12 Cyber Tips to Avoid Holiday Hacks

While your household may be a merry and bright this holiday season, let us not forget what tends to be our most joyous time of the year is also our most vulnerable—especially when it comes to your cybersecurity. Hackers count on the chaos of the holiday season to infiltrate our most private information. So, instead of attracting attention, consider making yourself invisible during the holidays with these 12 tips.

1. SHOP FROM WEBSITES YOU KNOW AND TRUST.

Don’t click on “Christmas deals” or “hot deals” that aren’t likely too good to be true. Scammers often can blend into your interests, offering small discounts or deals to get the click. Now is NOT the time to experiment with new retailers and apps.

2. LOOK FOR THE LOCK.

Secure websites will often have a lock icon in the browser address bar to indicate it is a secure connection.

3. UPDATE YOUR OPERATING SYSTEM.

With a little more down time during the holidays, take a few minutes to update your operating systems as you would at any time. This will go a long way for apps on your phone.

4. DON’T GO “PUBLIC”.

Avoid public Wi-Fi when using the Internet, especially when accessing sensitive data like your bank account balance or emails.

5. DON’T CLICK ON LINKS.

Scammers will impersonate real stores and sites to get you to open the email with a link within them. Be smart and open the link for them to install malware on your computer and before you know it, your data is stolen and compromised.

6. GET CREATIVE WITH IDENTITY QUESTIONS.

Your mother’s maiden name or favorite hobby are most likely to be found online somewhere, so try getting creative with your security questions to access your accounts. Choose a metric you’re likely or choose an answer to a question that is completely opposite of the actual answer you would normally select.

7. UNABLE AUTO CONNECT.

Some devices will auto connect to available network behavior. Disable this function so that you can ensure you are connected to wireless and Bluetooth networks only when you want to be. Removing being connected is the opportunity time for hackers to cause damage right under your nose.

8. STORE DEVICES WHEN AWAY.

If you’re a busy executive, criminals seek out new paths to hack your devices. For unattended locations, especially where attending conventions or trade shows where guests need taxis more vulnerable to attacks (just install to become a list of your personal information or data). Let someone in a convenient location.

9. DISABLE AUTO CONNECT.

Some devices will automatically connect to available WiFi networks. Disable this feature so that you can ensure you are connected to wireless and Bluetooth networks only when you want to be. Removing being connected is the opportunity for hackers to cause damage right under your nose.

10. WATCH YOUR BANK AND CARD ACTIVITY.

If you’re not careful, hackers can see your financial activity when you’re sleeping and when you’re awake. Regularly monitor your bank account and card activity and update your financial service provider if you notice any suspicious activity.

11. PRACTICE PERSEVERANT PRIVACY.

Hackers aren’t just looking to exploit individual data, they also target businesses knowing many take extra time off this time of year to spend with families. Ensure your company has strong cybersecurity practices in place and key members of your threat intelligence, analytics, and fraud teams are consistently practicing responding to these scenarios.

It’s important to practice safe online behavior all year round, but the holidays bring about an extra level of digital activity that bad guys love to exploit. Make sure you are taking proactive measures to ensure you are having the most wonderful time of the year on and off-line—and cybercriminals aren’t.

To ensure your cyber team is prepared for any potential cyber predators, consider Project Ares as your safeguard platform to practice proactive cyber readiness techniques during the holidays—and year-round.

LEARN MORE ABOUT PROJECT ARES

PROJECT ARES

303.413.8800 • www.circadence.com • sales-cyber@circadence.com

HEADQUARTERS Boulder, CO 80302
ADVANCED RESEARCH & DEVELOPMENT FACILITY Tupelo, MS 38864
CENTER FOR CYBER AUTONOMY San Diego, CA 92123
WASHINGTON D.C. SALES McLean, VA 22101

©2019 Circadence Corporation. All rights reserved. Circadence, the Circadence logo, Project Ares, and the Project Ares logo, are trademarks or registered trademarks of Circadence in the US and other countries.