



TEN TIPS FOR RECOGNIZING AND AVOIDING ONLINE SHOPPING SECURITY RISKS

1. INSTALL SECURITY UPDATES.

Programs installed on computers and operating systems should be updated on a regular basis.

2. INSTALL ANTIVIRUS SOFTWARE AND MAKE SURE IT IS ACTIVATED.

Most antivirus software includes an automatic update feature.

3. INSTALL A FIREWALL.

A firewall will protect your computer(s) from unauthorized access and use by hackers.

4. TRUST YOUR INSTINCTS.

When purchasing software or other products online, if the price seems "too good to be true," it probably is. Take special care to avoid sellers offering "backup" copies of software. This is a clear indication that the software is illegal. Also, be wary of compilations of software titles from different publishers on a single disk or CD.

5. DO YOUR HOMEWORK.

Look for a feedback section on the site and look for comments about the seller based on previous transactions. Look for a "trust mark" from a reputable organization, like BBBOnline, to make sure the online retailer is reliable and has a proven track record of satisfying customers. If in doubt, conduct Web searches about the site in order to determine its legitimacy and check for a Better Business Bureau (BBB) report at www.bbb.org.

6. UNDERSTAND THE PRIVACY POLICY.

Find and read the Web site's privacy policies to understand what personal information is being requested as well as why and how it will be used.

7. ENSURE SECURE PAYMENT.

Before you give your payment information, check that the Internet connections you will be using are secure.

8. CHECK THE VENDOR'S IDENTIFYING INFORMATION.

If the vendor is unfamiliar to you, look for an online and offline customer support contact, especially when shopping for software programs on auction sites.

9. UNDERSTAND THE TRANSACTION TERMS.

Get a clear explanation of the merchant's policies concerning returns and refunds, shipping costs, and security and privacy protection before you complete the transaction.

10. RECOGNIZE SPAM.

Indicators that an e-mail is spam include senders whose names you don't recognize, typos and misspellings in the subject line, and prices that seem "too good to be true."

From the Business Software Alliance and the Council of Better Business Bureaus

