

Public Forum

Page 6

Wednesday, December 10, 2014

Don't forget about holiday online security

By James Collins

Cyber Security professionals have coined a new term, "data breach fatigue," to explain why many consumers are becoming complacent about protecting their personal information because they now believe that data breaches are inevitable and just a part of today's digital world.

Over 120 million customers' credit- and debit-card information was compromised by data breaches at major retailers this year. A federal organization announced this month that another 53 million customers' and 750,000 employees' personal information may have been compromised. Data breaches are up by 25 percent compared to the same period last year. There have been over 600 breaches this year, which is about two per day.

The Ponemon Institute reported that more than one-third of consumers ignored data-breach notifications and did nothing, while more than 50 percent "did not take any steps to protect themselves from identity theft afterwards."

My staff and I are passionate about protecting Delawareans and offer the following tips for safeguarding your personal information this holiday shopping season. These strategies are not entirely breach-proof but they can help you to have a more-secure online shopping experience.

There are three common ways that cyber attackers can take advantage of online shoppers:

- Targeting vulnerable computers: If your device is not protected from viruses or other malicious activities, an attacker may be able



"Unlike traditional shopping, where you are in a physical building, attackers can create bogus websites that appear to be legitimate online stores. Charities may also be misrepresented in this way, especially during the holiday season."

— James Collins

to gain access to your information. Make sure that your anti-virus protection is active and up-to-date.

- Creating fraudulent sites and email messages: Unlike traditional shopping, where you are in a physical building, attackers can create bogus websites that appear to be legitimate online stores. Charities may also be misrepresented in this way, especially during the holiday season. Attackers create malicious sites and email messages to try to convince you to disclose personal and financial information. Pay close attention to the web addresses of the sites you are using to ensure you have not been redirected to a fraudulent site.

- Intercepting insecure transactions: If an online vendor does not encrypt (transmit the data securely) or protect the buyer's data, an attacker may be able to intercept the information as it is being transmitted. Limit your purchases to trusted, secure sites of companies you know are legitimate.

To help thwart attackers and be cyber-shopping savvy, follow these simple guidelines:

- Keep a Clean Machine — All devices used for shopping should have up-to-date software, security, operating systems, programs and apps.

When in Doubt, Throw it Out — Links in online advertising, texts, tweets and posts are ways cybercriminals compromise your information. If it looks suspicious, delete or mark as junk email.

Be Savvy about Wi-Fi Hotspots — Sure, it might be nice to shop online while sipping a beverage in your favorite coffee shop, but unsecured Wi-Fi networks that don't require a password can be cybercriminals' best sources for capturing your personal and financial information.

Make Sure the Site is Secure — This includes a closed padlock on your web browser's address bar and a URL address that begins with s-http or https.

Use Safe Payment Options — Credit cards are generally the best option because they help buyers seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Check your card-issuing establishment to know what their policy is in the event of identity theft.

For more information on cyber safety and security, go to: <http://digi-know.delaware.gov>.

Editor's note: James Collins is the state of Delaware chief information officer.