

Secure Online Shopping

There are many advantages to shopping online – at home convenience, no crowds, no pushy salesmen, etc. However, increased convenience can have negative consequences especially when personal financial information is being transmitted in cyberspace. Although risks do exist, there are simple security practices that you can follow to help protect yourself.

Keep a clean machine. Make sure your software, operating system, and antivirus programs are updated.

Connect with care. Do not do online shopping on unsecure wireless networks, such as places with public and free Wi-Fi.

Pay attention to website URLs. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain. Also, only shop from a site that uses https://.

Set strong passwords. Make sure your passwords are complex and unique to each account. Create passwords with eight characters or more that use a combination of numbers, letters, and symbols.

Don't believe everything you see. Always be aware of cyber scams – if it sounds too good to be true, it probably is.

Use a credit card. There are laws that limit your liability for fraudulent card charges. You may not have the same level of protection when using a debit card.

By consistently implementing these simple practices, you can greatly enhance the security of your online shopping and other web activities.

For questions concerning the DOE Cybersecurity Program, please send an email to cybsectrn@hq.doe.gov.

Bob Brese is the CIO for the U.S. Department of Energy.