Staying Safe Online Explained

Unsafe surfing can lead to threats. This could be anything from embarrassing personal comments to cyber bullying. Once images are online, it is almost impossible to erase them, so be careful what you share. Careless posting can get you mixed up with people you rather have nothing to do with. Here are 10 Top Internet Safety rules it is suggested you follow to help you avoid getting into trouble online (and offline).

1. Keep Personal Information Professional and Limited

Potential employers or customers 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 get in touch with you. You would not give your personal information to strangers so do not give it to millions of people online.

2. Keep Your Privacy Settings On

Marketing companies love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. It is recommended you take charge of your information. As noted by a 'Life Hacker' – 'both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook have privacy and enhancing settings available. These settings can be deliberately hard to find because companies want your personal information for its marketing value'. Make sure you always enable the privacy settings and safeguards and keep them enabled.

3. Practice Safe Browsing

You would not choose to walk in a dangerous area, so do not visit dangerous areas online, because Cybercriminals may use lurid content as bait. They know people are sometimes tempted by dubious content, with users letting their guard down when searching. The Interne is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect a device with malware. By resisting the urge, you do not give hackers the chance.

4. Make Sure Your Internet Connection is Secure

When going online in a public place, for example by using a public Wi-Fi connection, you have no direct control over its security. Corporate cybersecurity experts worry about "endpoints" (the place where a private network connects to the outside world). Your vulnerable endpoint is your local Internet connection. 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 details.

5. Be Careful What You Download

The goal of cybercriminals is to trick you into downloading malware, (programs or Apps that carry malware to steel information). Malware can be disguised as an App: anything from a popular game to something that checks traffic or the weather. PC World advises that you 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 currently there is 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 easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you do not forget them. 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: These sites 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, as many people have found out! Any comment or image you post online may stay online forever because removing the original (say, from Twitter) does not remove any copies that other people may have 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 your mom or a prospective employer to see now or ever!

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. InfoWorld reports, fake social media profiles are a popular way for hackers to cosy up to unwary 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 always up to date. Be sure to keep your operating system and applications current by installing recommended updates. They provide a vital layer of security.

Follow these 10 basic Internet safety rules and you will avoid many of the nasty surprises that lurk online for the careless.