NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Cyber Security Awareness Month – Daily Tips, Week 5: Lock Down Your Login

Release Date: **October 27, 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 5: Lock Down Your Login

Monday, 10/30. Build better passwords…be better protected.

Take steps to strengthen the security around your online accounts by creating longer, more complex passwords that are tougher to crack. Use a passphrase: a combination of numbers, letters and special characters that spells out a phrase that you will remember.

For example, the phrase "I am happy to be here!" could be coded as "Iam:)2bH!"

Keep unique passwords for every online account and make sure to use an especially strong password for your email. Many websites send password update and account access emails to consumers, so getting a hold of these emails could potentially give a hacker access to all of your online accounts. Your email password should be the toughest to decode.

For more tips, check out DATCP's "Creating Strong Passwords" fact sheet: https://datcp.wi.gov/Documents/IDTheftPasswordsCreating658.pdf #CyberAware

Tuesday, 10/31. Use two-factor authentication when available

Two-factor authentication is a security process in which you provide two means of identification in order to log into a system – something you have and something you know. Something you have is typically a physical token, such as a fob, fingerprint or a code sent to your smartphone. Something you know is something memorized, such as a personal identification number (PIN) or a password.

If this sounds confusing, think about this: when you use your credit card at the gas pump, you already use two-factor authentication. You swipe your card (something you have) and enter your ZIP code (something you know). So if one of your favorite websites strengthens its security features and offers to send you an additional passcode for logging in, take them up on it. #CyberAware