Wisconsin Dept. of Agriculture, Trade and Consumer Protection: Fake Amazon order cancellation emails making the rounds

Posted on Thursday, Jun 29, 2017

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

Screenshots of fake emails (links in screenshots are inactive): email #1 email #2

MADISON – Did you get an order cancellation email from Amazon.com for a product you don't remember buying? It may be a scam. Do not click any links contained in the email.

The Wisconsin Department of Agriculture, Trade and Consumer Protection is aware of a phishing scam involving fake Amazon order cancellation emails and asks consumers to be suspicious of any similar emails they receive. If you click any links in the email, you could unintentionally download malicious software onto your device or be driven to a site that aims to collect your Amazon account username and password or other personal information.

If you receive a cancellation email and you wish to inquire further, do NOT click the links in the email. Instead, go directly to Amazon.com or use the company's app to check your account. If you share access to an Amazon account with a family member, check with that person to see if they did cancel the supposed order before you take any additional action.

In most fraudulent emails, you can check the sender's email address for an easy tipoff – the web address (URL) referenced in the sender's email address does not match the actual URL for the business in question (see screenshot example #1). For example, a fake email that

claims to come from Amazon may have a sender address of "JoeSchmo@somefakecompany.com" instead of "___@ amazon.com."

But some of these phony Amazon cancellation emails have had "spoofed" sender addresses that actually appear to come directly from "___@ amazon.com" (see screenshot example #2). Consumers should be aware that spoofing of email addresses is possible and that the displayed sender address may not be legitimate.

With this in mind, the best way to avoid being scammed is to simply delete similar emails and go directly to Amazon.com or the company's app to check your account.

Follow these additional tips to spot and avoid spam emails:

- Hover your mouse over any link in the message (again, do NOT click your mouse!). The URL that the link points to will appear in the bottom of your browser window. If it does not match the sender's URL, the email is likely a fake.
    - NOTE: in the case of the two messages attached to this alert, one had links that would direct a victim to a website for models and the other to a tech company – both of these pages were likely compromised.
- Be suspicious of any request to open an attached file or click a link (e.g. "view your account" or "unsubscribe here"). Either action could lead you to a compromised website where your device and personal information are at risk.
- Watch for poor grammar, misspellings, awkward language and a general lack of professionalism. Legitimate corporate emails will be clear and grammatically accurate.
- Refuse requests to reply to an email with confidential information such as user names, passwords and personal details.

For additional information, visit the Consumer Protection Bureau at http://datcp.wisconsin.gov, send an e-mail to datcphotline@wisconsin.gov or call the Consumer Protection Hotline at 1-800-422-7128.