How to Avoid the Top Five Holiday Shopping Cyber Threats?

This special report is published on behalf of WatchGuard Technologies and LogicalTech by Cassidy Poon, National Marketing Manager for LogicalTech Group and Cassidy Poon is one of Australia's leading B2B Enterprise Technology Media Publicist.

Perhaps you're the type of person who gathers all the ads on Christmas morning, planning how your family can synchronously hit three different stores to reap all their door-buster deals. Maybe you're that guy who scours the Internet for early leaked copies of Monday's sales, programming your scripts to ensure you're the first to click buy. Or perchance—like me—you'd rather sleep in with a full belly and let others battle it out. Whichever profile fits you, Christmas & Boxing Day are coming, launching us into the busiest shopping season of the year… and bringing the cyber criminals scurrying out of the cracks in droves.Criminal hackers follow the money. They track big trends and know when the biggest shopping seasons occur. Plus, like all good social engineers, they're masters of human psychology, preying on our behavioral weaknesses to get what they want. You can bet criminal hackers are just as excited about the holiday sales season as the discount-seeking shoppers. For that reason, it's important you enter this period with a little awareness and your eyes wide open. To help with the former, here are the top five cyber threats to watch out for during the shopping season:1. Seasonal email phishing scams:Attackers know you have your eye out for emails containing the latest sales and discounts and that you may have packages in transit from recent purchases. This makes it a great time for them to leverage some seasonal phishing scams to try and lure you to malicious sites or malware. Some of the most common malicious emails during the holidays are fake UPS, FedEx, or DHL messages claiming a delivery failed, bogus flight notices, and even phony secret Santa messages. All of these seasonal scams prey on common trends for the season, such as holiday vacations and trips, and people ordering more stuff online. To give you a specific example, right now a nasty new ransomware variant called Cryptolocker is spreading using the fake FedEx or UPS trick, and has cost many victims a lot of money. Avoid clicking links and attachments in unsolicited emails.2. Fake product giveaways:Every year the holiday shopping bonanza brings us at least one or two "must-have" items for the holiday season, whether they be Tickle-Me Elmo dolls or the latest gaming console. Cyber criminals always seem to recognize these popular consumer items early, and use them to lure unsuspecting victims to their trap. This year, two such items are the latest video game consoles—the PlayStation 4 and Xbox One. We've already seen phishers trying to steal personal information from victims by tricking them into filling out details to win one of these next-generation consoles. While some of these giveaways might be legit, you should be careful where you share your information, and what type of information you're willing to give up.3. Dastardly Digital Downloads:During any special event or holiday, malicious hackers often pull out old reliable tricks of the trade. One such trick is the free screensaver, ringtone, or e-card offer. The attackers can easily theme their free download offers from whatever holiday or pop culture event they want, be it Thanksgiving, Christmas, or whatnot. If it sounds too good to be free, it probably is. As always, be careful what you download.4. Fraudulent e-commerce sites:The bad guys are great at faking web sites. They can fake your banking site, your favorite social network, and even online shopping sites that have suspiciously good deals for that one hot ticket item you're looking for during the upcoming sales. Of course, if they can lure you to their replica sites, they can leverage your trust in them to steal your personal information, swipe your credit card number, or force you into a drive-by download malware infection. Pay close attention to the domain names you visit, and vet your online retailers before ordering from them.5. Booby-trapped Ads and Blackhat SEO:Bad guys are always looking for new ways to attract you to their fake or malicious web sites. Phishing emails, instant messages, and social network posts with appealing links work, but they always experiment with new lures. Two popular new techniques are malicious online advertisements and evil search engine optimization (SEO) tricks. By either buying online ad space, or hacking online ad systems, hackers can inject fake advertisements into legitimate web sites, which redirect back to malicious sites. They can also leverage various SEO tricks to get their web sites to show up in the top results for popular searches. Are you searching for Lululemon yoga pants sales for your girlfriend this holiday?If criminals think that's a popular gift, they can poison search results and hijack ads to use your interest against you. As you consider clicking ad links or following search results, be aware of the domains and URLs you click on.The top five threats above all have consumers in mind, but let me share one last holiday cyber threat that merchants need too look out for; Distributed Denial of Service (DDoS) attacks. Cyber criminals realize the holidays are a very important seasons for online retailers—especially days like Cyber Monday. They know that even an hour of downtime can translate into millions in lost sales for big retailers, and they want to steal a piece of your pie. Expect to see some DDoS attacks targeting online store during the holidays, followed by extortion letters asking for money to stop the attack.One of the best defenses to cyber attacks is a bit of awareness and vigilance. Now that you know what types of threats and scams to expect this holiday season, you can look out for them, and avoid becoming a patsy. While I shared a few security tips already, let me summarize a few other steps you can take to make your holidays hacker free.1. Patch your software – If you let Microsoft, Apple, and Adobe (and other products) automatic software updates patch your machine regularly, you will remain safe from most cyber criminal's technical attacks.2. Don't click on unsolicited links or attachments – Enough said.3. Look for the padlock while shopping online – Though it's no a guarantee you're on the right site, do not share your personal or financial info with an online

retailer unless you see a green padlock in your web browsers URL dialog (the icon’s appearance may differ slightly depending on your browser).4. Use password best practices on shopping sites – You should use different, strong (i.e. long) passwords on every site you visit. If you are not familiar with password security, this post has some good advice.5. Vet online merchants before clicking buy – A little online research can go a long way. Do Internet searches on a merchant before buying from them, paying close attention to customer reviews. When people get scammed they tend to share, so a little research can help you identify fakes retailers.The holidays should be about family and fun. Keep your eye out for these five top threats and follow my basic security tips and you’ll surely enjoy a happy holiday season, and hopefully nab a cool treat for you and your family during this shopping season.LogicalTech is one of the leading Professional Partner with WatchGuard Technologies in Australia. Find out more by contacting an authorized WatchGuard reseller, LogicalTech today. Visit us at www.logicaltech.com.au or follow our techblog at www.logicaltechgroup.com

Contacts

Cassidy Poon
0386436444
mailto: cassidyp@logicaltech.com.au