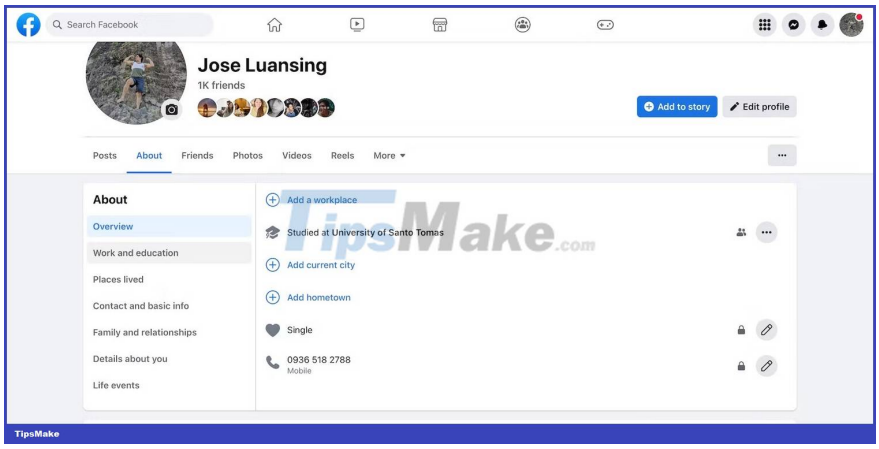
7 security mistakes you often make

Although revolutionary, the ease and convenience of disseminating information online also lurks some security threats. Many people have unknowingly engaged in risky online activities.

Although revolutionary, the ease and convenience of disseminating information online also lurks some security threats. Many people have unknowingly engaged in risky online activities.

In fact, you're probably making some serious security and privacy mistakes on the Internet right now. Find out below!

1. Revealing too much information on social media



For many people, social media plays a very important role. They can share their inner thoughts, post their daily experiences, or even create a completely different personality online. It's a fun, satisfying form of self-expression.

While social sharing helps you find like-minded individuals, it also puts you at risk of identity theft. Your profile contains sensitive personally identifiable information (PII). Hackers can do significant damage with identifiers, such as race, gender, home address, contact number or date of birth.

You don't have to stop using social media altogether - just filter your posts. Good practices like hiding your current location, turning off GPS, deleting your profile profile and posting less often will protect your social media accounts from hackers.

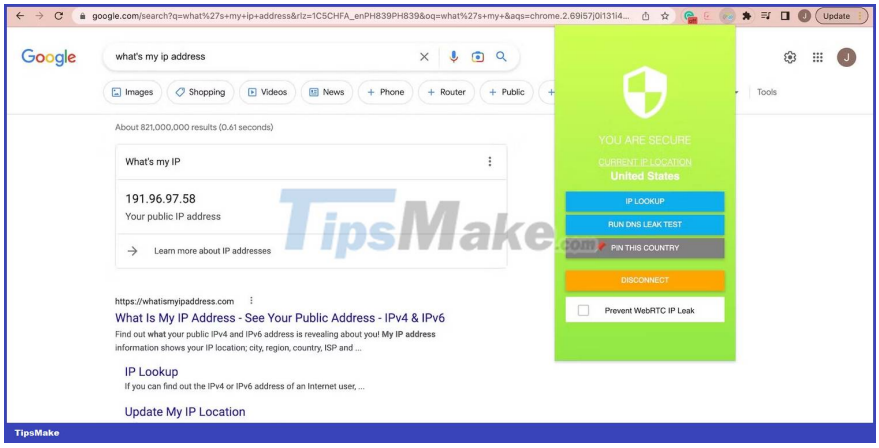
2. Skip backing up data in important files

Many people often skip backing up data. They find the process tedious and don't want to bother with it at all. Making copies of files can take anywhere from a few seconds to over an hour, depending on their size.

While this process may sound unappealing, it is essential. Data backup solutions help combat a number of cybersecurity threats, including data breaches, ransomware attacks, IT system failures, and data corruption. Personal and work files both need backup.

Instead of delaying backing up your data, discover ways you can overcome bottlenecks and roadblocks in the process. Focus on speeding up file copying and moving. You can automate migrations through secure cloud storage systems, use lightweight data backup programs that run in the background, and delete redundant files.

3. Blindly trust free VPN service providers

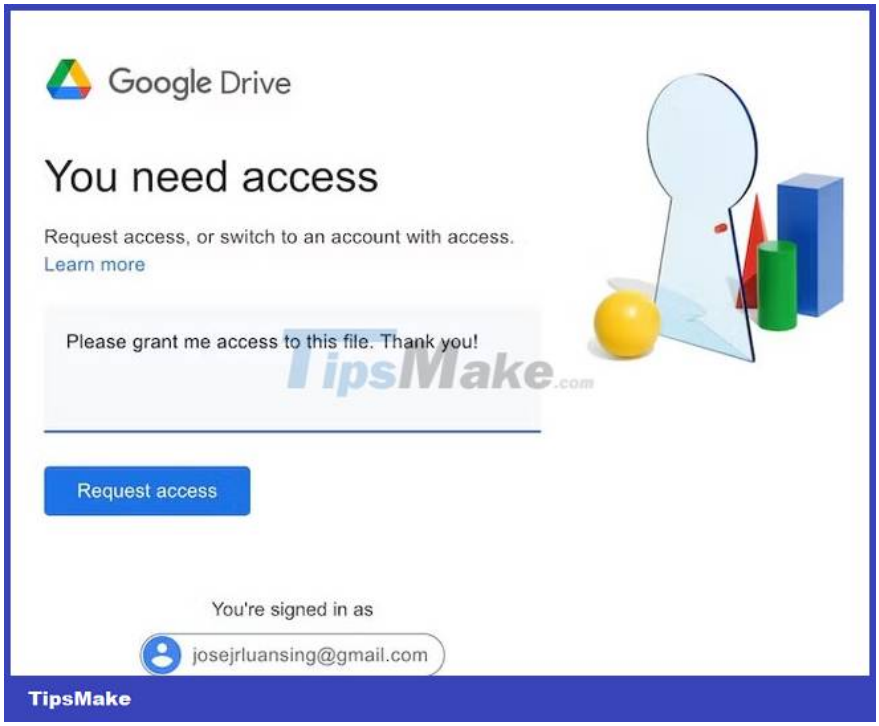


People often use free VPNs for accessibility and cost savings. Instead of paying for a premium VPN, you can simply download and install free alternatives if needed. Setting up an account takes a few minutes. You can even create new accounts every time you encounter geo-restricted content.

While free VPNs are convenient, they also pose a security risk. With relatively weaker encryption keys and reused dirty IP addresses, they won't effectively hide your online identity. Cybercriminals are skilled enough to crack basic encryption methods.

Of course, you can still use reliable, trusted free VPNs, but be aware of their limitations. They are great for bypassing geo-restrictions. But you should consider more sophisticated, premium options to secure your online identity.

4. Unlimited access to specific files



Data management is mainly based on file access control. Regulate who accesses your data and how they modify it to prevent data breaches. After all, cybersecurity threats like theft, account takeover, and accidental disclosure often stem from unauthorized access.

Although access control is extremely important, many people tend to ignore it. They are unaware of the severity of the account hijacking or are inconvenienced by the steps involved in setting up the permission restriction process.

As a rule of thumb, make your documents private by default. Get in the habit of adjusting user accessibility when sharing files, whether for work or personal purposes. Only grant access to authorized users.

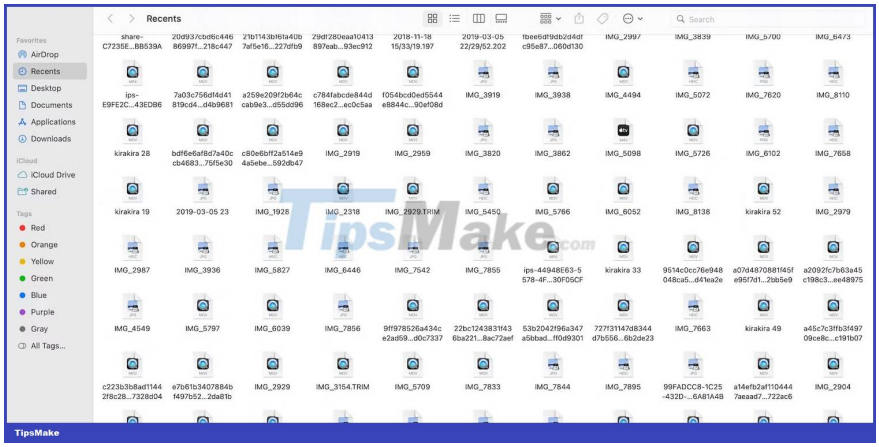
5. Open work software and files on personal devices

Like many remote workers, you can sometimes mix personal and company-issued devices. This is extremely common but very risky. Even seemingly innocuous actions like accessing Facebook on your work laptop or sending office documents via smartphone carry some cybersecurity risks.

Stop opening work files on your personal devices and vice versa. Smartphones or laptops don't have complex security systems like those set up by the company. If a data breach occurs, you will be held responsible.

In addition, company-issued devices are regularly scanned by time tracking and employee monitoring tools. They take scheduled screenshots, track app usage, and share screen activity. You may not feel comfortable when your employer gets to know your personal issues better.

6. Excessive hoarding of files and software programs



Digital clutter is a common problem these days. Even tech-savvy people tend to hoard old folders and files that they haven't accessed in years. Some keep them for emotional reasons, while others don't bother to categorize the data.

Either way, hoarding digital files puts you at risk of cyberattacks, so you should try to keep your digital life organized. Start with small changes like deleting old files. Move them to the cloud, then delete their original copies on your local servers. You can even encrypt them for extra security measures.

7. Do not track file access history and logs

Users rarely track their file access history. Modern day employees deal with dozens of files - keeping track of everyone's access to data is not an easy task.

Although reviewing file history is time-consuming and expensive, it plays an important role in any cybersecurity strategy. Addressing a data breach begins with preventing unauthorized access. If someone takes over your files, report them immediately to the appropriate channels.

Most platforms provide basic logging functionality. For example, Microsoft 365 (i.e. Office) records file edits, the storage system displays the user's access history, and the cloud server tracks file uploads/downloads.

But if you need more extensive tracking, use third-party apps. Options like LEO Privacy Guard and FileAudit can provide additional user access data on your local and cloud servers.

You finished reading the article "**7 security mistakes you often make**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.