NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Cybersecurity Awareness Month Week Three: Securing Internet-Connected Devices in Healthcare

Release Date: October 19, 2020

Media Contact: Ti Gauger, Public Information Officer, (608) 224-5007, Ti.Gauger@Wisconsin.gov

MADISON – The healthcare industry is increasingly relying upon internet-connected devices and solutions to improve patient care, organizational efficiency, and speed of crisis response. The emergence of telemedicine, digital health records, internet-connected medical devices, patient wellness apps, and an increasing amount of third parties entering the health supply chain, has exposed the industry to vulnerabilities that cybercriminals regularly attempt to exploit.

During the third week of National Cybersecurity Awareness Month (NCSAM) the Department of Agriculture, Trade and Consumer Protection (DATCP), highlights how consumers can take steps to remain secure on internet-connected health services such as telemedicine and health care apps.

"Apps can be a helpful tool for consumers to get easy access to information or resources to manage their health, but consumers should take steps to be cyber smart when using these resources," said Lara Sutherlin, Administrator of DATCP's Division Trade and Consumer Protection.

- **Use secure connections to sign into healthcare websites and apps.** Accessing the internet using a public Wi-Fi hotspot is convenient and often free, but hotspots may not be secure. If you are not required to enter a password provided by the Wi-Fi host (i.e. coffee shop or hotel) before gaining access to the network, another Wi-Fi user could hack into your device and access sensitive personal information.
- **Review the privacy policies** of any applications you use to know and understand how your information may be accessed and shared with others.
- **Use two-factor/multi-factor authentication** when supported to help prevent unauthorized access in case your username and password are compromised. Two-factor authentication is an added layer of security that combines a physical item you have, such as a card or a code, with something you know, such as a personal identification number (PIN) or password.
- **Never allow devices to remember your passwords.** This may be convenient, but if your device is compromised the intruder may be able to access any app that has a saved password.
- **Don't open health care apps through other apps**. Always open and log in to health care apps manually. Do not let other apps, such as social media accounts, access your health care apps or log you in.
- **Completely sign out of apps** when you are finished using them to help prevent unauthorized access.
- **Delete unused apps.** When you are no longer using an app on your phone or other device, don't forget to close your account and delete the app from your device.

Join DATCP during the 17th annual National Cybersecurity Awareness Month (NCSAM) to **"Do Your Part. #BeCyberSmart."** Learn more by following @WIConsumer and @widatcp on Facebook or Twitter.

###

Find more DATCP news in our newsroom, on Facebook, Twitter, and Instagram.