

ALABAMA SECURITIES COMMISSION

Post Office Box 304700 Montgomery, Alabama 36130-4700
Telephone: (334) 242-2984 or 1-800-222-1253 Fax: (334) 242-0240
Email: asc@asc.alabama.gov Website: www.asc.alabama.gov

ASC ENCOURAGES CLEAN CYBER HYGIENE TO HELP PREVENT YOU FROM BECOMING A VICTIM OF A RANSOMWARE ATTACK

MONTGOMERY, ALABAMA (June 22, 2021) – The Alabama Securities Commission (ASC) warns of an uptick in cybercrimes impacting investment accounts, particularly those involving ransomware. A ransomware attack is a type of phishing scam that attempts to obtain sensitive information or data in exchange for money, and recent publicized attacks involve gas and meat suppliers.

Hackers are not only targeting companies, but victimize computer and smartphone users. Through email and social media, hackers trick users into downloading a file, or virus, that will essentially give them control over the user's device. They then threaten to release embarrassing information or keep the device locked until the ransom has been paid, and will often demand a hard-to-trace payment, such as a cryptocurrency or a pre-paid gift card. Stolen passwords are then used to steal money from financial and other accounts.

"We must remain vigilant in protecting our personal and financial information. Hackers can steal money without ever stepping foot in your house," said ASC Director Joseph P. Borg. "Not protecting your online accounts is equivalent to not locking your door, don't be surprised when your prized possessions are missing. Fraudsters can steal your life savings with just a click of a button."

Clean cyber hygiene is about training yourself to think proactively about cybersecurity. Establishing a cybersecurity plan is key to safeguarding online investment accounts and personal information. Follow these steps to improve cyber hygiene:

- Secure your internet network and change the generic password that comes with the router.
- Strengthen your password by making it at least 12 characters or longer, and add numbers.
- Use two-factor authentication when logging into financial accounts.
- Exercise extreme caution when using a free Wi-Fi network. Hackers can set up decoy networks that appear to be legitimate networks in hotels, restaurants, and coffee shops, which allows them to see and record your activity.
- Update the software on all of your devices (tablets, smartphones, and computers).
- If you receive an email from an unknown sender (even if the details appear accurate), do not respond, and do not click on any links or attachments found in that email. Instead, call to verify the information.
- Slow down and think before you click. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy.
- Be cautious of generic greetings such as "Hello Investor," as these are often signs of phishing attempts. If concerned about the legitimacy of an email, call the company directly.
- Never give out personal information, account numbers, and passwords to anyone, especially in response to unsolicited emails, text messages, or phone calls for the information.

"Always monitor investment, banking, and credit card accounts on a regular basis for suspicious activity. If you think your accounts have been compromised, change your passwords, contact third parties, including your bank,

-more-

financial advisor, law enforcement authorities, and the Federal Trade Commission- which can help you develop a recovery plan- and check credit reports for further invasions. Consider putting a ‘freeze’ on your account until the extent of damage has been surveyed,” said Chief Deputy Director and Chair of the North American Securities Administrators Association Cybersecurity Committee, Amanda Senn.

The ASC cautions citizen investors of all ages and experience to thoroughly scrutinize and research any investment opportunity or offer. Contact the ASC at 1-800-222-1253 to check out any person or a financial professional offering an investment opportunity or investment advice for a fee and the products they offer for proper registration. Contact the ASC to report suspected fraud, inappropriate securities business practices, or to obtain consumer information. The ASC provides free investor education and fraud prevention materials in print, on our website, and through educational presentations upon request.

###

For further information contact Dan Lord, Education and Public Affairs Manager, 334-353-4858.

ALABAMA SECURITIES COMMISSION

Post Office Box 304700 Montgomery, Alabama 36130-4700

Telephone: (334) 242-2984 or 1-800-222-1253 Fax: (334) 242-0240

Email: asc@asc.alabama.gov Website: www.asc.alabama.gov