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 13, 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 3: Cyber Scam Risks

Monday, 10/16. 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). Either way, you're ripped off.

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: https://datcp.wi.gov/Pages/Publications/Spam284.aspx #CyberAware

Tuesday, 10/17. 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.

If you allow these scammers to access your computer, they can load any number of malicious software programs onto your machine and they may access your files as well. If you give them your credit card number to pay for their "services," you can expect to get ripped off there too. 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

(MORE)

Wednesday, 10/18. 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 use information from real estate listings 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 to multiple people, taking security deposits and first month's rents from all of these parties. Their listings may also be ploys to get you to pay for a credit report service…the scammers get a commission if you do.

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, 10/19. Think before you post

Your fun-filled vacation photos could cause your grandma to get ripped off.

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

Consider the infamous "grandparent scam," where elderly citizens are called by a scammer claiming to be the person's grandchild. The "grandchild" says they are on vacation, were in an accident, and need an immediate wire transfer to get out of jail or the hospital. 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. #CyberAware

Friday, 10/20. 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 gotten a threatening call demanding money from someone claiming to be with the IRS? That's a regularly used con. Did you get an email from "State Court" about a required appearance? That's another one (do NOT open the attachment in one of these emails!).

But it's not just government agencies whose identities are misused. Scammers falsely claiming to represent the local utility company, regularly call consumers and businesses and make threats that they will cut off the electrical service if the call recipient doesn't make an immediate payment. And our tip on Tuesday covered calls from fake tech support representatives looking for money for "repairs" and access to victim's computers.

Don't fall for these scams. Delete the emails and hang up on these callers. They 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