Attorney General Doug Peterson

News Release

FOR IMMEDIATE RELEASE
October 3, 2017

Contact: Suzanne Gage
402.471.2656
suzanne.gage@nebraska.gov

Nebraska Attorney General's Office
Recognizes Cyber Security Awareness Month

You don't have to be a computer expert to understand the basics of cyber security. Even small actions can make a huge difference in keeping you safe online. As cybercrimes like fraud and scams, identity theft, and network breaches continue to increase, it's more important than ever to know how to protect yourself in the cyber world.

During the month of October, the Nebraska Attorney General's Consumer Protection Division is joining with the Department of Homeland Security's Stop. Think. Connect. ™ Campaign and its partners across the country to recognize National Cyber Security Awareness Month and highlight the importance of online safety.

It's easier than you think to practice good cyber security every day. The Consumer Protection Division encourages all Nebraska consumers to take these simple steps toward greater cyber security.

- **Make Your Passwords Long and Strong**. Use complex passwords with a combination of numbers, symbols, and letters. Use unique passwords for different accounts. Change your passwords regularly, especially if you believe they have been compromised. This is especially important in the wake of the recent Equifax data breach.

- **Keep a Clean Machine.** Update the security software, operating system, and web browser on all of your Internet-connected devices. Keeping you security software up-to-date will prevent attackers from taking advantage of known vulnerabilities.

- **Secure Your Wi-Fi Network**. Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi

network, and your digital devices, by changing the factory-set default password and username. Again, the best passwords are long and strong using a combination of numbers, symbols, and letters.

- **Use Encryption on Your Wireless Network**. Encrypt the information you send over your wireless network so that nearby attackers can't eavesdrop on your communications. Encryption scrambles the information into a code not accessible to others. Using encryption is the most effective way to secure your network from intruders.

  Two main types of encryption are available for this purpose: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). WPA2 is strongest; use it if you have a choice. It should protect you again most hackers. Note that routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how.

- **Share with Care.** Limit the amount of personal information you share about yourself online. Your full name, phone number, address, school or work location, and other sensitive information, such as your birthday, should not be published widely. Disable geo-tagging features that let people online know where you are. Limit your online social networks to the people you know in real life, and set your privacy preferences to the strictest settings.

- **Avoid Conducting Sensitive Activities Through Public Networks**. Avoid online shopping, banking, and sensitive work that requires passwords or credit card information while using public Wi-Fi. Before connecting to any public wireless hotspot like in an airport, hotel, or café, be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. Most hotspots are not secure and do not encrypt the information you send over the Internet, leaving it vulnerable to cybercriminals. You own mobile network connection is generally more secure than using a public wireless network.

For additional details about keeping yourself safe online, visit the Nebraska Attorney General's Office, Consumer Protection Division website: https://ProtectTheGoodLife.Nebraska.gov.

###