THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

November 2022

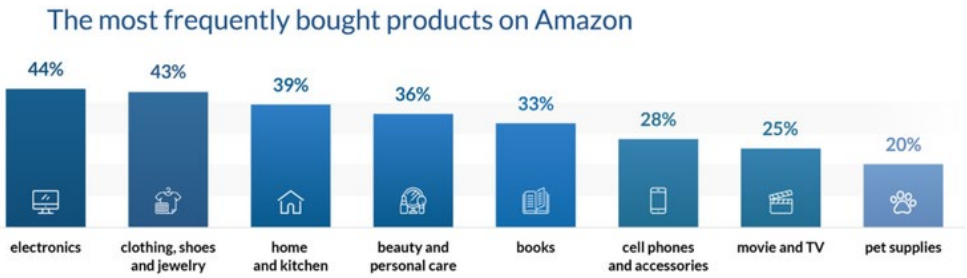
Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

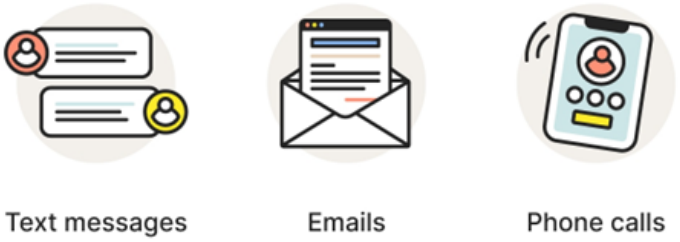
With the holidays right around the corner and the Black Friday shopping season coming up (that never seems to end) it is time to be a bit more vigilant when shopping in person and online. Although scammers work all year around, they greatly increase their efforts during the high traffic, high spending, holiday season. For this month's news article I thought I would bring to light a few items that will help keep you safe from cybercrime.

Text Messages, E-mails, and Phone Calls

Cybercriminals always take advantage of distracted behavior such as the emotional state of urgency. Be aware that when purchasing popular products, such as item(s) that are the latest craze and in high demand this holiday season, you will likely see messages targeted by scammers who are actively reviewing online vendor sales activity. Considering that popular sites like Amazon are often e-mail spoofed, cybercriminals are most likely to catch someone off guard by sending mass e-mails that look like they came from Amazon.



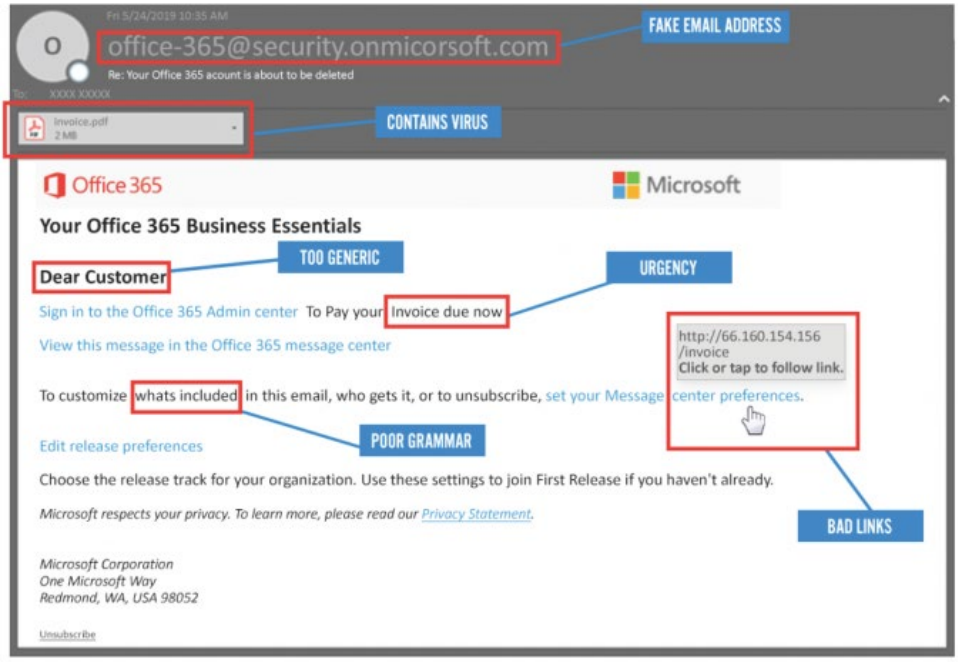
What does this mean? Expect more Phishing emails and spam text messages than normal that will be targeted, i.e., look very close to what vendors normally send out (e-receipts, text advertisements or e-mail advertisements). Expect an uptick in spam phone calls where criminals pretend to be affiliated with a vendor/store asking for any financial information to give a refund or even ask for you to install an application on your computer in order to give you a refund.



As a review:

- Never provide sensitive information over e-mail or text messages.
- Always verify the sender of a message by calling direct and not using information in a sender's message.
- Never click on any links provided by suspicious e-mails or texts.

How do I identify a malicious e-mail? Here are some things to look out for:



Extra precautions

Your credit cards may have extra security features available to keep you safe when using them.

- **Text to confirm:** Whenever you are using a credit card, you can have a text message sent to you for purchases over a specified amount. Such charges can be put on hold until you reply **Yes** to the text message.
- **Temporary purchase number(s):** Some credit cards allow you to generate single-use card numbers for online purchases.
- **Virtual credit card number(s):** These are digital versions of your physical card. They're often provided to prevent fraud and identity theft while shopping online or over the phone. If anything happens to your virtual card, you can delete it and get a new one.
- **Lock your Card from further use:** Some cards allow an app (or available on card issuer website) to lock your credit card from being used at the push of a button. The lock halts future transactions from occurring.

Anything you want to see in a future newsletter for December? Please let us know if there are any topics you are interested in. We welcome and are open to any suggestions. E-mail suggestions to security@bsd.uchicago.edu.