November, 2017
Volume 12, Issue 11

Shopping Safely Online

Making #CyberMonday #CyberSecure

OhioDAS
SERVICE · SUPPORT · SOLUTIONS
DEPARTMENT OF ADMINISTRATIVE SERVICES

Office of Information Security and Privacy

From the desk of Russ Forsythe, Chief Information Security Officer

As Cyber Monday and the season for online shopping quickly approaches, it's worth taking a few moments to ensure you're not giving the gift of your personal or financial information to online criminals! Identity theft, scams, frauds, and malware infections are serious problems that target shoppers during the holiday season and can arise from using your devices to find the perfect gift. Below, we will explore some key tips on how to follow safe online shopping practices in order to make your holiday purchasing more secure.

Create and maintain your online shopping accounts safely

- **Establish a strong password for each online shopping account.** Always use more than ten total characters consisting of upper case letters, lower case letters, numbers, and special characters to create a strong password.
- **Use different passwords on each of your online accounts.** If one retailer experiences a data breach in which your credentials are leaked, using the same password between accounts makes it quick and easy for criminals to exploit you and your information. If you have trouble remembering all your unique passwords, consider using a pattern for your password or a password manager. We talk more about how to do that in our newsletter focused on this topic: https://www.cisecurity.org/newsletter/why-strong-unique-passwords-matter/ .
- **Check out as a guest to avoid saving payment information online.** The inconvenience of having to enter your credit card information each time keeps you safer because a data breach at a retailer will not expose your financial information. It also means your payment information is not saved or ready to be used by anyone who gets access to your account.
- **Use one credit card online or pay through a secure online mechanism.** By using only one credit card online you're limiting the damage that can happen if malicious actors gain that information. Alternatively, use one of the online payment mechanisms, such as PayPal.

Shop with trusted online retailers while browsing safely

- **Use well-known online retailers that have an established reputation for cybersecurity.** Verify that they have good contact information listed on their site, and check with the Better Business Bureau or the FTC if you have questions or concerns.
- **Look for the lock symbol at the top of your browser or "https" in your URL bar.** These mean that your communications with the website are encrypted and safe from prying eyes.
- **Never shop or login to personal accounts when on public Wi-Fi or a public device.** Public Wi-Fi can make all the personal information that you transmit visible to criminals. Public, shared devices, such as kiosks or library computers, can be infected with malware that will steal your information.
- **Do not leave your browser open on a shopping site for long periods of time.** Websites that use advertising feeds have occasionally had them hijacked by cyber criminals, who are then able to put malware on your device. This malware can steal your personal information or encrypt your device and demand a ransom to return it to your control.
- **Keep your devices up-to-date.** Always apply updates to your devices and software when they are available. Keeping devices up-to-date means you have applied all the available fixes for known problems and vulnerabilities. This makes you more secure.

Be smart when it comes to email confirmations and tracking information

- **Be careful which links you click in your emails.** At this time of a year a favorite trick among cyber criminals is to send emails purportedly from the major shipping companies with a link to track your package. These may be a scam to download malware. They count on the fact that you've ordered many things online and are waiting for a package. Instead, cut and paste the tracking number into the shipping company's website in order to track it. Additionally, always head directly to the site of the company you want to shop with by entering the URL into your browser when aiming to log in. Avoid clicking links directing you to log in, as they may send you to a malicious site that looks real, but can just steal your information.
- **Do not use your work email address for retail accounts.** By using one of the free webmail accounts, such as Gmail or Hotmail, it will be much easier to identify a potentially malicious email coming to your work email, since the online retailers should not know that email address. This can also help you prevent criminals from knowing where you work, which is information than can potentially use to hack into your work account!

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™