

Dept. of Agriculture, Trade and Consumer Protection: Every day is April Fool's Day for email scammers

Posted on Thursday, Mar 30, 2017

>> **WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. [Get the app or access via desktop.](#)**

Media Contact: [Jerad Albracht](#), Senior Communications Specialist, [608-224-5007](#) or [Bill Cosh](#), Communications Director, [608-224-5020](#)

Spam Email Screenshot Examples (.jpg files): [#1](#) [#2](#) [#3](#)

MADISON - When someone plays a harmless prank on April Fool's Day, usually you laugh it off. After all, it's safe to assume that the tricks stop by the next morning. But for email users, every day is another chance to get tricked by a scammer. Scammers see email as a cheap way to send batches of rip-off attempts (known as "spam") all over the world with one click. The Wisconsin Department of Agriculture, Trade and Consumer Protection asks Wisconsin residents to be on the lookout for phony email pitches that could put their finances and personal information at risk.

"Some spam emails are carefully crafted and appear to come from legitimate sources while others are poorly constructed but aim to draw you in with over-the-top claims," said Frank Frassetto, Division Administrator for Trade and Consumer Protection. "Regardless of appearance, the risks to your finances and sensitive information are the same. Any messages you receive need to be carefully screened and deleted if you suspect they are fake."

A number of recent spam emails have falsely promised a gift card for a major retailer. The email subject lines include "Thank You!," "Congratulations!," or something similar. The emails appear to contain separate links for different actions, but the entire content of the email is actually one graphic that is presumably linked to a malicious website. You will be sent to that same address regardless of where you click on the message.

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

Keep these tips in mind to avoid spam emails:

- Watch for poor grammar, misspellings, awkward language choices and a general lack of professionalism. Legitimate corporate emails will be clear and grammatically accurate. A spam email may have the name, logo and color scheme of a well-known business, but these language clues can tip you off to a fake message that otherwise appears to be real.
- Check the sender’s email address for another easy tipoff. In many spam 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 cause you to download malware on your device.
- 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 appear in the bottom of your browser window.
- 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 email that claims to be from a major business, call the business directly to inquire about its legitimacy.

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](tel:800-422-7128) or send an e-mail to datcphotline@wisconsin.gov.

Connect with us on Facebook at www.facebook.com/wiconsumer.