4 Tips to Protect Against Cyber Thieves During the Holidays

December 21, 2017
by SentinelOne

It's the busiest time of the year for shopping. Americans are on pace to exceed last year's record-setting online holiday spending, while cyber thieves are also on track to exploit those digital processes with newly developed viruses, and highly sophisticated malware. Consumers who want to benefit from the sales without losing their shirts to thieves should be prepared for what will undoubtedly be an eventful holiday shopping season.

High Holiday Expectations

During the 2017 holiday season, Americans are expected to fork out more than 3 percent more for gifts and goodies than they did last year, averaging a total of $967 per shopper. And for the first time, online buying is expected to surpass traditional mall wandering.

Consumers are also expected to rely more than ever on their digital devices to seek out and complete their purchases. In many cases, however, mobile devices do not provide the same level of security that desktop or laptop computers have, making those users vulnerable to a higher-than-normal risk of cybertheft.

High Holiday Security Needs

So, since it is certain that cyber thieves will also be using the latest and greatest in security-breaching tools to up their thieving game, shoppers who plan to use any digital tool, mobile or fixed, should follow four basic steps before getting started:

1. Update Everything

Web browsers, operating systems and banking apps periodically release updates with improved security measures. Figure out which programs will be used for online shopping purposes and be sure to have the most up to date version installed before starting your holiday shopping.

2. Update Your Passwords

2017 has been a year filled with headlines surrounding major breaches. Chances are that if you have not changed your password over the last 6 months your information could be floating around the Dark Web. Change your password, if only for the holiday season while attackers will be the most active. The action may prove especially beneficial when digital devices automatically access banking information. Highly secure passwords include letters, numbers and symbols; highly secure shoppers use a unique password for each account.

3. Add Additional Layers of Authentications

After the password, authentication layers add increasing complexity to account access and can alert you to most hacking attempts. Some sites will text or email an access code through which that one and only transaction can occur. Other sites ask for data specific to the shopper such as the name of their first cat or favorite childhood friend. Consumers should always reply affirmatively when given the option to require additional authentication before each account access.

4. Ensure the Website Is Secure Before Shopping

Of course, retailers are also highly sensitive to the possibility of digital hacking on their sites (See how SentinelOne can help Here). Merchant giants such as Target, TJ Maxx and eBay have all paid out millions of dollars to consumers whose data was stolen after shopping on their e-commerce sites. Consequently, many have added security features specifically to protect their patrons, one of which is the little green padlock at the front of the URL that denotes the site is secure. A safe site is also indicated when that URL begins with HTTPS instead of just HTTP.

Conclusion

Ensuring proper "cyber hygiene" is a process, not an event, and every consumer and corporation benefits when they exercise safe browsing and computing practices all year round. However, by employing these tips throughout the holiday shopping season, consumers make themselves a more difficult target and reduce their chances of becoming a victim as we enter the new year!

For enterprises serious about their security, check out SentinelOne and see why Fortune 500 companies are switching from their traditional solutions.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- 8 Visionary Predictions for Information Security in 2018
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls
- How to Modernize Vulnerability Management in Today's Evolving Threat Landscape