NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

College Students: Outsmart Social Media Scammers

Release Date: **August 28, 2017**

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

MADISON – Social media applications are everywhere: on our computers, our phones, our televisions and even in our cars. Nowhere is this more evident than on a college campus, where students use these apps as a means of making personal and professional connections to help them prepare for the future. But all of that goodwill can be undone by scammers and identity thieves who set up traps on these apps with a goal of capturing users' money and personal information.

The Wisconsin Department of Agriculture, Trade and Consumer Protection asks college students to help protect their identities and their wallets by tightening the security around their social media accounts and by thinking before they click on links in social posts.

"Academic and lifelong learning is the primary focus for a college student, and spending time undoing damage caused by a scammer or identity thief takes away from that experience," said Frank Frassetto, Division Administrator for Trade and Consumer Protection. "There are numerous scams targeting users of all of the major social media apps, and the best protection for a student is to limit the sharing of personal information and clicking of suspicious links."

Users of all services should set up complex passwords or passphrases for their social media accounts, turn on two-factor authentication if it is offered, and use the security features available in the apps to block public access to their posts. To avoid scams, users should be very suspicious of links in posts that direct them to unfamiliar websites or that advertise unrealistic offers for popular products.

Scammers often use fake account support emails to gather login details from social media users. These "phishing" emails falsely warn recipients that they need to provide their usernames and passwords in order to update a social media account or avoid an account suspension. Delete similar emails and log directly into the service if you need to check your account status.

Each social media application has its own risks for identity theft and scams. Watch for these app-specific risks:

Twitter:

- Watch out for links in direct messages from users you don't know. These links may be included with a message intended to draw you in, like "Can you believe this is true?"
- Watch for warnings from Twitter about unsafe links. According to Twitter, these links match a database of potentially harmful URLs which could lead to phishing, malware or spam sites.
- Buying followers and engagements and using "free followers" apps could compromise your account and may also violate Twitter's rules.

Facebook:

- Watch for "profile viewer tracking" service pitches – Facebook does NOT offer this feature.
- Hacked accounts can send malicious posts to everyone in your friends list, and the messages will post to their feeds (potentially attracting other victims). The links in

(MORE)

these posts could drive users to websites where malware is transmitted to their devices.

- Fake surveys and quizzes can be ploys to harvest personal information.

LinkedIn:

- Watch for "get rich quick" and work-from-home scams. Do your research on a company before you apply for a job posting, particularly if it seems too good to be true.
- Third-party websites claim to provide LinkedIn phone support for a fee, but these groups are not affiliated with LinkedIn. LinkedIn does not charge users for support and will not request login information from customers.
- Other common scams according to LinkedIn: mystery shopper offers, phony inheritance scams (advance fee scams), romance scams.

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

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

###