

# Holiday Shopping Tips

How do you protect yourself while shopping online?

By: Robert Adams, Esq.

Date: October 17, 2018

As the holiday shopping season rapidly approaches, many consumers will be shopping online this year instead of visiting a physical store. It is usually easier and faster with a larger selection than what is available from a brick-and-mortar location. But with that convenience comes some unexpected dangers. According to Consumer Affairs, consumers lost approximately \$7.5 billion in 2017 due to holiday shopping scams and this year promises to be even worse unless you are prepared.

Here are several important tips to keep in mind this holiday season to help protect your identity as well as your pocketbook. Follow these important online shopping tips to keep yourself safe:

1. The biggest rule to keep in the back of your mind at all times is **“if the deal’s too good to be true, then it’s probably not legitimate.”** Do not get tricked into clicking on suspicious links in unsolicited emails offering amazing deals.
2. Only make online purchases from **reputable websites** that you already **know and trust**.
3. Be aware of **social media scams** that try to entice you to click on a link for free vouchers or gift cards. Avoid clicking on anything from social media websites.
4. Only enter your username and password on **reputable websites** where the address starts with **“HTTPS://”**.
5. Do not be fooled by fake websites pretending to be legitimate ones. Do not click on links in emails. Instead, **open a new browser window** and manually enter the URL for the reputable website you are trying to access.

6. Never give out your password to anyone, including over the phone, chat windows, or emails. Remember, **no one should ever ask for your password** and if someone does, that is the number one reason to become suspicious of their malicious intent.
7. Avoid using your regular email address to register for unknown websites. This will help prevent SPAM being sent to your regular personal email address.
8. Select a **unique password for every online account you access**, including your work account. Each account should have its own unique and separate password. That way if the password were to become compromised, it has only compromised that one account.
9. Change all your passwords **regularly** and **avoid using passwords that contain information that can be easily researched** about yourself.
10. If you suspect any malicious activity, **immediately change your password for every site that uses that same password** to a unique and separate password. Continue to monitor that account to ensure no further malicious activity occurs. If necessary, contact the company and inform them of the suspected activity.

**Happy holidays and safe shopping!**