

10. Keep Your Antivirus Program Up to Date

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it is to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

Best Free internet Security Software

1. <https://www.totalav.com/en/free-antivirus>
2. https://www.avast.com/en-gb/index?sid=SID_35_4adb5e8eb47dd3e60d0378779f696857_t1_7#pc
3. https://www.avg.com/en-gb/free-antivirus-download?utm_source=commissionjunction&utm_medium=affiliate&utm_campaign=3211374&utm_content=11609239&couponfield=yes&cjevent=4b0c3e12738511ec83ec71880a18050f#pc

Struggling with IT or Computer skills? Contact Mike or Kevin and book on to our twice weekly Computer skills classes. They are free and take you from basic to advanced.

www.grassmarket.org