Public Safety Bulletin

December 10, 2018

Don't Let Someone Hack Your Holidays – Stay Safe Online This Season

Busy, unsuspecting shoppers are attractive targets for profit-motivated hackers and scammers, especially during the holidays. With a limited amount of time to prepare for a season filled with family, friends, food, and fun, these criminals know that people may be less likely to take basic security precautions to protect their accounts and information. To keep them from ruining your holidays, remember the following tips when you are shopping, traveling, and celebrating.

- **Make sure the websites you visit are secure by looking for https:// and a green padlock in your web browser's URL field.** These verify that any information entered into the website is encrypted and protected while being transmitted to the website's servers. The presence of https:// and a green padlock do not, however, verify the authenticity of the website so be sure to double-check the full URL before you enter any sensitive information.

- **Avoid clicking on enticing and unexpected links in emails, text messages, and private messages (PMs) or direct messages (DMs) sent through social media platforms.** Additionally, be wary of clicking on shortened links posted on social media as it can be difficult to determine where that link will redirect your browser. Hackers use these methods to send victims to malicious websites designed to infect systems with malware or to steal login credentials and payment card information.

- **Beware of deals that seem "too good to be true."** Scammers will try to appeal to a shopper's desire to save money by advertising high-end goods at unreasonably low prices. However, shoppers who fall for these deals are often disappointed when either the quality of the goods purchased does not match what was advertised or the goods are not delivered at all and they are left fighting fraudulent charges on a payment card bill. To avoid these scenarios, shop with reputable companies and visit their websites directly to see what deals or coupons they offer.

- **Verify that any mobile apps you download and use this holiday season are legitimate and not malicious.** Only download apps from official app stores and avoid "sideloading" apps from unofficial sources. To determine if an app is legitimate, research the developer and read user reviews prior to installation. Oftentimes, if there is a problem with the app, users will post reviews detailing their experiences to warn others.

- **Do not connect mobile devices to unsecured, public Wi-Fi hotspots.** Hackers can monitor these hotspots and use them to steal information and take over active browsing sessions. If you must use public Wi-Fi, do not use it to log into personal accounts such as email, banking, and social media.

- **Use two-factor authentication (2FA) on every account that offers it.** 2FA can help protect your accounts if somebody steals your username and password. It is also helpful by alerting you to unauthorized attempts to login into your accounts, so you know when you've become a target.

- **Lastly, keep your software and operating systems up-to-date with the latest patches.** Make sure your antivirus software is running and updated to protect your systems and devices against the latest cyber threats. This simple action can reduce your risk of a malware infection.