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 18, 2018**

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 page and Twitter account.

To assist media partners that may wish to cover the cyber tip topics, DATCP will send out a release each Thursday 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, 10/22. 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. Cyber thieves know this and will do anything to get at that data.

Use a unique passcode for each device. For added security, use the device's fingerprint reader for unlocks. We'll address mobile device safety further in tomorrow's tip. #CyberAware

Tuesday, 10/23. 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. #CyberAware

(MORE)

Wednesday, 10/24. 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 your device to hide your password character entries. Hold off on using online banking websites or sites that require personal information (like Social Security numbers) until you are on a secure private network or a home computer.

Be aware that there are “imposter” hotspots out there – Wi-Fi networks run by scammers that are made to appear like they are provided by a local business. The actions you take on an impostor network are visible to the person running the network. Again, limit the types of actions you take on any public network to minimize your risk of unknowingly sharing information with crooks.

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 personal information like passwords, security questions, banking information, etc. 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.” Easy, right? #CyberAware

Thursday, 10/25. Watch for data hungry apps

Every time you download a new application, check the data usage settings in the device settings menu to ensure that the app will not drain your data behind the scenes. Even programs that have solid ratings in the app stores may run data-intensive processing in the background. You may not realize that this is occurring until your service provider warns you that you’re running low on available data for the month – depending on your service plan, this could end up costing you an additional payment for more data or could lead to your data speeds being throttled for the rest of the month. #CyberAware

Friday, 10/26. 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 data could be used by criminals to target you in a scam or ID theft operation.

Pay attention to which applications use location-based features in your device and app settings. #CyberAware