Free! Public Hacking

How often do you see signs for free wifi access and charging stations for your mobile devices? These amenities are available for your convenience in many public spaces like coffee shops and airports. Unfortunately, cybercriminals love free wifi and charging stations, too. Cybercriminals can hack into public wifi networks and charging stations to steal your sensitive information.

Public Wifi

Cybercriminals can gain access to a public wifi network with a fake access page phishing scam. This fake access page will prompt you to put in personal information like your name, email address, and phone number. If you share this information with cybercriminals, they can target you in future scams to steal more sensitive information, such as your credit card number or passwords.

Public Charging Stations

Cybercriminals can use charging stations to access your device. While charging stations may seem convenient and harmless, cybercriminals can load malware onto public USB chargers. If you plug your device into the infected USB charger, cybercriminals will be able to look at and download your personal data, such as saved passwords. If you enter your login credentials, cybercriminals will use them to access your accounts and steal your sensitive information.

What Can I Do to Stay Safe?

Follow the tips below to stay safe from public wifi and charging station scams:

- Be careful using your mobile device when connected to public wifi. If you need to enter or review sensitive information, disconnect from the public wifi.
- Never plug any public charging accessories into your mobile devices. Instead, bring a spare device charger or battery with you for emergencies.

Stay Safe While Working in Public Locations

It's important to protect your information from cyberattacks no matter where you are, especially when working at the airport or a local cafe. If you don't follow your organization's cybersecurity practices while working in a public location, cybercriminals can steal your information when you least expect it.

Follow the tips below to protect your information from cybercriminals while working in public locations:

Only join safe networks.

- Only join safe Wi-Fi networks. Don't allow your devices to automatically connect to public Wi-Fi networks, and don't connect to random hotspots.
- Disable Bluetooth on your devices when you aren't using it. Don't allow unauthorized devices to connect to your device via Bluetooth.

Be cautious when in public.

- Avoid using public charging stations or chargers that you find lying around. Cybercriminals can use fake charging cords or USB plugs to upload malware onto your device. It's best to use your own chargers when possible.
- Don't use public computers to work on important projects. Many public locations such as hotels have "business centers" with computers that you can use for free. These computers may contain keyloggers or other malware, so use them with caution.
- Look out for fake QR codes, or "quick response" codes. Public locations such as restaurants or airports may prompt you to scan QR codes for deals and offers. cybercriminals can embed malicious URLs into fake QR codes, which could result in malware being downloaded onto your device.

Protect sensitive information from bystanders.

- If you need to make a business call in public, be sure to use headphones. Don't allow bystanders to overhear sensitive work information.
- Turn screens away from public view when possible. Don't leave sensitive information on your screen for long periods of time.

- Don’t leave your devices unattended. If you need to use the restroom or step away for a moment, take your belongings with you so that cybercriminals can’t steal them.

Protect Your Computer While Using Public WiFi

Using free public WiFi at a coffee shop or an airport may be convenient, but it can also be dangerous. Most public places that offer free WiFi don’t use encryption to secure their WiFi networks. It’s important to remember that when you connect to public WiFi networks, you will be sharing the networks with other people.

Some technology allows you to view the wireless computer communications that are within range of your device. Unfortunately, cybercriminals can use this technology to see what you do on your devices, as well as the data you share with websites.

However, there are a couple of precautions you can take to help protect your devices while connecting to public WiFi networks:

- Look for website URLs that include HTTPS at the beginning of the URL. The “S” at the end of HTTPS means “secure.” These types of websites are encrypted, which helps protect your information.

How Secure is Your Mobile Device?

Most of us have a smartphone, but how many of us really think about the security threats faced by these mobile devices? Mobile devices are vulnerable to many different types of threats. The bad guys are increasing attacks on mobile devices and targeting your phone using malicious applications. Using these methods, they can steal personal and business information without you having any idea what’s going on.

Even if you’ve downloaded a security or antivirus application, securing your smartphone goes beyond these services. Improving your mobile security practices is your best defense against the privacy and security issues associated with your mobile device.

How can I improve my mobile security practices?

Always remember these best practices to minimize the risk of exploits to your mobile devices:

1. **Ensure your phone's operating system is always up to date.**
   Operating systems are often updated in order to fix security flaws. Many malicious threats are caused by security flaws that remain unfixed due to an out of date operating system.
2. **Watch out for malicious apps in your app store.**
   Official app stores regularly remove applications containing malware, but sometimes these dangerous apps slip past and can be downloaded by unsuspecting users. Do your research, read reviews and pay attention to the number of downloads it has. Never download applications from sources other than official app stores.
3. **Ensure applications are not asking for access to things on your phone that are irrelevant to their function.**
   Applications usually ask for a list of permissions to files, folders, other applications, and data before they're downloaded. Don't blindly approve these permissions. If the permission requests seem unnecessary, look for an alternative application in your app store.
4. **No password or weak password protection.**
   Many people still don't use a password to lock their phone. If your device is lost or stolen, thieves will have easy access to all of the information stored on your phone.
5. **Be careful with public WiFi.**
   The bad guys use technology that lets them see what you're doing. Avoid logging in to your online services or performing any sensitive transactions (such as banking) over public WiFi.

Holiday Travel

Have you ever been on a trip and realized that you forgot to pack something important? It's easy to overlook things during the hustle and bustle of traveling, especially during the holidays. Unfortunately, cybercriminals take advantage of this busyness to target

holiday travelers. Their goal is to catch you off guard when or where you least expect it. Don’t let cybercriminals ruin your holiday plans! Follow the tips below for safe travels:

Secure your devices when they are not in use.

Never leave your phone, tablet, or computer unattended. Try to take your device with you wherever you go. If you do need to step away, lock your device. Then, ask a trusted friend or family member to keep your device safe while you’re gone.

Use strong passwords.

Use strong passwords for all your devices, apps, and services! Don't forget to include the apps and services that you only use while traveling, such as hotel websites and translation apps. For added security, many apps allow you to use biometric identifiers instead of a password. If your device has a fingerprint scanner or facial recognition, set up this feature before leaving on your trip.

Beware of public Wi-Fi networks.

Always disable the option to automatically connect to Wi-Fi networks on your phone, tablet, or computer. Instead, manually choose which network you'd like to join. Only use Wi-Fi networks that you know are safe, and never connect to random hotspots.