Monthly Cybersecurity Tips Newsletter
November 2022 VOLUME 17, ISSUE 11 • 2022

Shop Smart and Stay Safe This Holiday Season

From the desk of Paul Hoffman, Director of MS-ISAC Member Engagement

'Tis the season for holiday gifts and shopping! To avoid waiting in lines and traffic, many people opt out of going to malls and choose to shop online.

Cyber threat actors (CTAs) are aware of that fact, and it is their time to be active and develop new methods of tricking people. Be vigilant and avoid falling into their traps. Act and protect your personal and financial information.

The security tips below will help reduce the likelihood of your information falling into the wrong hands and ensure that you have a more hassle-free shopping experience this holiday season.

Avoid Using Public Wi-Fi

- While using public Wi-Fi is convenient, it is not secure.
- Public Wi-Fi does not protect your sensitive data, and CTAs may access your personal and financial information.
- Abstain from using public Wi-Fi at all costs while purchasing and placing orders.
- Confirm that you do not allow the "Connect automatically" Wi-Fi network preference on any of your devices.

Shop Safely

While shopping and making payments, verify the following:

- The internet connection is secure. If you are required to provide a password to access a Wi-Fi network, this will indicate that the communication between your device and the wireless router is encrypted.
- Payment sites have SSL protection, i.e., the URL should begin with "HTTPS." Avoid making any payments to sites that do not have the "s" after the "HTTP."

Check Shopping Sites

Browse sites that are well-known, legitimate, and secure. Please check for the following:

- The site has a “lock” (padlock symbol) in the URL bar. This means the website is secure, i.e., the information between your browser and the server is encrypted.
- The URL starts with “HTTPS,” which indicates that the site uses encryption and will thus protect your data.

Resist the Urge to Click

- Be cautious with offers that look too good to be true. These may be traps.
- Stop and think before you click and take any action.

Use Credit Cards

Avoid using debit cards. It is safer not to use them since they are related to bank accounts. Use credit cards instead; they offer many protections to users:

- Credit card companies will stop payments that look fishy.
- They may call customers to check if transactions are valid.
- Users can dispute all invalid charges with credit card companies, and these providers will generally nullify all suspicious charges and send a replacement card in the mail.

Be Wary of Emails

- Resist the urge to open emails right away. Check who the email is from.
- Be cautious when emails look too good to be true. They may be scams to get your information.

Verify What You Are Buying

- Make sure you’re clear about what you are buying and what you are paying for.
- If in doubt about the site, google the company name.

Strengthen Passwords

- Have strong and secure passwords. This is one of the most secure ways to protect yourself.
- Change your passwords regularly.
- Use paraphrases that make sense to you and are only known to you.

Monitor Your Credit Cards

- Keep track of your credit cards and accounts, especially during the holiday season.
- Monitor your transactions to check if they are valid and legit.
- If something looks suspicious, reach out to the customer service departments of the credit card companies and/or banks involved by contacting their toll-free number, email, or website chat services.

Use Smartphones Wisely

- Avoid using your smartphones for any purchases.
- Refrain from clinking on links from unknown text messages.
- Protect your smartphones with a password and anti-malware software.

Follow Safety Tips

- Close all browsers after using public Wi-Fi.
- Clean up your browser cache.
- Do not save credit cards, passwords, payments, or any other information on your site.
- Make sure to update your laptop software regularly.
- Install anti-malware software on your laptop. Some solutions are free, such as SUPERAntiSpyware
- Scan your computer for malware at least weekly.

Additional Resources

Some users may still fall victim to identity theft or scams – even if they follow good security practices. For even more information on holiday shopping safety, visit the following resources:

- https://www.memberspluscu.org/blog/2022/10/reduce-fraud-this-holiday-season-with-these-tips/
- https://staysafeonline.org/resources/online-shopping/
- https://securityintelligence.com/articles/holiday-cybersecurity-tips/
- https://securityspecialists.com/blog/holiday-season-safety-and-security-tips-to-remember/
- https://megasystemssecurity.com/holidays-security-tips/
- https://www.ramseysolutions.com/budgeting/home-security-tips

---