Aug 3, 2023

**Contact** Kylie Mason

**Phone** (850) 245-0150

OFFICE OF ATTORNEY GENERAL ASHLEY MOODY

*Stronger, Safer Florida*

# Attorney General Ashley Moody News Release

## VIDEO: SUMMER SCAMS SERIES: Attorney General Moody Warns About Screen-Sharing Scams


TALLAHASSEE, Fla.—Attorney General Ashley Moody is continuing the Summer Scams Series: Tech Traps with a warning about screen-sharing scams. An umbrella term, screen-sharing scams include banking, tech support and any scam where fraudsters trick targets into giving full remote access to their computer, allowing personal and financial information to be stolen. These scams often target seniors—sometimes costing the victims entire life savings. The Federal Bureau of Investigation tracks the origin of many of these scams to India, including this one scamming U.S. citizens out of more than $20 million, yet it is known to occur worldwide.

**Attorney General Ashley Moody** said, "As we continue our Summer Scams Series, it's important that Floridians know to never share their screens or access to their devices with anyone they don't know or trust. If scammers do get access, then they will be able to steal personal and financial information to enact all sorts of devastating schemes. To stay ahead of screen-sharing scams, check out our series at MyFloridaLegal.com."

Screen-sharing scams work like this: a target answers an illicit robocall, or online message, and connects with a scammer who claims to be a representative from a trusted business, such as a bank or technology company. The scammer then tells the victim that the account is compromised, and that the scammer will need to download screen-sharing software to help.

Once the screen-sharing software is downloaded, the fraudster receives full access to the victim's computer and can hack accounts, steal personal information and set traps to further the scam. The FBI's Boston division reports a 137% increase nationwide in losses from tech-support scams from 2020 to 2021.

Screen-sharing scams can be financially devastating. Once a victim agrees to share a screen, the fraudster will try to gain a victim's confidence and lay a trap to further the scam. One common scheme occurs when a scammer pretends to be giving a victim a refund and 'accidentally' sends more money than originally intended. The fraudster then brings up a second website displaying what looks to be the victim's bank account, but it's really a fake screen that has been tampered with to show a fake bank balance, 'proving' that they sent too much money. Taking advantage of the victim's generosity, the scammer pleads to have the money returned. If the victim goes through with the return, it will soon become clear that no money ever transferred, and the victim's money is now stolen. The scammer may also use that fake website to steal the login credentials of the victim, allowing total control of the account.

There are reports of fraudsters verbally berating seniors over the phone and schemes resulting in major losses from victims, like a Tamarac couple who lost $99,000 in life savings after falling victim to a screen-sharing scam.

To avoid screen-sharing scams:

- Never share your screen or allow remote access with a stranger—a bank will never need to access a screen to view account information;
- Avoid clicking on any suspicious links;
- Ignore unsolicited contact from supposed tech-support companies;
- Be aware that phone numbers and emails can be tampered with, making it look like a call is originating from a trusted source; and
- Verify the validity of a call that appears to come from a legitimate business by hanging up and calling the number listed on the company's website.

The Federal Trade Commission released resource guides with tips for consumers to stop unwanted robocalls. Floridians should report robocalls to the FTC online at FTC.gov/Complaint.

Victims of cybercrimes should report incidents to the Florida Department of Law Enforcement Computer Crime Center.

Anyone who receives an illegal robocall can file a complaint with the Florida Attorney General's Office online at MyFloridaLegal.com or by calling 1(866) 9NO-SCAM.

# # #

*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. To view*

*recent Consumer Alerts and for other information about avoiding scams, visit MyFloridaLegal.com/ConsumerAlert.*