SECURITY Smart™
NEWSLETTER
SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Think Twice Before Connecting to Public Wi-Fi

THOUGH IT'S GENERALLY BEST, to avoid public Wi-Fi, you might run into a situation where your work simply cannot wait and your only option is to use an unsecured, free Wi-Fi hotspot. If that happens, understanding the risks of public Wi-Fi may prevent you from falling victim to an attack.

One of the primary threats with free Wi-Fi is that hackers can position themselves between you and the connection point, so instead of communicating directly with the hotspot, you end up sending your information to the hacker. The hacker also can access all the information you send out—emails, phone numbers, credit card numbers, business data. Once a hacker has that information, you've basically given away the keys to the kingdom.

Remember that anything you do on a public Wi-Fi network is not secure. If you absolutely must connect to Wi-Fi (first, ask yourself if you really need to connect) here are a few safety tips:

1. Do not touch any of your personally identifiable information (PII).
Avoid touching any PII including banking information, Social Security numbers, and home addresses at all costs. Remember, some accounts require you to enter details like phone numbers when you sign up, so even though you may not remember entering it, you may inadvertently be allowing access to personal information.


PeopleImages / Getty Images

2. Use virtual private networks (VPN) instead of Wi-Fi.
A VPN allows you to create a secure connection to another network over the internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more. While they do cost some money, the peace of mind and additional security are well worth it. Ask your IT department if your employer can equip you with a way to connect to a VPN when you're on the go.

3. Use SSL connections.
If you don't have access to a VPN, you can still add a layer of encryption to your connection. When browsing the internet, be sure to enable the "Always Use HTTPS" option on websites you visit frequently. Most websites that require an account or credentials have the "HTTPS" option somewhere in their settings.

4. Invest in an unlimited data plan.
People often connect to public Wi-Fi networks to avoid overage charges on their phone bills. But your mobile is just as likely to be attacked as your laptop, if not more. Investing in an unlimited data plan will not only eliminate your need to access insecure Wi-Fi networks, it will also often allow you to use your mobile device to create a personal internet "hotspot," so you wouldn't need a VPN connection.

5. Turn off file sharing.
File sharing is usually easy to turn off from the system preferences or control panel. Or let Windows turn it off for you by choosing the "public" option the first time you connect to a new, unsecured network.

CSO FROM IDG Security Smart is published by CSO, the leader in news, analysis and research on security and risk management.
To purchase an individual subscription, email **securitysmart@idg.com** or **marketing@idg.com** for more information.