NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Media Advisory: DATCP Recognizes National Cyber Security Awareness Month with Daily Safety Tips

Release Date: **September 27, 2018**

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

Editor's Note: Next week's cyber security tips are included on the second and third pages of this release.

MADISON – October is not just a time for black cats, jack-o-lanterns, and bed sheet ghosts…it is also National Cyber Security Awareness Month. Given our reliance on mobile devices and the increasing number of web-connected devices we are welcoming into our homes, Wisconsin consumers are asked to use this month to consider ways to stay protected from scam artists looking to trick you and treat themselves to your personal information and hard-earned money.

The Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) will recognize this campaign through a cyber safety tip each weekday in October, with each week addressing a different theme. The agency will release each daily tip 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 Thursday in October with the next week's messages (the first week's tips are included on the second and third pages of this advisory).

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.

###

(MORE)

Cyber Security Awareness Month, Week 1 daily tips: Simple Tips. Serious Protection.

Monday, 10/1. Take stock of your web-connected lifestyle

As we welcome additional web-enabled devices and applications into our lives, the line between our online and offline lives becomes less defined. We need to ensure that our accounts are secure so that we can use our devices with confidence.

The first step in strengthening the security around your devices and accounts is to take stock of these items in your home. Don't forget to include web-connected home devices as well, such as gaming devices, smartwatches, thermostats, smart TVs, routers, and voice assistants (Google Home, Amazon Alexa, etc.).

Once you have accounted for all of your devices (and your family members' devices), update the operating systems and antivirus software on the devices in order to protect against recent viruses and to patch any holes that hackers can use to access your systems.

Bonus tip: join DATCP each weekday in October on the Bureau of Consumer Protection's Facebook or Twitter feeds for more quick and easy cyber tips. We'll see you here again tomorrow! #CyberAware

Tuesday, 10/2. 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 minute." A couple of seconds is long enough for a thief to disappear with your device and your valuable data like contacts, messages, schedules, photos, music, mobile payment accounts and more.

Yesterday 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

Wednesday, 10/3. Take active steps to protect your kids BEFORE they log on

Keep your home computer in a central location where you can monitor your children's online usage.

Look for any protection features (i.e. parental controls) that are built into the websites and software that your kids access and adjust them accordingly.

All major Internet service providers (ISPs) and cellular providers have tools to help you manage children's online experiences (e.g., selecting approved websites, monitoring the amount of time they spend online, limiting in-app purchases or limiting the people who can contact them).

For these tips and many more, visit the "Raising Digital Citizens" page on the StaySafeOnline.org site. #CyberAware

Thursday, 10/4. Think before you act

Ignore unsolicited emails, social media messages, phone calls or texts that create a sense of urgency and require you to respond immediately to a problem – particularly ones that supposedly involve your online account, bank account, taxes or package delivery. This type of message is likely a scam. When in doubt, don't respond.

If you question the legitimacy of a message that claims to be from a business or government agency, call the organization directly to inquire. Don't contact the organization on any phone number provided in the unsolicited call or voicemail and don't click any links in the email, social media post or text message. #CyberAware

Friday, 10/5. Saying goodbye to an old device? Don't say goodbye to your identity.

Looking to swap out for the latest smartphone? If you are trading in your phone at a retail store, the business will likely transfer your contacts to your new phone and wipe your data off your old phone. That's great. But what if you intend to donate, resell or recycle your old equipment?

Before you turn your old phone over to anyone or throw it in a donation bin, remember to completely erase your data and reset the phone to its initial factory settings. Check your device's general settings for a factory data reset option. If you don't know where to go, search online for information about your specific phone model or check with your cellular provider. Additional tips are covered on the Federal Trade Commission's (FTC) "Disposing of Your Mobile Device" webpage.

If you are getting rid of a desktop or laptop computer, you should make sure the hard drive is wiped completely clean before you let it go. The FTC's "Disposing of Old Computers" webpage includes considerations you need to make when disposing of a computer, including the importance of using specialized utility programs to wipe drives. #CyberAware