Dept. of Agriculture, Trade and Consumer Protection: Data Privacy Day: Shrink your digital footprint, one step at a time

Posted on Tuesday, Jan 23, 2018

CONTACT: Jerad Albracht, Senior Communications Specialist, 608-224-5007
Bill Cosh, Communications Director, 608-224-5020

MADISON – New online applications are launched every day, and internet users are only a couple of clicks away from downloading these programs and setting up accounts. With each new account we create, we continue the spread of our personal (and often financial) information across the internet, expanding our "digital footprint."

To remind everyone of how important it is to consider the amount and types of information we share online, Sunday has been designated as Data Privacy Day (1/28). Governor Scott Walker issued a proclamation in recognition of this international campaign, and the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) asks Wisconsin residents to set aside a couple of minutes on that day to evaluate their online presence and the steps they take to protect their personal information.

"Today almost everyone has a digital footprint, and we need to be sure to protect it," said Michelle Reinen, Director of the Bureau of Consumer Protection. "Data Privacy Day is a day to stop and consider how we interact online and the potential risks of oversharing personal information."

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. We rely on these organizations to safeguard our data, but we can help protect our information by making decisions on how and where we share our information online.

To better protect their digital footprints, consumers could use Data Privacy Day to:

- Delete apps that they no longer use. Having an abundance of unused, out-of-date apps can create vulnerabilities that could threaten your accounts and your devices.
- Purge the application permissions list in their social media accounts. Many people use their social media accounts to log into other services rather than creating usernames and passwords for those apps. These connections could give the third-party service the right to reuse information from your social account such as your name, birthdate, contacts and even your messages. This could put your social accounts at risk if a linked service is compromised.
- Review the settings of each app to see which services it accesses in their devices. Some apps may access your device’s camera, seek your physical location (using information from GPS, cellular and Wi-Fi networks or Bluetooth), or access your device’s mobile pay features. Turn off any connections you are uncomfortable with or delete the app altogether.
- Pay close attention to requests for data or device services that appear during the setup stage for a new app or online account. If you are uncomfortable with any of the data or services that the program will utilize, deny the request.
- Update passwords. Be sure they are long and strong, with a combination of at least eight uppercase and lowercase letters, numbers and special characters.
- Update all web-enabled devices to the latest operating system and antivirus package in order to protect against the newest viruses and vulnerabilities.
- Remind friends and family members not to click on links in unsolicited emails or social media posts and to avoid completing unsolicited surveys that ask for personal information.