Daily Union Article

Saturday, December 8, 2018

Title: Online Safety for the Holidays

If you have let time slip away from you without finishing your holiday shopping, you might be considering online retail services to help bail you out. More than ever, the holiday season is a time to be proactive in protecting yourself and family members who spend money and time online.

Being intentional in how you practice internet safety can save you time, money, and energy. Here are some online safety tips offered by the Cybersecurity and Infrastructure Security agency of the US Department of Homeland Security:

- **Do business with reputable vendors** – Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. Some attackers may try to trick you by creating malicious websites that appear to be legitimate, so you should verify the legitimacy before supplying any information. Attackers may obtain a site certificate for a malicious website to appear more authentic, so review the certificate information, particularly the "issued to" information. Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill.
- **Make sure your information is being encrypted** – Many sites use secure sockets layer to encrypt information. Indications that your information will be encrypted include a Uniform Resource Locator that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by browser; for example, it may be to the right of the address bar or at the bottom of the window. Some attackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.
- **Be wary of emails requesting information** – Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email. If you receive an unsolicited email from a business, instead of clicking on the provided link, directly log on to the authentic website by typing the address yourself.
- **Use a credit card** – There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills. You can minimize potential damage by using a single, low-limit credit card to make all of your online purchases. Also use a credit card when using a payment gateway such as PayPal, Google Wallet, or Apple Pay.
- **Check your shopping app settings** – Look for apps that tell you what they do with your data and how they keep it secure. Keep in mind that there is no legal limit on your liability with money stored in a shopping app (or on a gift card). Unless otherwise stated under the terms of service, you are responsible for all charges made through your shopping app.
- **Check your statements** – Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately.
- **Check privacy policies** – Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.

Additionally, you want to take steps to keep your family members safe when they are home from school for winter break and spending time online. The following simple steps can protect you and your family from some of the risks associated with the internet:

1) Download security updates as soon as they become available. Delaying security software updates can put your family and computer at risk. To maintain maximum security, don't ignore legitimate update messages that appear on your computer.
2) Be cautious when downloading free software like games or screensavers onto your computer. It is best to monitor the games that children are interested in downloading. Do not allow children to download games without parental permission. For your best protection, avoid gaming websites.
3) Put a lock on your home's wireless internet system. Do not share the password with people outside of the immediate family.
4) To avoid loss of personal documents back-up your documents on a regular bases. Invest in an inexpensive data back-up system that allows you to preserve information, photos, music, and precious data.
5) Teach children to practice online safety procedures. They should never share personal family information, address, phone number, passwords, schedules, school information, or vacation plans when online.

For more information on how to keep your children and grandchildren safe while online, check out https://www.netsmartz.org/internetsafety. This is a great interactive, educational internet resource hosted by the National Center for Missing & Exploited Children® (NCMEC) The website provides age-appropriate resources to help teach children how to be safer on- and offline. It is designed for children ages 5-17, parents and guardians, educators, and law enforcement. With resources such as videos, games, activity cards, and presentations, NetSmartz entertains while it educates. Everyone wants to have a relaxing and enjoyable holiday season. By following these suggestions, you can avoid the stress and frustration caused when your computer and online security have been breached. Until next time, keep living resourcefully!