Using Public Wi-Fi Networks

From the Office of Minnesota Attorney General Lori Swanson

In today's digitally-connected world, public Wi-Fi networks—also called Wi-Fi hotspots—can be found in nearly every kind of public space, including airports, hotels, schools, restaurants, and coffee shops, to name a few. While these networks offer free and convenient access to the Internet, many people do not realize the risks of using them. In some cases, for example, other network users may be able to watch your activity online and obtain your passwords and account information, which may put you at risk of theft or identity theft.

How Can Someone Get My Information Using Public Wi-Fi Networks?

Public Wi-Fi networks that allow people to join anonymously are an ideal environment for hackers looking to steal other people's money and information. People with minimal computer experience can download free software on the Internet to monitor your web browsing activity and view anything that appears on your device's screen while using the public Wi-Fi network. In addition, hackers may use public Wi-Fi networks to remotely access people's smartphones, tablets and computers to install malware or spyware that can transmit information from the device directly to the hacker.

What Information is at Risk?

The short answer is almost everything on your device, from user names, passwords, and e-mail addresses to the apps installed, credit card and bank account information, Social Security numbers, and birth dates. A hacker can acquire a large amount of information about you in an instant. If a hacker acquires your account credentials (user name and password), this information may be used to steal additional information or money from your accounts.

What Can I Do To Protect Myself?

Use the Most Secure Network Available.

If you must use a public Wi-Fi network, choose the most secure network available. Never assume that a network is secure. If you are not sure whether the network is secure, ask an employee. Common secure network types include WEP, WPA, and WPA2 (the strongest). While encrypted networks offer more protection than unsecured networks, they are not a guarantee that your device and information will be safe while using the network, as some hackers may be able to bypass a secure network's encryption methods.

Use Encrypted Websites.

If you send personal information through a website using a public Wi-Fi network, make sure the website is encrypted. Encryption simply means that the information sent through the website is converted to a jumbled code that reverts back to its original state once it reaches its destination. This makes it more difficult for other network users to make sense of the information being sent from your computer. You can determine whether a website is encrypted by looking at the website address. If it begins with "https," then it is encrypted. Remember that the "s" stands for "secure." Make sure that you check for encryption on every page where you send or receive information—even within the same website, as some pages may be encrypted while others are not. An encrypted website will protect only the information sent and received through that particular website.

Protect Your Device.

Make sure that your computer software is up to date and never turn your firewall off. Use security software and firewalls, and keep them updated. Your computer will notify you when an update of the software is available. You will also want to install antispyware/antimalware software. Several reputable products are available online for free or have a free trial period. Beware of scams that attempt to lure you into disclosing your personal or financial information or that direct you to download programs that may contain malware with the ability to drain private information from your computer.

Identify any public Wi-Fi network that you connect to as a "Public Network" and turn off file sharing on your computer. It can also be helpful to disable your wireless connection if you are using your device in a place with a public Wi-Fi network and do not need Internet access.

You may wish to consider using a virtual private network ("VPN"), which encrypt information between your device and the Internet. It can also be helpful to install certain add-ons or plug-ins through your web browser that add encryption to some more well known websites using the browser. Check with the specific web browser you use for more information.

A Word On Mobile Phones and Apps

Unfortunately, mobile apps are not always encrypted, and when they are, the information may not get encrypted correctly. Therefore, it can be best to avoid using mobile apps for relaying important information on public Wi-Fi networks altogether. If you have to use a mobile app to send sensitive information, only use Wi-Fi networks you know are secure or a 3G or 4G network. Some smartphones have a feature that will automatically connect them to any available network. Turn off this feature in the phone's settings, or turn the phone to "airplane mode."

Overall Tips:

When you consider joining a Wi-Fi network, keep the following in mind:

- Don't assume that a public Wi-Fi network is secure (many are not).
- The best place to make financial transactions or use sensitive information is on a secured home connection. If you must use a public Wi-Fi network to conduct sensitive transactions online, look for "https" websites and be alert to any warnings you receive from your web browser. If your using a mobile device, it may be more secure to use your cellular network.
- If you log-in to an account using a public Wi-Fi network, sign out as soon as you are done using the account. Otherwise, someone could access your account long after you were accessing it.
- If you are using your device but not accessing the Internet, disable your computer's wireless connection and put your phone in airplane mode.
- Use strong passwords, and vary them between your accounts. Using the same password for multiple accounts makes it easier for hackers to access several of your accounts.
- Keep your operating system, antivirus software and web browser up to date. Never update them using a public Wi-Fi network.
- Never turn off your firewall.
- Some tablets and smartphones have a feature that will automatically join available networks. If you have a device that does this, turn this feature off.

Steps to Take if Your Online Account is Hacked

You might not realize your online account was hacked right away. Once you discover the intrusion, however, take the following steps:

1. Change your password immediately. Hackers may change your password, preventing you from accessing your account. If you are unable to access your account, contact the website directly and it can assist you in restoring your account.
2. If the hacked account contains financial information, contact your bank or credit card companies immediately. Let them know that your account may have been compromised. Your bank or credit card company may issue you a new card or account number. Monitor the activity on the account for any fraudulent transactions. In some cases, hackers may not use your information right away, so it can be helpful to regularly monitor your account, especially if you are not given a new card or account number.
3. Contact your friends and family to let them know your account has been hacked. Hackers may try to gain access to your e-mail contact list and send e-mails from your account purporting to be from you. Notifying family and friends that your account has been compromised may help them protect them from hackers.

For additional information, contact the Office of Minnesota Attorney General Lori Swanson as follows:

Office of Minnesota Attorney General
Lori Swanson
1400 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101
(651) 296-3353 or 1-800-657-3787
TTY: (651) 297-7206 or 1-800-366-4812
www.ag.state.mn.us