United States Secret Service
Cybercrime Investigations

Consumer Tips for Secure Online Shopping
2020 Holiday Season

U.S. retail e-commerce sales are expected to explode this holiday season. With the ongoing COVID-19 pandemic changing shopping behaviors, retail online sales are predicted to increase by 25%-35% over last year's holiday season sales and generate up to $196 billion. With that much predicted revenue, the risk of online fraud increases exponentially. Online criminals will be stepping up their efforts to prey upon unsuspecting or unprepared consumers. The U.S. Secret Service would like to remind you to stay vigilant and provide you with the following information and best practices to achieve a more secure online shopping experience this holiday season.

Software and Antivirus Updates: Install operating system and antivirus definition updates as soon as they are available for all devices you use for shopping, to help protect yourself online.

Account Passwords: Change passwords to online shopping sites and other accounts regularly, and use different passwords for each system and account. Utilize multi-factor authentication for an added layer of login security, when available. Immediately change factory preset passwords on home networking equipment, such as Wi-Fi routers and smart devices.

Payment Cards: Credit cards have better protections for the consumer if fraud occurs. For more information, visit the Federal Trade Commission (FTC) Consumer Information. Verify online transactions by checking your credit card and banking statements routinely.

Public Wi-Fi: Do not conduct online shopping or banking using publicly available Wi-Fi networks. While the network in a restaurant, coffee shop or store may require a password, there is no guarantee as to how secure the network is, or who may be monitoring and intercepting your online transactions.

Phishing and Smishing: Phishing (email) and Smishing (text message) are types of fraud schemes which criminals use to elicit funds, credit card and personally identifiable information (PII), or install malware on computers and electronic devices. Never respond to emails or text messages from unknown sources, and avoid opening attachments or clicking on links from senders you do not recognize. Often, these attachments or links can contain malicious content that can infect your device or computer and steal your information.

Social Engineering: Be wary of emails or calls asking you to provide your PII information such as your login, password, account number, etc. Legitimate businesses and government agencies will never solicit personal information by sending you an email, text message, or calling you. Utilize the customer service numbers on your credit/debit cards/bank statements or the merchant websites to verify any requests for information.

Online Transactions: Reputable and established online businesses utilize encryption, such as TLS/SSL security, to protect your PII and payment information as it is transmitted to and from your computer or device. SSL/TLS are protocols for establishing authenticated and encrypted links between networked computers. To protect your information, look for the Lock icon next to a website address in your browser. Do not ignore certificate error notifications, they can be a warning sign that you may be visiting a fraudulent or "spoofed" website. A website's certificate provides identification of the web server. If the certificate has an error, it might indicate that your connection has been intercepted or that the web server is misrepresenting its identity. Always verify website addresses by manually typing them in the browser, or access websites from internet searches. When shopping from your phone, only consider vetted apps from trusted businesses and download only from the device designated app store.

Remember, if the offer sounds too good to be true, then it probably is.

For law enforcement assistance, please contact your local U.S. Secret Service field office Cyber Fraud Task Force (CFTF), or visit www.secretservice.gov/investigation for additional information.