Aug 16, 2022

Contact Kylie Mason

Phone 850-245-0150

OFFICE OF
ATTORNEY GENERAL
ASHLEY MOODY
Stronger, Safer Florida

Attorney General Ashley Moody News Release

CA: Spear Phishing--Businesses at Risk

TALLAHASSEE, Fla.—Attorney General Ashley Moody is issuing a Consumer Alert to warn Florida business owners about a recent increase in spear-phishing reports. There are already more reports of spear-phishing in the first half of this year than received during all of 2021. Spear-phishing is an advanced form of a phishing attack. While phishing attacks cast a wide net via a more generalized message sent to large groups of people, spear-phishing involves narrowly tailored messages using personal information and sent to an individual or smaller group of people—like employees of a specific business.

Often, these messages are designed to appear to be from a manager or company executive. Scammers will typically include the target's full name, title and an urgent message that distracts the target. Often, these messages contain or have links to malicious viruses designed to steal corporate data, usernames, passwords and personnel records.

Attorney General Ashley Moody said, "Spear-phishing attacks are individualized and more specific than the more common scam messages we see—and that is what makes them more dangerous. As we see an increase in reports of these types of cyberattacks, businesses need to make sure team members are trained to spot and report suspicious messages immediately—to protect themselves, the company and its customers."

The following are 10 tips for Florida businesses to help guard against spear-phishing attacks:

1. Train employees in security principles. Establish basic security practices and policies for

employees, such as requiring strong passwords, or issuing penalties for violating company cybersecurity policies. Have employees double-check the sender's address of a suspicious email before clicking any links. Put in place rules of behavior describing how to handle and protect customer information and other vital data.

2. Protect information, computers and networks from cyberattacks. Using the latest software, web browsers and operating systems are the best defenses against viruses, malware and other online threats. Make sure antivirus software conducts scans of the device after each update.

3. Provide firewall security for your internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the system’s firewall is enabled. If working from home, ensure that an employee’s home system is protected by a firewall.

4. Create a mobile-device action plan. Require employees to use passwords, encrypt data and install security apps to prevent criminals from stealing information while the phone or mobile device is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. Make backup copies of important business data and information. Regularly back up the data on all computers. Backup data automatically if possible, or at least weekly, and store the copies either offsite or in a cloud program.

6. Control physical access to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops in particular can easily be lost or targeted for theft so secure them when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted information-technology staff and key personnel.

7. Secure Wi-Fi networks. To hide a Wi-Fi network, set up a wireless access point or router so it does not broadcast the network name. Protect access to the router by requiring a password.

8. Employ best practices on payment cards. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. Isolate payment systems from other, less-secure programs and do not use the same computer to process payments and browse the internet.

9. Limit employee access to data and information. Limit authority to install software.

10. Passwords and authentication. Ensure employees use unique passwords and require workers to change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.

If money is lost to a spear phishing scam, immediately contact local law enforcement. Additionally, cybercrimes can be reported to the Federal Bureau of Investigation’s Internet Crime Complaint Center.

Additional cyber security alerts, tips and guidance can be found on the websites of the Florida

Department of Law Enforcement and the Federal Trade Commission.

To view other recent Consumer Alerts, visit Attorney General Moody’s Consumer Alert webpage at MyFloridaLegal.com/ConsumerAlert.

# # #

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.