Oct 29, 2020

Contact Kylie Mason

Phone 850-245-0150

OFFICE OF THE ATTORNEY GENERAL STATE OF FLORIDA

Florida Attorney General's Office News Release

Cybersecurity Awareness Month: Be Proactive to Prevent Cybercrime



TALLAHASSEE, Fla.—October is National Cybersecurity Awareness Month, and with the pandemic forcing more Floridians to work, learn and socialize online, Attorney General Ashley Moody is issuing a Consumer Alert to encourage hyper-vigilance as a host of new cybersecurity threats have emerged—from Zoombombing to imposter websites infected with malware. Floridians must prepare and be proactive to safely navigate this new and increasingly digital society.

Attorney General Ashley Moody said, “If 2020 has taught us anything, it is that we can use technology to keep moving forward when faced with unprecedented challenges. It has also reminded us that any major shift in behavior or advancement in technology will be exploited by criminals to deceive the public. That is why we must remain hyper-vigilant. In recognition of National Cybersecurity Awareness Month, I am asking all Floridians to be proactive and take steps to protect their identities and finances from hackers, scammers and other types of cybercriminals.”

As Floridians have seen throughout the pandemic, cyber scammers often target people through emails or text messages. Two common messaging scams are phishing scams and attachments embedded with malware. Phishing scams involve messages that appear to be from a trusted source, such as a family member, co-worker or bank, often requesting the recipient to send money to assist a family or friend, or to donate to a fake charity. These scams also commonly

ask the recipient to click on a link to provide a username and password or other personal information to allow the scammer access to the person's financial accounts or other protected information.

Malware scams involve messages with a link that, when clicked, will infect the user's computer with a virus. The scammer may then demand payment to fix the computer for the user or may provide the scammer with access to computer files that are used to steal the user's identity. Earlier this year, malware was used to link to a website that mimicked a legitimate map of COVID-19 cases—infecting the devices of countless, unsuspecting visitors with malware designed to steal personal information.



Figure 1. Screenshot of the malicious website "Corona-Virus-Map[dot]com" pretending to be a legitimate COVID-19 tracker.

To avoid common phishing or malware scams, follow these tips:

- Never open attachments in a message that comes from an unknown source;
- Do not click on links in any solicitation;
- Mark any suspicious messages as spam; and
- Keep security software installed and up to date.

Another cybersecurity threat that increased this year with more people utilizing video conferencing to conduct business meetings, classes and religious ceremonies during the pandemic is Zoombombing. Zoombombing occurs when hackers hijack internet video conferences, like those offered by Zoom. These hackers often present inappropriate, offensive material or otherwise disrupt the conference.

To increase privacy and guard against Zoombombing, Attorney General Moody encourages organizers to:

- Create separate passwords for each virtual meeting;
- Establish a waiting room for meeting participants;
- Lock down the meeting once everyone invited to attend has joined; and
- Avoid posting meeting links on social media or any other public forum.

In April, Attorney General Moody issued a Consumer Alert warning of the cybersecurity threat and provided tips for preventing Zoombombing. To view the warning, click here.

Many cybercriminals aim to steal Floridians' identities, hack into personal accounts or pilfer hard-earned money. Below are tips to help Floridians protect identities and financial information:

- Ensure the internet browser has a secure connection—a padlock should appear in the URL bar if the session is secure;
- Do not include personal financial information in an email;
- Use a credit card instead of a debit card when online shopping. While both credit and debit card sales can be disputed, it may take more time to have money returned to a debit card. Additionally, some credit card providers offer single-use numbers to be used online to further protect financial information;
- Create unique passwords for different sites and ensure a strong password by using uppercase and lowercase letters, numbers and special characters;
- Never use public Wi-Fi to transmit or access private information;
- Always read privacy statements to determine how personal information will be used and whether it will be sold to third parties;
- Enable two-factor authentication whenever possible; and
- Check your financial accounts regularly to ensure there are no duplicate or fraudulent charges.

For more tips on preventing identity theft, click here.

For more information on National Cybersecurity Awareness Month, click here.

Report potential phishing or malware scams to the Florida Attorney General's Office by visiting MyFloridaLegal.com, or 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.