NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Data Privacy Day: Be Aware. Take Control.

Release Date: **January 28, 2016**

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

MADISON – With every visit to the internet we expose ourselves to the risks of identity theft and malware. There are safeguards in place both on our devices and online that help us stay protected during the vast majority of our browsing, reading and posting, but we are always one misplaced mouse click away from damaging consequences.

Got your attention?

Today is Data Privacy Day, and the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) is asking consumers to think about how they use the internet, question the amount of information they are sharing online, and evaluate the steps they are taking to protect their personal information.

Governor Scott Walker issued a proclamation in recognition of this international awareness effort, noting the importance for individuals, government agencies, businesses, and educational and healthcare institutions to identify data privacy risks and to counteract threats to valuable personal information.

"We often presume that the devices and web services we use are inherently secure, and we don't put any extra thought or effort into protecting our information," said Frank Frassetto, Division Administrator for Trade and Consumer Protection. "Data Privacy Day is a chance for Wisconsinites to pause and consider whether they need to take a more active role in securing their personal and financial information online and on their internet-enabled devices."

The best way for consumers to protect their valuable information is to use caution when sharing personal and financial details online and to make use of the added security features built into the internet-connected devices and online services they use.

Consumers can start building a more secure online presence by:

Strengthening the security around online devices

- **Protect your devices.** Update the operating system and antivirus software on your devices to target recent viruses and patch any holes that hackers can use to access your system. For added security, set your device to require regular password unlocks.
- **Always keep your phone in a secure location.** Your smartphone and tablet contain a wealth of personal information like your contacts, messages, media files and schedules. Know where your phone is at all times and keep it locked away in public.
- **Set up your device with privacy in mind.** Set your smartphones, tablets and computers to "time out" every so often and to require a password or fingerprint to log back in.
- **Consider turning off "geotagging."** Mobile devices often link GPS data with photos and online posts by default, and many programs request this data from the device during normal usage. Be very careful how you utilize this feature – this information can give criminals the tools they need to track or rob you. If you wish to disable this feature, look in your device's settings menu for references to "Location" or "Location Services" services and turn these options off. Watch for apps that ask for this data before you install them.

Taking the fight online – protecting accounts and browsing wisely

(MORE)

- **Secure your home network.** At home, password-protect both your router and your WiFi network and choose the WPA2 setting when you setup the network.
- **Enter sensitive information only into encrypted websites.** Before you enter personal or banking information into a website, make sure the URL starts with "https" rather than "http" (the "s" stands for secure). This signals that your connection to the site is encrypted and more resistant to spoofing or tampering.
- **Use caution on public networks.** If you are using a public Wi-Fi hotspot to connect to your personal accounts on a mobile device, limit the types of business you conduct and set your device to hide your password character entries. Other network users could monitor your information if it is not encrypted (again, look for "https").
- **Change your internet passwords frequently.** Use a long combination of numbers, letters and special characters. Use different passwords for different websites.
- **Protect your email account.** Use a complex and unique password that is specific to your email account. Many websites send password update and account access emails to customers, so getting a hold of these emails could potentially give a hacker access to all of these online accounts.
- **Use two-factor authentication when offered.** Two-factor authentication is a security process in which you, the user, provide two means of identification – something you have and something you know. Something you have is typically a physical token, such as a card or a code sent to your smartphone. Something you know is something memorized, such as a personal identification number (PIN) or a password.

Remaining cautious and attentive when browsing and posting online

- **Keep personal information private.** Never give out personal information in a reply to an unsolicited text message or email.
- **Think before you click.** Never open any links or attachments in an unsolicited email. Research unfamiliar websites and companies before you interact with them.
- **Think before you post.** What you post can last a lifetime. Adjust the privacy settings for your social media accounts to block your content from strangers. 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.
- **Think before you app.** Before downloading a mobile app, understand what information (your location, access to social networks, etc.) the app accesses to function.

For additional consumer information or to file a complaint, visit the Consumer Protection Bureau at datcp.wisconsin.gov, send an e-mail to datcphotline@wisconsin.gov or call the Consumer Information Hotline at 800-422-7128.

Connect with us on Facebook at www.facebook.com/wiconsumer.

###