10 Internet Safety Tips to Protect Yourself Online

The Internet is an important part of daily modern life, however it's also home to numerous scammers and crooks. Here are 10 practical tips to help you stay safe on the internet and avoid the loss of money, Data or identity.

1. Email Scams - Don't fall prey to 'clickbait'

If you receive an email promising you a million dollars or a free cruise through the Bahamas, know that it's *always* too good to be true. Your Bank will NOT email or contact you to update or confirm details. Nor do they want Gift Cards to pay debts. If in doubt contact your Bank etc directly.

Email providers generally have good SPAM detection - Try checking your email settings to make sure you have your **filter** turned 'on.' This will help prevent fake emails meant to give your device a virus from coming into your inbox. This might stop certain emails you want from coming through, so just make sure you check your 'junk' folder every once in a while.

Some handy links - https://www.scamwatch.gov.au for lots of info and shorturl.at/rtyLP on **Phishing scams**

2. Don't over share personal information online

Don't share personal information on public social media platforms. Pretty straightforward, right?

Make your social media accounts private if you share your heart and soul with your friends. Also, don't have your personal email address where anyone can find it. This will minimize the number of 'free cruises' you're offered over email.

3. Be wary of what you download

Cybercriminals love installing malware through free downloads. Never download apps or documents unless they come from a website you know and trust. Know what you're downloading before you click on that "free and easy download" that's not actually real. If you must download something then at the very least scan it with your Anti-Virus

4. Invest in a reliable virtual private network (VPN)

Using a virtual private network (VPN) is an excellent way to protect your online activity, especially when you're using public Wi-Fi networks. VPNs work by routing your internet connection through a private server, rather than coming directly from your computer. Since the VPN encrypts your data, your identity stays anonymous, which means that hackers won't be able to steal your personal information as easily. Investing in a good VPN is an important step to online safety and security.

5. Use and Update your antivirus program

There are plenty of internet security programs to choose from. While it can't protect you from every online threat, it's important to update your security program so it can detect the latest versions of threatening malware.

Even the most updated antivirus programs can't protect you from every hacker. In order to protect your privacy further, consider using a VPN in addition to an antivirus program.

6. Know how to choose strong passwords

Passwords like "thisismypassword" or "rememberpassword" are examples you should stay away from. Think of something unique to you; use numbers and a mix of upper and lower case letters. Instead of creating a password that's easy to remember, create a unique strong password, and take the time to write it down.

Here's another tip: don't use the same password over and over. You don't want the hacker that broke into your Facebook account to also know how to access your online banking, Instagram, Gmail, Netflix, and Amazon Prime.

Here is a ***simple*** example – tested on MS Password Tester for Windows 8 (from Windows App Store)

Simplepassword 16%	s1mpl3password 54%	S1mpl3password 90%	s1mpl3password15042121 100%
Thisismypassword 18%	Th1s1smypassword 58%		Th1s1smypassword15042121 100%

7. Practice safe shopping habits

When shopping online, remember to pay attention to website domains. If the website starts with "**https**," it's more secure than sites beginning with "http." Remember to look closely at the website domain (the name in the search bar) before you buy that fancy new phone on such a great deal.

Use credit cards or Paypal - at least that way you have a chance of getting your money back. But watch out for excuses that are designed to stop you putting a stop on a transaction before it's too late.

8. Remember to protect your mobile phone and other hand-held devices

Sometimes it's easy to think of internet safety as only important for your laptop or PC. However, your phone, tablet, and other devices are at risk just as much, if not more. Many people use public Wi-Fi on their mobile devices even more than on their laptop. There's lots of ways now that you can set a lock on your mobile or tablet device to keep it secure, whether it's a password, Personal Identification Number (PIN), passcode, gesture or fingerprint that must be entered to unlock the device – so use one.

9. Backup your data

I can't overstress this ... Backing up your data is important, no matter what. Avoid accidentally losing the photos you took on that trip abroad or those papers that took so long to write. Back them up somewhere you can access if something happens to your device, or if you're techy then try Google Drive. Remember, internet safety isn't only about stopping hackers, it's also important because it helps you avoid unwanted incidents like losing important work.

10. Turn 'off' your Bluetooth, or make sure you use a good password to protect your device.

It great for quickly connecting to your car, but Bluetooth works by using UHF radio waves to make the connection between devices wireless. Like any wireless connection, it can be disrupted by hackers. By having your Bluetooth on, you make your data more vulnerable by exposing your device through the Bluetooth connection. So make sure you setup your Bluetooth with a good password or, when in public, do yourself a favour; check your settings and turn Bluetooth 'off.'