



Data Privacy Day: Take Small Steps for Big Protection

Release Date: January 26, 2017

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

MADISON – Our personal information has a life of its own online. Our names, addresses, birthdates, Social Security numbers and more are stored throughout the internet in databases owned and maintained by businesses, government agencies, healthcare organizations and educational institutions. For protection of this sensitive information, we rely on these organizations to properly safeguard our data and we make the best decisions we can with how and where we share our details online.

Saturday is Data Privacy Day nationwide, and the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) asks consumers to think about how they use the internet, question the amount and type 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.

“Data Privacy Day gives us all a chance to take a step back and think through the ways we share our information and the actions we take with our web-enabled devices,” said Frank Frassetto, Division Administrator for Trade and Consumer Protection. “We hope that Wisconsin consumers will make at least one small change in their digital habits to strengthen the security around their devices and accounts, such as second guessing links in emails and social media posts.”

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. Our devices and the web services we utilize are not inherently secure, so we have to take some responsibility for our own privacy. For example, when we setup a new device or open an online account with a new service, we should take a moment to create custom passcodes on the device and setup two-factor authentication on the account.

Consumers can start building a more secure online presence by:

Strengthening the security around web-enabled 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 devices in a secure location.** Your smartphone and tablet contain a wealth of personal information like your contacts, messages, media files and schedules. Know where they are at all times and keep them hidden from public view.
- **Setup your device with privacy in mind.** Set 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, giving criminals the tools they need to track or rob you. Disable this feature in your device’s settings menu by turning off “Location” or

(MORE)

“Location Services” services. Watch for apps that ask for this data before you install them.

Taking the fight online – protecting accounts and browsing wisely

- **Secure your home network.** At home, password-protect both your router and your WiFi network. Do not rely on default passwords that come with your device.
- **Enter sensitive information only into encrypted websites.** Before you enter personal or banking information into a website, make sure the URL starts with “https” (the “s” stands for “secure”) or you see a padlock icon. This signals that your connection to the site is encrypted and more resistant to spoofing or tampering.
- **Use caution on public networks.** Limit your use of public WiFi networks and never send sensitive personal or financial information over an unsecured connection. Other network users could monitor your information if it is not encrypted.
- **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 your 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 PIN code 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 identity thieves.
- **Think before you app.** Before downloading a mobile app, understand what information (your location, access to social networks, etc.) it accesses to function.

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

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