@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

November 2018

Ready, Set, Shop - Safely

Consumers say they will spend an average of $1,007.24 during the holiday season this year, up 4.1 percent from 2017, according to the National Retail Federation.

HOLIDAY ONLINE HAZZARDS

The holiday shopping season is prime time for cyber criminals to target online shoppers and harvest their banking details, website logins, and personal information. Below are scams that are prevalent this time of year.

- **FAKE WEBSITES -** Many of these nearly mimic the actual retailers' sites with their levels of sophistication in logos and product photos. Look in the address bar of your browser to check the URL. Misspellings and addresses that don't correspond with the retailers' name are signs of a scam site. Also, be sure to check for the lock symbol in the browser address bar, indicating the webpage connection is secure, as verified by a trusted third-party authority.

- **eCARDS -** Many people send holiday e-greeting cards. Malware can be hidden in email attachments, and criminals can create emails with links to "retrieve cards" that direct users to phishing sites.
- **GIFT CARDS** - Phony gift cards, stolen gift cards, and legitimate gift cards purchased using stolen credit cards are abundant online. Be safe and buy gift cards directly from the vendor or from a store that you know is legitimate. Be wary of emails that claim you have won a gift card; these are rarely legitimate.
- **DELIVERY NOTIFICATIONS**- During this season many of us receive items shipped by UPS, FedEx, and the US Postal Service. Criminals exploit this by sending emails and text messages that impersonate correspondence from these services and that deliver malware via attachments or direct users to phishing websites. Track your deliveries by typing the shippers' URL address into your browser.
- **FAKE SHOPPING SURVEYS** - Be wary of surveys that offer big rewards for participation, especially those on social media. Avoid clicking on survey links in emails or shared on social media.

WELCOME OUR NEW CSO

DTI welcomes **Solomon Adote** as our Chief Security Officer. Solomon will be responsible for enhancing and improving the state's cyber security strategy, including the design and execution of the Delaware Information Security Program and the Continuity of Government and Disaster Recovery Program.

"Cyber security is more important now than ever and we are excited to welcome Solomon back to lead our efforts," said Chief Information Officer James Collins. "He brings a great blend of organizational and tactical information security experience."

For more information for safe online shopping:

- https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/
- https://www.netsafe.org.nz/online-shopping
- https://www.us-cert.gov/ncas/current-activity/2017/11/16/Holiday-Scams-and-Malware-Campaigns

Visit the DTI Digiknow website for previous issues

eSecurity Newsletters

Questions, comments or topic suggestions?
Email us at eSecurity@state.de.us