Apr 15, 2022

Contact Kylie Mason

Phone 850-245-0150

OFFICE OF ATTORNEY GENERAL ASHLEY MOODY

Stronger, Safer Florida

Attorney General Ashley Moody News Release

CA: Using Public Wi-Fi can Expose Personal Information

TALLAHASSEE, Fla.—Attorney General Ashley Moody is advising Floridians to refrain from using public WiFi when accessing personal and financial files or apps online. There are a multitude of ways hackers take advantage of public Wi-Fi, but all are easily avoidable if the correct precautions are taken by citizens. Attorney General Moody is informing Floridians about common public Wi-Fi hacks and providing tips on how to avoid them.

Attorney General Ashley Moody said, “Public Wi-Fi networks are commonly offered by businesses, restaurants and other locations catering to visitors. Unfortunately, these networks are often unsecure, and hackers can take advantage of vulnerable connections. Be cautious when using public Wi-Fi networks to prevent hackers from stealing your personal and financial information.”

Although there are many scams associated with public WiFi, the AARP notes the two most common are the Evil Twin Attack and the Man in the Middle Attack. The Evil Twin Attack is when a hacker creates a Wi-Fi network with a similar name as the public Wi-Fi a business offers. The Man in the Middle Attack is when a hacker lines up between a user and the network router and intercepts data. Both schemes give hackers the ability to track online movements and sift through a victim’s device in search of personal or financial information.

To stay secure when using electronic devices away from home, Attorney General Moody recommends Floridians to remember the following tips:

- Never access apps that contain personal or financial information;

- Do not stay permanently logged in to accounts—even if an app is running in the background, a hacker could still access the information;
- Use a cellular connection if accessing information is necessary;
- Only access websites that begin with ‘https’ rather than ‘http’—the ‘s’ stands for secure—or have a padlock next to the URL; and
- Research and install browser-encryption features.

The Federal Trade Commission provides additional tips on how to safely use public Wi-Fi networks. For more information, click here.

To report public WiFi scams, or identity theft as a result of a public Wi-Fi scam, visit the FTC’s Identity Theft website, or call (877) 438-4338.

# # #

The Florida Attorney General's Consumer Protection Division issues Consumer Alerts to inform Floridians of emerging scams, new methods used to commit fraud, increased reports of common scams, or any other deceptive practice. Consumer Alerts are designed to notify Floridians about scams and available refunds in an effort to prevent financial losses or other harm caused by deceptive practices. Anyone encountering a scam should report the incident to the Florida Attorney General's Office by calling 1(866) 9NO-SCAM or visiting MyFloridaLegal.com.