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

National Cyber Security Awareness Month, Week #2:
Your Best Defense Against Data Breaches? Your Employees.

Release Date: October 12, 2016

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

MADISON – For a business owner, the threats posed by a data breach are enough to keep you up at night — consider the legal ramifications, damage to your reputation, risk to your employees' sensitive financial and personal information, and the monetary cost of providing credit monitoring service to your affected customers.

As part of National Cyber Security Awareness Month, the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) asks business leaders to consider the strength of their company's data security plans and to share the importance of cyber safety across the organization.

"A business's cybersecurity plans may start in the boardroom, but its employees are typically the front line in the battle against online threats," said Frank Frassetto, Division Administrator for Trade and Consumer Protection. "Some of your strongest protections can come from training your team members on best practices for handling and storing sensitive data and on the risks of phishing emails."

Phishing emails have long been a way for cybercriminals to gather personal or banking information from a business's employees or to install malware on a business's systems in order to gain access to its records.

Recent phishing operations have become more sophisticated, however, with scammers sending targeted emails that use familiarity as a tool to make the message seem legitimate. In these "spear phishing" attempts, the scammer may have basic information about the employee including their name, title, co-workers' names or some other piece of specific information.

A scammer could forge (or "spoof") the email address of an executive and request passwords or sensitive information such as tax documents from a human resources or payroll employee. Or a scammer could spoof the address of a vendor and request financial records in order to "follow up on a sale" or ask a recipient to download and review a malicious attachment.

"By posing as a friend or business contact, the scammer is banking on the employee opening a link or an attachment to learn more about the inquiry or to accommodate what appears to be a legitimate request for information," said Frassetto.

Data security is a complicated issue, but taking simple steps (such as setting up firewall safeguards or teaching employees how to spot and handle questionable email requests) can pay dividends in the form of added protection. Kick start a data security evaluation for your business by downloading free educational tools on the DATCP website (datcp.wi.gov). There you will find: the "Fraud Against Business" fact sheet, a handful of business resources from the Federal Trade Commission, hotline numbers and identity theft resources. You can also request a presentation from a Bureau of Consumer Protection representative to your company or community group.

Take action this Cyber Security Awareness Month. Your business, employees and customers all depend on you.

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.

###