# How To Stay Safe Online: 8 Tips And Tricks



Is your private information protected?

We all use the internet everyday, but do you really know how well your personal information is secured?

[Cyber security is key](https://www.benchmarkitservices.com/cyber-security/). From hackers to phishers, there are people trying to take your money, your data and your life!

Thankfully, with a little knowledge you can stay safe from these influences, and by taking the 8 following steps you’ll be able to sleep easy knowing your digital life is in safe hands.

## 1. Understand Hackers Can Target You

Hackers are always on the lookout for unsuspecting users. They are always hunting for personal and financial information.

That said, everyone needs to understand that they too can be targeted/victims, hence take a proactive approach to keep the hackers out. One of the best ways to do this would be by remaining vigilant and careful whenever surfing the internet.

[It’s always a good idea to back up your data just in case!](https://www.benchmarkitservices.com/blog/top-5-reasons-you-should-backup-your-data/)

## 2. Ensure You Have the Latest Software Updates

Operating Systems and programs get regular updates to patch any vulnerabilities they might have, among other functions.

While it may not seem essential for you, keeping your operating system up-to-date, as well as the programs helps keep hackers away. Turning automatic updates on should help ensure your operating system gets updates whenever they are updated.

You should also do the same for other apps as well. This includes web browsers and plug-ins.

[This will help ensure you don’t get any nasty malware or viruses.](https://www.benchmarkitservices.com/computer-services/malware-virus-removal/)

## 3. Beware of Phishing (Suspicious) Phone Calls and Emails

Hackers and malicious individuals use phishing emails and even phone calls, which trick you into giving them your personal as well as login details for your banking and credit accounts.

Phishing emails are cleverly designed to look like the original emails, hence could easily trick you. Beware of emails and phone calls that ask you to provide your login details, personal information, or even click a link.

[Air conditioner repair expert](https://aircaresolutions.com.au/air-conditioning-repair-bondi/) Karl Ammoun says “*be sure to call the respective company if unsure of what to do. Calling the official number provided by the provider ensures you don't fall into a scammer's tricks. I’ve spoken to many clients, especially older ones, who have either been scammed or know someone who’s been scammed this way. It pays to be a little cautious.”*

## 4. Use Strong and Unique Passwords

The average person has at least 5 passwords for various sites and accounts.

Many people, however, have a tendency of using the same password across accounts or even write them up in a sticky pad or book. This isn't particularly smart as anyone could guess one password and try it across all your accounts.

Proper password management is the only way you can be sure all your accounts are safe and secure. For starters, make sure your passwords are at least 20 characters long and unique for each account. You could also use a password management program to help store your credentials and passwords automatically, notes [Search It Local](https://www.searchitlocal.com.au/) HR Manager Jacqueline Payne. She says “*tools like LastPass are a lifesaver. Not just by keeping outside influences at bay, but by keeping all passwords hidden from staff, but still accessible, there is even less of a security risk. Password peace of mind is a real thing, and it’s worth having!”.*

This way, you only need to remember one password. You can find both free and paid programs for this.

In addition to this, you should consider:

*a. Updating your passwords regularly*

*b. Never share your passwords with anyone*

*c. Never mix passwords across websites*

##

## 5. Don't Click on Any Suspicious Links

Only click on links you are sure of, and especially those included in emails. You also shouldn't download files and software from untrusted sources.

Visiting some of these sites grants them access to your computer, hence could install malware to your computer silently. Avoid downloading any attachments automatically onto your computer too.

## 6. Keep Sensitive Data Safe and Secured

Sensitive data should always be kept in a safe vault. ]

Here are a few tips how:

* *Don't keep sensitive information/data on your laptop, workstation, or mobile phones. These include credit card information, SSN's, health information, and student records.*
* *Get rid of sensitive information from your computer once done with it.*
* *Contact a specialist for help securing your data.*

## 7. Use Mobile Devices Responsibly



Many of us rely on our mobile devices, especially phones, every day. This makes them a specific target for hackers. Keeping your mobile devices safe could however work. Some of the ways to keep your mobile devices safe are by:

* Use a password or PIN on your device
* Only download and install apps from trusted sources
* Keep the operating system up to date
* Never click on attachments or links from unsolicited texts and emails
* Don't store personal information on the device
* Use data encryption tools for your device, e.g., Android Device Manager for Android and Apple's Find my iPhone.

These tools come in handy, especially when you can't find your device, as well as secure your data should it be stolen.

## 8. Install an Antivirus

Installing an antivirus program (from a trusted source) can help prevent/block malware and phishing emails from your device. Like the operating system, the antivirus program should be kept up-to-date to be effective.

There are plenty of both paid and free antivirus programs to use for your personal computer. Be sure to research more about the antivirus programs available before settling for one.

Take these 8 steps and you’ll be stopping anyone from targeting you.

Do you have any tips or tricks we missed? Let us know in the comments.

**Are you in need of quick and reliable virus or malware removal?** [Chat to the experts from Benchmark IT Services to find out more!](https://www.benchmarkitservices.com/get-a-free-quote/)