10 cyber savvy holiday shopping tips

James J. Giszczak | Monday, November 25, 2019

The holiday season is upon us, and with it comes a huge surge in cybercrime. Increasingly, hackers and cybercriminals are taking advantage of the increased volume of shopping this time of year to steal personal and financial information. In 2017, organizations reported a 57.5 % increase worldwide in attempted cyberattacks between Thanksgiving and New Year's Day with spikes on Black Friday/Cyber Monday and a notable uptick in the days immediately following Christmas, according to Carbon Black's 2018 Holiday Threat Report. This increased threat applies to both businesses and individuals.

Organizations are often short staffed during the holiday season and individuals who focus on cybersecurity or incident response may be out. Temporary staff, who have not received training on things like phishing, may be filling in for those who would typically be more alert for these types of attacks. Exacerbating the risk at this time of year is the non-stop flood of emails appearing in inboxes offering amazing holiday deals. Unfortunately, one wrong click can make for a very unhappy holiday.

With increased cyberthreats posing a significant risk to individuals and businesses, now is the perfect time to get cyber savvy for the holidays. Here are 10 cyber safety tips to keep in mind as you do your holiday shopping this year.

1. Shop secure, reputable sites – Secure websites start with "https," not simply "http." The "s" indicates the website is encrypted and your information is more likely to be protected as it travels to a server. On almost all browsers secure websites will have a padlock icon next to the URL, and some will also indicate whether a site is secure or not using red or green in the address bar. Websites that are Verisign approved (look for their seal) add another level of security that makes it difficult, but not impossible, for your information to be captured by cybercriminals.

And before you use that secure website, make sure your online purchase is from a real company. Scammers regularly set up fake websites or apps, but do so increasingly during this time of year to take advantage of unsuspecting shoppers looking for deals. With U.S. holiday spending reaching $850 billion in 2018, a study by RiskIQ collecting data in the month following Black Friday identified 169,138 malicious apps, representing a 220% increase. If you're searching for this season's hottest holiday gift and find it for a price that seems too good to be true – it probably is. Other red flags include poor grammar and misspellings, or when a website advertises high availability of hard-to-find items. Do research on the company before purchasing from less-familiar websites to make sure you aren't just giving away your personal and financial information to a hacker. Read any customer reviews available, check for complaints with the Better Business Bureau, and look to see if they have a phone number or physical mailing address listed anywhere on the website.

2. Check out using services where credit card information is already stored – The rise of "internet skimming," or Magecart attacks, in 2019 has seen internet crooks find ways to add code to the websites of reputable companies. This code, which can be embedded outside of an organization's firewall using malware infecting third-party partners (see Ticketmaster's 2018 breach) is capable of capturing data as it is entered and even redirecting shoppers from a reputable site to a malicious site. In October, the FBI issued an alert about an increase in Magecart attacks, which are difficult for consumers to recognize. Because it is always safer to enter credit card information once rather than on multiple occasions, shoppers can find some safety by taking advantage of the already stored information on websites of trusted larger companies. For example, if you have a credit card saved on Amazon, look for the opportunity to use Amazon Pay if available while shopping other sites. Apple Pay and PayPal can offer similar benefits through their use of one-time-use tokens that can't be reused even if the information is captured by cyber criminals.

3. Use credit over debit, or use alternative payment methods – Using a credit card instead of your debit card provides you with a few small layers of protection. If your credit card information is stolen, in most cases you are only liable for up to $50 of unauthorized charges. Always make certain you check all statements and timely dispute any fraudulent charges. Most credit cards have security features that can and should be utilized this time of year, such as setting a limit on the amount spent on a single purchase or the number of times a card can be used in one hour. As you use your credit card, don't wait for the monthly statement to review the charges. By regularly monitoring your account and your statements you can identify discrepancies early and dispute them. It is best to get an alert when each purchase is made so you can immediately dispute an unknown charge. Instead of regular plastic, also consider using PayPal, Google Wallet, or Apple Wallet for an added layer of protection.

4. Protect your passwords – It is tempting to say "yes" to your web browser storing your password and login information for shopping websites you frequently use. Doing this, however, is just asking for trouble.

As you are shopping online this holiday season, use different passwords for different websites and accounts. Change your passwords regularly, but certainly after the holiday shopping season is over. When it comes to selecting a password, avoid using personal information (birthday, mother's maiden name, etc.) that someone could easily guess based on what is available about you online. And please do not use PASSWORD or 1234. You laugh, but they are the most common passwords used. Whenever possible, set up multifactor authentication for your accounts.

5. Only give what information is necessary for rewards accounts – Almost all stores and restaurants offer some type of reward program that requires you to set up an account. While it can be worth it to score extra discounts and promotions during the holidays, when setting up your account make sure that you only provide the information that is necessary. The more personal information you give away, the greater the risk. And remember, no rewards program will ever need your Social Security or driver's license number.

6. Don't get hooked by a phishing scam – This time of year, phishing emails are often designed to look like confirmation for purchases or updates on shipping information. The best defense against phishing scams is simple – don't open emails from unknown senders and don't click on any links. If you're unsure whether an email you received is legitimate or not, manually type the address into your browser to visit the website to confirm whether the requested action in the email is legitimate. When it comes to tracking packages, go directly to the carriers website and manually type in the shipping tracking number you were given instead of clicking on a link from an email.

7. Be vigilant when shopping in person too – If you're someone who still loves shopping in stores, keep an eye out for skimmers placed on regular card readers or bank ATMs. These devices placed in the mouth of a payment card reader copy the information stored on the magnetic strip of your card for criminals to use or sell online. Also be aware of your surroundings any time you are using your card. The person behind you talking on their phone or taking a selfie could actually be stealing all the information they need to go on their own spending spree.

8. Donate wisely – Many people use this time of year to make charitable donations – and many cybercriminals use this time of year to take advantage of that charity. Make sure you are knowledgeable about any organization before handing over your financial information or donation. Check the IRS database of charities or look the organization up on Charity Navigator or Guidestar.org. Never make a donation over the phone to an unsolicited caller. And any organization that asks you to wire money overseas is a big red flag.

9. Activate transaction alerts on all credit cards and bank accounts – Most credit card companies and banks make this safety feature free for customers. With the ability to send messages to a shopper's cell phone asking if they made a particular purchase with a prompt to reply "YES" or "NO," the alerts offer the ability to confirm or dispute a transaction in real time.

10. If you fall victim to a cybercrime, report it to the FBI – The FBI's Internet Crime Complaint Center, or IC3, was created in 2000 with the mission of providing the public with "a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness." In addition to providing a form to file a complaint, the IC3 website offers valuable information on current threats in its Press Room.

10 cyber savvy holiday shopping tips?utm_campaign=NEW Newsletter – Business Advocate Digest

These criminals are not going away. In fact, it is just the opposite - they are getting much better at their craft and the wave of cybercrimes is growing exponentially. While you cannot eliminate this threat, you should take all steps you can to reduce the likelihood of becoming a cyber victim. Give yourself a real holiday gift and be cyber savvy while enjoying the holidays with friends and family!

James J. Giszczak

Team member bio