NEWS RELEASE
Wisconsin Department of Agriculture, Trade and Consumer Protection
datcp.wi.gov

Cybersecurity Awareness Month Week Two: Securing Devices at Home and Work

Release Date: October 12, 2020

Media Contact: Ti Gauger, Public Information Officer, (608) 224-5007, Ti.Gauger@Wisconsin.gov

MADISON – The year 2020 saw major changes to the way many of us work, learn, and socialize online. Our homes and businesses are more dependent on the internet than ever. With more people now working from home, our personal and professional lives are more connected than ever, introducing a completely new set of potential security vulnerabilities.

During week two of National Cybersecurity Awareness Month (NCSAM), consumers and businesses are encouraged to focus on the steps users and organizations can take to protect their internet-connected devices for both personal and professional use.

There are several steps you can take to secure your devices at home and at work:

1. **Think before you click.** Phishing emails are sent to business email accounts to try and gain access to the businesses' systems. Clicking links may install malware or spy software onto your system.
    - Ignore unsolicited emails, social media messages, calls, or texts, especially if they create a sense of urgency and require you to respond immediately to a problem.
    - Be wary when these requests supposedly involve your online account, bank account, taxes, or package delivery. These messages are likely scams.
    - When in doubt, do not respond. If you question the legitimacy of a message that claims to be from a contact at a business or government agency, call the organization directly using a number from a legitimate source. Do not contact the organization on any phone number provided in the unsolicited call or voicemail. Do not click any links in the email, social media post or text message.
2. **Back up your data.** At any given time, you are one hard drive crash, errant delete, device theft, or malware attack away from losing your sensitive documents, and valuable files. One of the best ways to protect yourself from data loss is to regularly backup your data. Follow your employer's policies for work backups. Backups can be made using physical or cloud storage.
    - Physical storage includes local backups using removable media, including USB flash drives and external hard drives (or CD/DVD for smaller amounts). This method allows for fast and accessible storage, but can be expensive, and is susceptible to physical failure. Storage devices themselves may also be vulnerable to malware.
    - Cloud backups are data stored that is stored in secure online locations and accessible from anywhere, usually by multiple devices. This is the most secure method and can be accessed anywhere. Backups can be set up to happen automatically in real time. This method usually requires a subscription cost and regular internet access.

    After deciding on a storage method, follow these steps to complete your backup:

    - Prepare the documents, the files, and folders to be saved. Back up the most important files first. Clean up your files and folders before initial backup.

- Create a backup schedule that works for you. Consumers may want to back up important information once a week, while small businesses might do so daily. Most cloud services allow users to set a fixed schedule for auto backups.
- Verify the backup by loading information from the storage device back to the computer. You can also check the cloud to ensure that the data copy is intact.

Join us during the 17th annual National Cybersecurity Awareness Month (NCSAM) to **“Do Your Part. #BeCyberSmart.”** Learn more by following @WIConsumer on Facebook or Twitter.

###

Find more DATCP news in our newsroom, on Facebook, Twitter, and Instagram.