NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Pre-Summer Break Homework: Take Cyber Security Steps

Release Date: June 11, 2019

Contact: Jerad Albracht, Communication Specialist
(608) 224-5007, jerad.albracht@wisconsin.gov

MADISON – With kids at home over the summer, there will likely be an increase in screen time in many Wisconsin homes. The Wisconsin Department of Agriculture, Trade and Consumer Protection asks parents and guardians to strengthen the security of their devices and to talk with their children about how to protect themselves from scams and identity thieves when online.

"Taking some simple steps ahead of summer break could help kids avoid online risks like malware and phishing scams," said Lara Sutherlin, Administrator for the Division of Trade and Consumer Protection. "Update your devices and applications to help fend off the latest hacks, set up parental controls on devices, and talk with your children about their online plans so that you can identify problematic activities."

Step #1: make sure your devices and apps are updated going into the summer break. WhatsApp (a popular messaging app owned by Facebook) was recently found to have been compromised, putting user devices at risk of installing spyware. The company responded with a patch for its 1.5 billion users – but only by updating the app would your device and account be protected. Download and install software updates for operating systems, antivirus packages, and apps.

Follow these tips to help your children make smart cyber choices over the summer break:

- Restrict access to age-appropriate content by using parental controls on devices and web browsers. Specific kid-friendly search engines can limit results to sites that are safe for kids. Consider locking devices with a password so children can't download or buy apps without your approval.
- Talk to your kids about what they are doing online. Which games, social networking sites, and other online activities are your kids into? Are you comfortable with them? Research apps and websites and try them out yourself.
- Teach your children what NOT to click. Clicking links in unexpected texts or pop-up windows could infect a device with malware and raise the family's identity theft risk.
- Establish rules for downloading. Teach kids to be wary of online offers for "free stuff" – these pitches are likely either malware transmission ploys or phishing traps set to steal their personal information.
- Talk to your kids about the need for privacy. Make sure they understand not to share personally identifiable information (PII), especially via social media. PII can include their full name, birth date, home address, phone number, email address, or Social Security number.

If your kids are looking for an online activity, consider having them try the FBI's new "Safe Online Surfing" (or "SOS") website: sos.fbi.gov. SOS is a series of online games that teach valuable lessons about passwords, safe downloading practices, screening friend requests, and more. The site includes games for grades three through eight in both English and Spanish.

For additional information, visit the Consumer Protection Bureau at datcp.wi.gov, call the Consumer Protection Hotline at 800-422-7128 or send an e-mail to datcphotline@wi.gov.

Connect with us on Facebook at www.facebook.com/wiconsumer or Twitter: @wiconsumer.

###