Hawthorne & Co.
Certified Public Accountants

5 TIPS TO PROTECT YOURSELF WHILE HOLIDAY SHOPPING ONLINE

From the AICPA Blog by Guest Blogger

This holiday season, researchers expect consumer spending to mirror prior seasons but with a huge swing to online shopping. While you're buying for your loved ones and feeling warm and fuzzy, cybercriminals are feeling the same about the uptick in online shopping because it presents more opportunities to steal data.

With cybercrime expected to reach $6 trillion in 2021, being aware and maintaining safe cyber practices will benefit you significantly. Here are five things you can do to protect yourself during the holiday season:

1. Manage your passwords

The average person has over 100 unique online accounts, often using some variation of the same password for all. If a hacker can breach just one of your accounts, the door can be opened to others.

When passwords and email addresses get into the hands of cybercriminals, this is sometimes referred to as "pwn" (rhymes with "own"). To learn if any of your online accounts have been compromised, visit this site created by a security expert: https://www.haveibeenpwned.com/. Once you've entered your email address, the site reports data breaches associated with that address. If you learn about breaches on a specific account, it'd be wise to change your username and password on every online account.

Alternatively, a password manager tool, such as Bitwarden or 1Password, is another solution that informs you when your username and password combination is weak or has been compromised in a data breach.

2. Use multi-factor authentication (MFA)

MFA, sometimes referred to as two-factor authentication (2FA), is the best way to prevent your accounts from being compromised, by far. Every year, more companies offer MFA to protect their customers' data; however, researchers estimate that only 10–15% of people enable MFA when it's available. Because the functionality is so effective, I urge everyone to use MFA when it's offered for your banking, social media, gaming, healthcare and e-commerce accounts.

3. Beware of phishing

Continue to be vigilant about phishing emails — phishing is the most successful method hackers use to steal your data, and every holiday season there is a spike in phishing emails. Unfortunately, we're seeing a soaring increase in phishing emails due to COVID-19.

Take time to closely look at the sender's information to ensure it's authentic. Some of the most common brands are impersonated in phishing emails: PayPal, Facebook, Microsoft, Netflix and Google. The Federal Trade Commission's website offers great advice on how to recognize and avoid phishing scams.

Gift cards are popular presents during the holidays. As a general practice: If a suspicious email has anything to do with gift cards, delete it.

4. Educate your children

It's important to convey the importance of protecting personal data with your children. In today's connected world, identifiable information — including data about kids and teens — has value.

Whether your child is attending school virtually due to the pandemic or just loves to play Fortnite, teaching them to make smart decisions about privacy and security will help keep them and their data safe. Google's cyber resource center for parents has a variety of resources for different age groups.

5. Be diligent

During the holiday season and throughout the year, be diligent about where and how you use your data:

- Use a credit card for online purchases.
- Ensure the websites you're using have SSL encryption before submitting personal data or credit card information. How can you tell if the site has SSL encryption? The letter "s" will be at the beginning of the URL —"https:" indicates you're on a website with a secure connection.
- Use a virtual private network (VPN) if you're on a public Wi-Fi network. Many organizations set up corporate VPNs for their staff to use while working from home, but people are also starting to incorporate VPNs on their personal devices.
- Hang up the phone if a person calling from an unknown number asks for your credit card or social security number. Recent phone scams were related to COVID-19 testing and election verification — scams tend to reflect current events. Stay alert.

Just because the world has changed significantly over the past year does not mean cybercriminals are slowing down. Too many have amplified their efforts, taking advantage of people living in this new environment.

Now that you have tips to secure your own data, there are steps you can take to help your clients or organization protect its data. Check out the following 10 free cybersecurity resources to brush up on your cybersecurity skills.