9 things you should never do when using public WiFi

The best way to stay safe when using public WiFi is to avoid doing anything that might give hackers what they're looking for.

Public WiFi seems like a necessity in the modern world but few people realize the level of security risks it poses. If you're using an open network, you're a hacker's dream. Whether you're casually browsing the web or trying to get a little work done, there are some things you should never do when using a public WiFi connection.

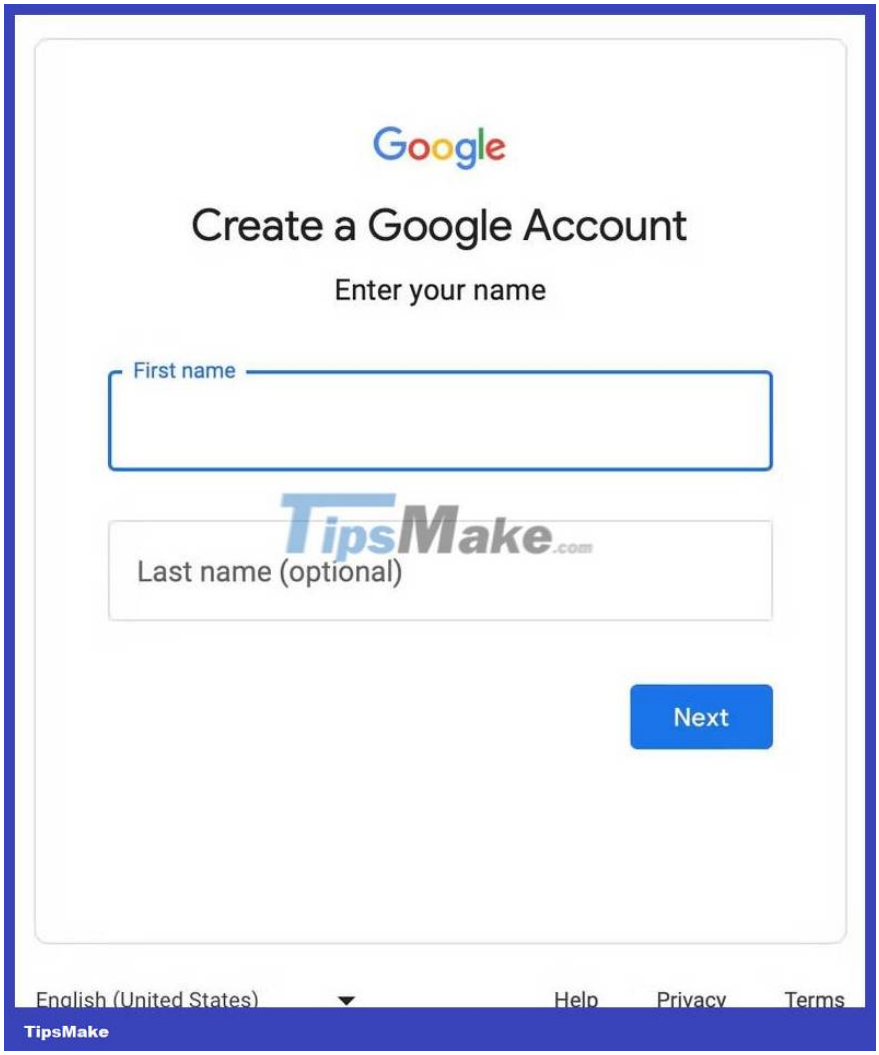
The best way to stay safe when using public WiFi is to avoid doing anything that might give hackers what they're looking for.

1. Don't log into anything that requires a password

The golden rule when using a public WiFi connection is to never send personal information: usernames, email addresses, passwords, etc. Hackers can intercept this data and gain access to your account. account or use your personal information in other attacks, such as identity theft.

Forget about logging into email accounts, social media sites, or anything else that requires a username and password. Using social media apps is generally safe - as long as you don't need to log in - but always remember that hackers could be on the prowl.

2. Don't create a new account



Signing into existing accounts is one thing, but creating new accounts while using public WiFi can give hackers the opportunity to access accounts from day one. This is especially dangerous if you fill in new account details: name, address, occupation, payment details, etc.

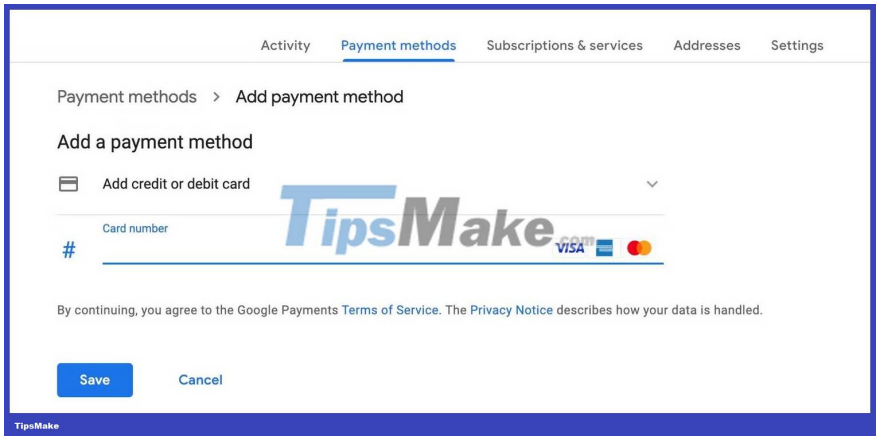
You should only use private, secure networks to create new accounts or do anything that involves sensitive information.

3. Don't verify your identity

From time to time, authorities, online services and others may ask you to verify your identity. Let's say you're traveling abroad, open your favorite social media app, and it asks for verification. This is a common security feature to verify that it is, in fact, you who is trying to access your account and not some stranger in a foreign country.

As tempting as it may seem, don't verify your identity using public WiFi - including the network at your hotel or Airbnb. You don't want to hand over any information used for identity verification to hackers (passports, government IDs, biometric data, etc.).

4. Do not submit payment details



Online shopping is the last thing you want to do while using public WiFi. Any payment details you enter during the checkout process are vulnerable to a variety of attack strategies: Phishing, keystroke logging, transaction manipulation, etc.

If you really need to buy something, use mobile data and create a hotspot with your phone if you want to connect to another device. Even if you are traveling in another country, it is better to buy a local SIM card or check how much roaming charges are for a short period of time or less to submit your payment details safely.

5. Do not use online banking

If there's anything more dangerous than giving hackers your payment information, it's giving them open access to your bank account. This is where cybercriminals can transfer all your money to one of their accounts – not something you want to risk.

Above all, never log into online banking through a web browser using public WiFi. Native mobile banking apps are significantly more secure than websites and web apps but they are not 100% secure.

Most importantly, make sure you are using the official app because clone apps are one of the most common strategies for account hacking. Always download your banking app and set up/log in to your account the first time on a secure network. Take advantage of your bank's mobile security features, including two-factor authentication and any other features they offer to protect you.

Even with the latest security features enabled, the only safe way to do online banking is to use a secure network. You don't want hackers to get your account number, sort code, bank balance or any of the digits in your password, right?

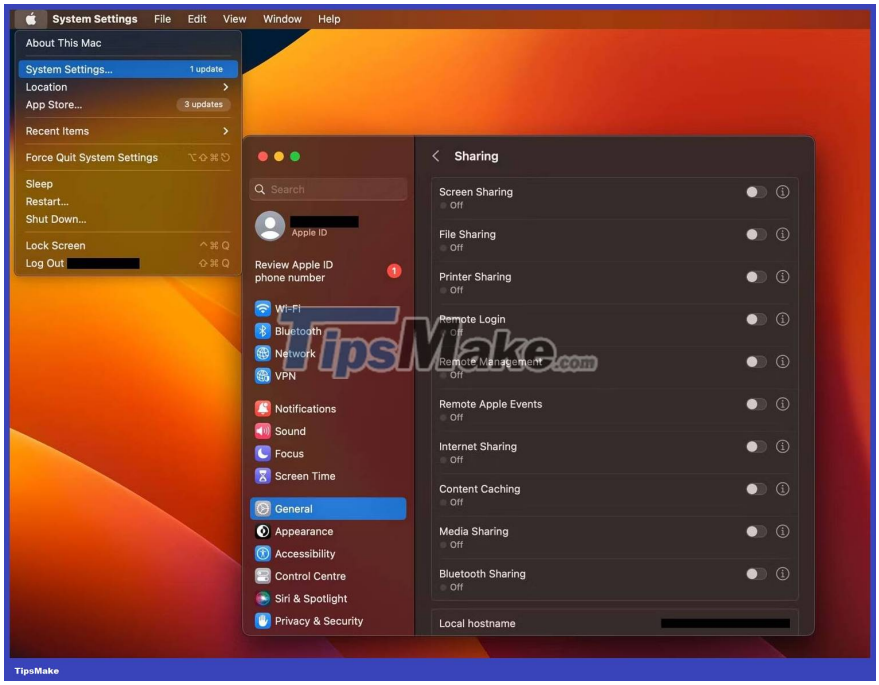
6. Don't work remotely

Remote working became a popular trend during the height of the COVID-19 pandemic. Unfortunately, inexperienced (and many experienced) remote workers may not understand the security risks of working online using networks outside the workplace.

Hopefully working from home isn't too much of an issue if your network is private and secure. However, as soon as you go to a coffee shop or co-working space, you are relying on a public, unsecured Internet connection. This is also the type of network that cybercriminals like to target, especially now that remote working has become

more popular.

7. Do not share files



There are two types of file sharing you should avoid when using public WiFi. First, you'll want to disable any file sharing settings on connected devices because hackers can exploit these settings to access files and folders.

For example, if you're using a macOS device, you can click the Apple menu icon and select **System Settings** > **General** > **Sharing** to see all the sharing settings that are currently enabled.

Turn off any sharing options you can to prevent others on the same network from accessing files and other data from your device.

Another type of file sharing you want to avoid is manually sharing files online with other users. For example, if you're using an app like Google Drive, wait until you can access a secure network before sharing any files - using the file sharing feature in Drive or other other media (for example, email attachments).

8. Do not access sensitive information or systems

This is one of the most difficult things to avoid when using public WiFi because we are so used to accessing and using sensitive information online. This includes the data you actually enter (username, password, payment details, etc.) but can also include anything visible on your screen such as email addresses, ID numbers and test results, even if you don't enter any data.

Simply accessing a system that stores sensitive information - such as the apps you use for work - is all a hacker needs to start spying. This includes checking your email inbox. Depending on the type of attack the hacker is performing, they can view email addresses, contact information, and message content. With the right type of attack, hackers can get just one purchase confirmation email and enough personal information to steal an

identity.

9. Don't leave your device unattended

Never leave any device unattended in a public place, especially if it is connected to an open network. Laptops, phones, and storage devices are gold mines for hackers. Even if they don't steal your device while you're away, you don't know what the hackers might have done with it when you return.

You finished reading the article "**9 things you should never do when using public WiFi**" 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.
