

9 common mistakes about technology need to stop immediately

As Ben Parker (the fictional character, Spider-Man's uncle) once said: The greater the power, the higher the responsibility, and the power of today's technology is so easy to grasp and use that they are I often forget that. So it's time for you to take responsibility and don't make 9 common technological mistakes like below!

We are all living in a society completely covered by technology. Not knowing how people feel, but there must be many people who cannot live without technology - because it is both passion and really necessary for their lives. As **Ben Parker** (*Spider-Man's fictional character*) once said: " *The greater the power, the higher the responsibility* ", and the power of today's technology is too easy to grasp and use. so we often forget that. So it's time for you to take responsibility and don't make **9 common technological mistakes** like below!

1. Share passwords for all accounts



Target, Adobe, Facebook, LinkedIn and Snapchat are among the big companies that have a database of customer information that has been compromised. If you are in the habit of sharing your username / password for all accounts, it is not helpful to change the password on a website. Because it is easy to find your login information in one of the hacking cases and use it to access any account that you share information with.

Therefore, shuffle the passwords and never reuse a password twice. This may sound difficult but you just need to choose a basic word like " *password* " and change it. For example, the Google password could be " *pA55w0rd1* " and the Facebook password could be " *pA55w0rd2* " to remember both easily without losing security. Also, you can see more tips on setting up passwords here: Summarize some of the safest ways to create and manage passwords

2. Do not use 2-step authentication

Signing in with 2-step verification



Speaking of passwords, it is no longer safe now. If you access any of your devices (*either directly or via the network*) , you can install keystroke tracking software and get all your passwords. Therefore, using **2-step authentication** will make this game more difficult to implement.

All major services (*Facebook, Google, Twitter, etc.*) all have 2-step authentication in some way and, if careless, you won't use them. Set up your accounts by sending a message to your phone, asking for a confirmation code, etc. when you have access from your source other than your personal or home network.

3. Connect to a public network without using a virtual private network (VPN)



Many large companies and organizations often use public Wi-Fi, including McDonald's, Starbucks, airports and gyms. However, using this public network will " *open the door* " of your computer to anyone online - like putting your wallet next to you while sleeping in the park bench.

Virtual private networks or VPN (*virtual private network - networks dedicated to connecting computers together via the public Internet*) keep information secure when using public networks. If you don't want to attend a *social* party with strangers without using " *safety protection* ", don't connect to the public network without using VPN.

1. 11 best VPN software

4. Do not update the software



In 2011, Sony PlayStation Network was hacked and personal information of all PlayStation users (*stored in a non-encrypted database*) was revealed. This happened a month after Sony missed an important Apache server upgrade. **Updating the software** is essential, so companies create continuous software to fight and patch security holes. If you don't update the software at least once a week, your data is at risk of being violated.

1. How to check and update the version of Android operating system in use

5. Disable "firewall - firewall" and antivirus software

Internet Security



In the computer network industry, *firewalls* are barriers that some individuals, organizations, enterprises and state agencies set up to prevent access to unwanted information from outside to the network. internal, as well as preventing the security information located on the internal network from being exported without permission. In addition, a firewall is a hardware device or software that operates in a networked computer environment to prevent a contact that is banned by an individual or organization's security policy, similar to Operation of fire barrier walls in buildings.

However, sometimes the firewall makes you feel uncomfortable - this is especially true for gamers and users of streaming data services, such as Netflix Hulu and Amazon Prime. It can disable your security software for easy access to your favorite websites, but that only makes things worse.

Instead, set specific rules for each page. This will take time for the first few days but its protection for your computer is extremely valuable. You can use security software like AVG (*antivirus software for desktops or laptops*), ZoneAlarm (*desktop or laptop firewall*) and Lookout Security (*antivirus software*) / *firewall for smartphones / tablets*), all with a free version.

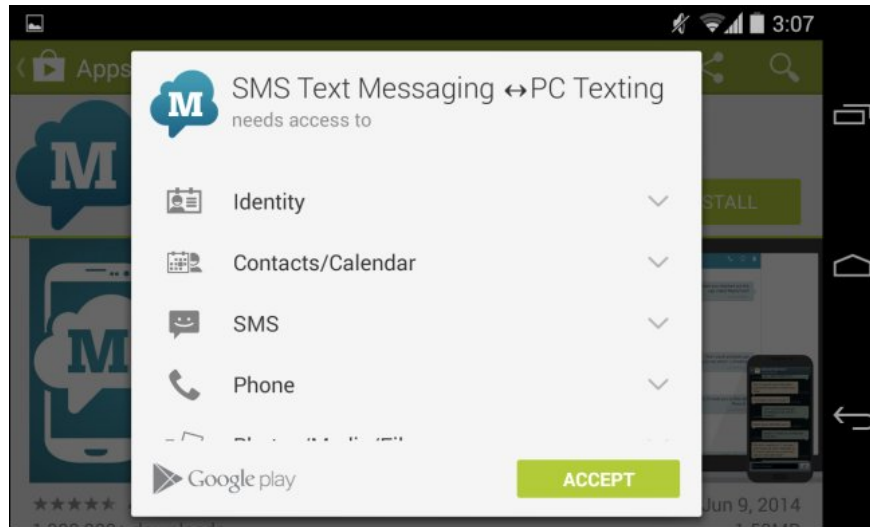
6. Ignore privacy settings on social networks



Facebook requires real information, so is LinkedIn and Google+. You can use some personal information (*basic demographic information, work history, etc.*) but don't show it all. **Right now privacy** is an unclear and best notion of caution. Surely no one wants others to use their personal information on social networks to resist themselves? This is especially dangerous for women who are being watched online at an alarming rate.

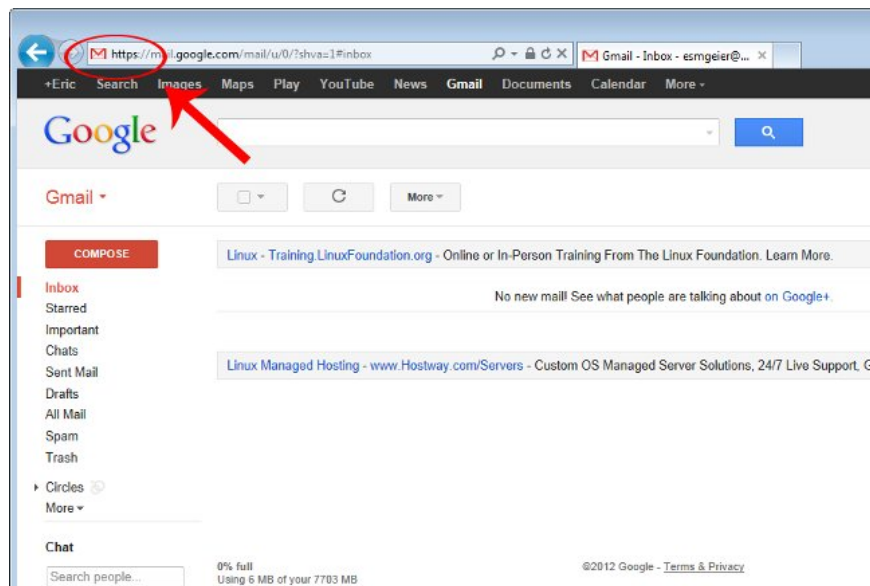
1. 5 Facebook privacy settings you should know

7. Skip the permission to use the application



Talking about the use of personal information, pay close attention to what consent allows when installing applications and games on mobile devices or when using social networking accounts to log into any any service period. The game **Candy Crush** doesn't need a satellite *positioning* (*Global Positioning System - GPS*); The Huffington Post newspaper doesn't need to know who your friends are and **Flappy Birds** does n't have to watch your phone book. Learning to say " *No* " is one of the important skills you can have - start with the software and continue with others.

8. No email encryption



Do you still remember the post office? The day before to send a message to someone, the postman had to go barefoot, up and down the hill on a cold day. Today we have a habit of sending email - email is essential, but keeping the postman image in mind is still important.

Email is not a letter - it is a postcard, and everyone can see the message on it. When encrypting email with the encryption method Pretty Good Privacy (PGP), you sealed the postcard in the same safe envelope that governments and corporations on the planet use. This method is 100% free. It is true that there is no reason for you not to do that.

9. No smartphone protection



Smart phones are so ubiquitous in today's life that we naturally admit it. They are computers, filled with your private personal information. When exchanging for a new phone, be sure to delete the personal information first. It's not just a deletion, you need to use the " *One Pass Zero* " method. This method not only deletes the data but also overrides with a string of zero (*remember that digital data in the single form is 0 and 1*).

It is similar to writing a note with pencil and paper. When you erase the pencil, you still see what you wrote. But if you write it all over the deleted part, it's much harder to see, right? If you have enough time and effort, do the deletion more than once, but the " *geniuses*" at the Apple store don't have those " *resources* ". However, if you don't do it, you'll end up like one of this Apple horror stories.

The Internet is a great place, but it is also very dangerous. Before going online, protect yourself and your data. You will not want the rent or mortgage repayed because someone hacked the server, or an application you downloaded and used for 5 minutes, to release personal information of all users online for others use.

Refer to some more articles:

1. 35 inventions that make your life easier
2. 15 habits of wasting time need to be removed immediately
3. Top 10 IT jobs with the highest salary in the future

Having fun!

You finished reading the article "**9 common mistakes about technology need to stop immediately**" 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.
