NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Cyber Security Awareness Month – Daily Tips, Week 4: Safety on the Go (Mobile Devices)

Release Date: **October 20, 2017**

Media Contact: **Jerad Albracht, 608-224-5007**
Bill Cosh, Communications Director, 608-224-5020

MADISON – In recognition of Wisconsin's Cyber Security Awareness Month, the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) will release a cyber safety tip each weekday in October, with each week addressing a different theme. The agency will release the daily tips through the Bureau of Consumer Protection's Facebook and Twitter accounts.

To assist media partners that may wish to cover the cyber tip topics, DATCP will send out a release each Friday in October with the next week's messages. Media partners can contact Jerad Albracht (Senior Communications Specialist, 608-224-5007, jerad.albracht@wisconsin.gov) if they would like to speak with a Bureau of Consumer Protection representative about the campaign or about a specific tip.

###

Cyber Security Awareness Month, Week 4: Safety on the Go (Mobile Devices)

Monday, 10/23. Mobile device passwords

Most smartphones and tablets require users to enter passcodes to access the device. It may be a minor inconvenience, but it's tough to argue how valuable that extra security step is…our mobile devices carry an incredible amount of information about us. Cyber thieves know this and will do anything to get at it.

Use a unique passcode for each device. For added security, set your device to require regular password entries and use the fingerprint reader devices for unlocks. We'll address mobile device safety further in tomorrow's tip. #CyberAware

Tuesday, 10/24. Lost phone? Bad. Lost data? Worse.

If your smartphone or tablet is lost or stolen, you want to have a fighting chance at finding it or at least at wiping out any personal data before it's accessed by the wrong party. For this purpose, there are tracking applications available for the major mobile device operating systems.

If you are a Google Android user, your device uses a "Find My Device" feature (available on the Google Play Store). On Apple devices, look for "Find My iPhone" in the Settings menu.

Using these tools, you can remotely locate your device or lock or erase your device, but you need to make sure the features are active and properly set up before you run into trouble. Read up on these services and decide if you want them available on your devices. #CyberAware

Wednesday, 10/25. Use caution on public networks

If you are using a public Wi-Fi hotspot to connect to your personal accounts on a mobile device, limit the types of business you conduct, shield your typing from prying eyes, and set

(MORE)

your device to hide your password character entries. Hold off on using online banking websites or sites that require sensitive personal information (like Social Security numbers) until you are on a secure private network or a home computer.

BONUS TIP: on any web browser (mobile or desktop/laptop alike), look to see if the website encrypts the information it transmits BEFORE you enter and submit any sensitive information. How can you tell if a site is encrypted? Check that the URL (the web address) starts with "https" rather than "http." The "s" stands for "secure." Cool, right? #CyberAware

Thursday, 10/26. Keep an eye on your devices

Kind of a simple, self-explanatory tip today, but always keep your mobile devices with you in public and never leave them out "just for a couple of seconds." A couple of seconds is long enough for a thief to disappear with your expensive device and your even more valuable data like contacts, messages, schedules, photos, music and more.

Earlier in the month we suggested tracking down and updating all of your family's online devices. Now that they are accounted for, keep an eye on them in public and keep them locked up when not in use. #CyberAware

Friday, 10/27. Tag, you're it! And in trouble.

"Geotagging," or linking GPS coordinates with your photos and online posts, is often turned on as a preset on mobile devices. Be very careful how you utilize this feature…this information can give criminals the tools they need to track or rob you.

Don't geotag pictures of your home or children and pay attention to which applications use the feature in your device and app settings. #CyberAware