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

This April Fools' Day, Don't Get Reeled in by Phishing Emails

Release Date: March 28, 2019

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

MADISON – For the ultimate tricksters – scammers and identity thieves – April Fools' Day is just one of 365 chances to rip you off each year. And it is a rare day when they don't pitch one of their favorite tricks your way: the phishing email.

Fake emails, sent to the general public, are a cheap and effective tool for scammers. There are a wide range of phishing email ploys that criminals use to steal money and personal information from unsuspecting consumers or to transmit malicious software to those consumers. Phishing emails often include vague details, prompting the recipient to open an attachment or click a link to find out more – taking either action can put your finances, identity, and device at risk.

Some of the common phishing email ploys include:

- Fake shipping emails made to look like they are from a legitimate shipper like UPS or FedEx. The emails claim that you have a package waiting or that there is a problem with a delivery. The recipient is prompted to open an attachment for the shipping details or to click a link to review their "account."
- Fake account closure emails that appear to be from major corporations like Microsoft or Amazon. The messages claim that you have an account at risk of closure and that you need to log in (using a provided link) to update your information.
- Fake gift card promises tied to the recipient's supposed participation in a "reward program" from a major retailer.
- Fake invoices and threats about past-due taxes sent using the names of government agencies.

The good news for consumers is that email scams can be easy to spot – but only if you know what to look for:

- Never click a link or open an attachment in an unsolicited email or text message.
- Phishing emails often include the name, logo, and color scheme of a well-known business, so the tipoff of a scam is often in the language used in the message. Watch for poor grammar, misspellings, awkward wording, and a general lack of professionalism. Legitimate corporate emails will be clear and grammatically accurate.
- Check the sender's email address for another easy tipoff. In many phishing messages, the web address (URL) referenced in the sender's email address does not match the true URL for the business in question. For example, an email that claims to come from the U.S. Postal Service may come from "JoeSchmo@somefakecompany.com" instead of "___@usps.com."
- Be suspicious of any request to open an attached file or click a link (including to "view your account"). Either action could lead you to download malware onto your device.
- On a desktop or laptop computer, if you hover your mouse over a link in an email (do NOT click your mouse!), the URL that the link directs you to will typically appear in the bottom of your browser window.

(MORE)

- Most of these emails end up in your "junk mail" folder if your security settings are high and your email provider is routing correctly, but the occasional junk email inevitably finds its way through the filters and into your inbox.

Refuse requests to reply to an email with confidential information such as user names, passwords, and personal details. If you question the validity of an unsolicited email that claims to be from a major business, call the business directly to inquire about its legitimacy. If you question the status of an online account after receiving an unsolicited email, visit the company's website directly and log in – don't log in using a link in the email.

For additional information or to file a complaint, 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.

###

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