NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Cyber Security Awareness Month – Daily Tips, Week 3: Cyber Scam Risks

Release Date: **October 11, 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 3: Cyber Scam Risks

Monday, 10/15. Email and text message spam and scams

The terms "scam" and "spam" are almost interchangeable when it comes to email and text messages. Spam messages are junk bulk emails or texts that you receive without permission. The senders may be hocking "get rich quick" schemes and questionable products or they could be looking to get you to turn over personal or credit information (a practice known as "phishing" for data).

Did we mention that the messages can also transmit malware?

Simply put, if you get an odd email or text message out of the blue, delete it and take no further action. There is a lot to cover on email and text spam, so your best resource is our DATCP fact sheet on spam. #CyberAware

Tuesday, 10/16. Microsoft is NOT calling. Watch for computer tech support scams

If you receive a call out of the blue claiming that your computer has a virus and that the caller can help you get rid of it, hang up immediately. It's a scam. The callers often falsely claim to represent Microsoft or a local tech support company to gain the consumer's trust. They tell the consumer that they can remove the (non-existent) virus from their computer for a fee. The caller asks the victim to download software from the internet that grants them remote access to the system.

(MORE)

If you allow these scammers to access your computer, they can load malicious software onto your machine and they may access your files as well. If you give them your credit card number to pay for their "services," they'll be happy to charge you despite doing nothing beneficial (and possibly causing harm) and they may add fake charges on your account.

This is typically a phone-based scam, but also shows up in online pop-up messages saying you have a computer virus and telling you to call them for help. Don't do it. #CyberAware

Wednesday, 10/17. That amazing, unbelievable online rental ad? Beware.

As always, if something seems too good to be true, it probably is. If you are looking online for a rental property and find an unreal deal, be very, very cautious.

Scammers steal information and pictures from real estate listings in order to post fraudulent apartment or home rental ads on Craigslist and other online sites. They may "rent out" a property that they don't own (or that doesn't even exist!) to multiple people, taking security deposits and first month's rents from all of these parties.

It's worth remembering that these types of fake classified ads are not only about rental properties – there are often fake ads for high-ticket items like cars, boats, and other vehicles. If a seller or a buyer refuses or is "unable" to meet for the transaction, by leery of the deal. If you are selling an item, turn away any buyer who sends you a check for way over your selling price and wants you to send back the difference (the check is fake and YOU will end up paying the bank back). If you are buying an item, watch out for requests to pay by wire transfer or pre-paid debit card…once your money is sent, it is nearly impossible to get it back if the ad is fake.

Craigslist offers these two simple tips on their website: "Do not rent or purchase sight-unseen – that amazing 'deal' may not exist" and "Refuse background/credit checks until you have met landlord/employer in person." #CyberAware

Thursday, 10/18. Think before you post

Your fun-filled vacation photos could cause your grandma or grandpa to get scammed.

Why? Criminals can use the information you share on social media sites to create a narrative that they weave into their phony stories.

Consider the infamous "grandparent scam," where older citizens are called by a scammer claiming to be the person's grandchild. The "grandchild" claims to be on vacation, was in an accident or got arrested, and needs an immediate wire transfer to get out of the hospital or out of jail. Your social media account could provide a tremendous amount of information for a scammer to use in their ploy, such as your name, family members' names, where you live and if you are away from home.

Remember those fun-filled pics I mentioned? By viewing your profile, the scammer knows you are away on vacation in ____ with your best friend ____. They can fill in the blanks, making for a much more believable con.

It's OK to share with friends and family on social media, but adjust the privacy settings for your accounts to block your content from strangers. Also, remember that sensitive information such as names, birth dates and Social Security numbers posted to social media accounts can be used by scammers to steal your identity. Keep private information private. #CyberAware

Friday, 10/19. Imposter scams

Many criminals are using government agency names or "look-alikes" in recent email and phone scams, hoping to add legitimacy to their ploys. Have you received an email from "State Court" about a required appearance? That's one (do NOT open the attachment in one of these emails!).

But it's not just government agencies whose identities are misused. Remember our tip on Tuesday regarding calls from fake tech support representatives looking for money for "repairs" and access to victims' computers? Those are imposter scams too, as are fake delivery confirmation emails that claim to come from legitimate shipping companies – these emails include a link or attachment that you are expected to click in order to learn about a supposed package delay or a problem with an order.

Don't fall for these ploys. Delete the emails and don't click any links. The fraudsters want your money, your personal information, or to infect your computer with malware. If you question the legitimacy of a communication from a business or governmental agency, contact DATCP's Consumer Protection Hotline (800-422-7128) or call the misrepresented agency directly to inquire (but don't use the phone number that was provided in the questionable message!). #CyberAware