Apr 20, 2022

Contact Kylie Mason

Phone 850-245-0150

OFFICE OF THE ATTORNEY GENERAL STATE OF FLORIDA

Florida Attorney General's Office News Release

VIDEO CA: Victims Losing Millions to SIM Swap Scam Found in Florida

TALLAHASSEE, Fla.—Attorney General Ashley Moody is warning Floridians about a phone-based hacking scam that is increasing drastically. According to the Federal Bureau of Investigation, Americans nationwide lost approximately $12 million to SIM Swap scams in 2020. In 2021, the amount skyrocketed to more than $68 million, nearly a 500% increase.

The scam involves a scammer hacking an email account to acquire personal information, including the victim's phone number. They then contact the victim's service provider—convincing the carrier to reassign the victim's number to a phone the scammer controls. Once the number is assigned to the new device, the scammer not only has access to the content associated with the victim's phone but is now equipped to overcome some two-factor authentication barriers to gain access to banking, investment or other sensitive accounts.

Attorney General Ashley Moody said, "This is a frightening scam involving hackers who steal identities and quickly drain the financial accounts of their victims. SIM Swap scams are responsible for more than $80 million in losses nationwide in just the past two years. I am asking Floridians to take steps to avoid falling prey by protecting their email accounts with strong passwords and watching out for any unusual bank withdrawals or other suspicious online activity."

Anyone with a phone number is at risk of being victimized by a SIM Swap scammer. At least one Floridian, a Tampa resident, already lost thousands to the scam. Even the former CEO of Twitter, Jack Dorsey, fell prey to the hack and had an unauthorized tweet sent from his personal Twitter account.

To guard against a SIM Swap scam, Attorney General Moody recommends Floridians:

- Use multi-factor authentication for all accounts, including email accounts;
- Download a two-factor authentication app to generate one-time access codes directly to devices and do not use authenticator systems that call your phone number;
- Establish a strong PIN in order to access mobile carrier accounts;
- Consider using a mobile carrier security app to receive alerts about attempted accesses to an account; and
- Refrain, when possible, from providing or posting a cellphone number.

The number one sign that a victim is being targeted by a SIM Swap scam is no longer being able to make or receive calls or text messages. When this happens, find a working phone and call the carrier immediately.

Report attempted SIM Swap scams to local law enforcement, the mobile carrier and to the FBI's Internet Crime Complaint Center at IC3.gov.

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.