NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Media Advisory: Helping You Stay Cyber Safe, One Tip at a Time

DATCP Recognizes National Cyber Security Awareness Month

Release Date: **October 2, 2017**

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

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

MADISON – Recent data breaches and widespread breakouts of malicious software have gained the attention of the nation. According to recent studies, 96 percent of Americans feel a personal responsibility to be safer and more secure online and 90 percent said they want to learn more about safe internet usage.[1] The message is clear: cyber threats affect everyone, and everyone has to take action to protect themselves and their families.

October is National Cyber Security Awareness Month, and consumers are advised to "Stop. Think. Connect." when using computers and web-enabled devices:

Stop

- others from accessing your accounts by setting secure passwords.
- sharing too much personal information.

Think

- before you click. Is this a trusted source?
- about what you post or share. What's online, stays online…maybe indefinitely.

Connect

- over secure networks. Wi-Fi hotspots may not offer the same protection.
- wisely. Trust your gut. If it doesn't seem right, then close out or delete the email.

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.

For more cyber safety information, visit the DATCP website at datcp.wi.gov, call the Consumer Protection Hotline at 800-422-7128 or send an e-mail to datcphotline@wisconsin.gov.

To assist media partners that may wish to cover the cyber tip topics, DATCP will send out a release each Friday from October 6th to October 27th with the next week's messages (Week 1 tips are included below).

Media partners can contact Jerad Albracht (Senior Communications Specialist, 608-224-5007, mailto: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.

###

[1] National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG).
https://www.stopthinkconnect.org/research-surveys/research-findings

Cyber Security Awareness Month, Week 1 daily tips: Cybersecurity is personal.

Monday, 10/2. What is "cyber security?" What is at risk?

According to Merriam-Webster, "cybersecurity" is defined as "*measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack.*"

In other words, cybersecurity means taking steps to protect yourself, your family and your friends from the risks of computer-driven crimes – crimes like the theft of your personal or financial information or damage to your computer system or online accounts.

Using unsafe internet practices and unsecured devices and networks can expose your finances and good name to a lifetime's worth of damage.

Thankfully, there are many simple steps that a computer or mobile device user can take to tighten the security around their sensitive data and make their systems more resilient in the face of cyber attacks. You are already off to a great start: joining DATCP each weekday in October on the Bureau of Consumer Protection's Facebook or Twitter feeds is a quick and easy way to learn a lot of useful information and to start taking meaningful action. We'll see you here again tomorrow! #CyberAware

Tuesday, 10/3. It's 10:00 p.m. Do you know where your child('s tablet) is?

Where are all of your family's web-enabled devices? Can you account for them all?

Think of all of the internet-connected devices in your household. Are you keeping track of your family's smartphones, tablets, laptops, desktops, smart TVs, etc.? Being able to account for all of the web-enabled devices in your household is an important first step in ensuring that your family members' personal information is safe.

Step two: now that they are accounted for, protect your devices. Update the operating systems and antivirus software on your devices in order to protect against recent viruses and to patch any holes that hackers can use to access your systems. #CyberAware

Wednesday, 10/4. 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 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, 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: https://staysafeonline.org/get-involved/at-home/raising-digital-citizens/ #CyberAware

Thursday, 10/5. 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 one involving your online account, bank account or taxes. 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 post or text message. #CyberAware

Friday, 10/6. 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 phone?

Before you turn your old phone over to anyone or throw it in a donation bin, you must remember to completely erase your data and reset the phone to its initial factory settings. Check your phone'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 need to 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