PENTAGON FORCE PROTECTION AGENCY

THREAT INTELLIGENCE CENTER

9000 Defense Pentagon
Washington, D.C. 20301
703-693-5000

Protect Yourself: Online Shopping

The world of electronic commerce, also known as e-commerce, enables consumers to shop at thousands of online stores and pay for their purchases without leaving the comfort of home. Consumers expect merchants to not only make their products available online, but to make payments a simple and secure process. However, the same things can go wrong shopping online as in the real world. Sometimes it is simply a case of a computer glitch or poor customer service. Other times, shoppers are cheated by clever scam artists.

1. **Shop at Secure Web Sites:**

a. Secure sites use encryption technology to transfer information from your computer to the online merchant's computer. Encryption scrambles the information you send, such as your credit card number, in order to prevent computer hackers from obtaining it en route. The only people who can unscramble the code are those with legitimate access privileges.

b. Here's how you can tell when you are dealing with a secure site:

(1) If you look at the top of your screen where the Web site address is displayed (the "address bar"), you should see https://. The "s" that is displayed after "http" indicates that Web site is secure. Often, you do not see the "s" until you actually move to the order page on the Web site.

(2) Another way to determine if a Web site is secure is to look for a closed padlock displayed on the address bar of your screen. If that lock is open, you should assume it is not a secure site.

2. **Research the Web Site Before You Order:**

a. Do business with companies you already know. If the company is unfamiliar, do your homework before buying their products. If you decide to buy something from an unknown company, start out with an inexpensive order to learn if the company is trustworthy.

b. Reliable companies should advertise their physical business address and at least one phone number, either customer service or an order line. Call the phone number and ask questions to determine if the business is legitimate. Even if you call after hours, many companies have a "live" answering service, especially if they don't want to miss orders. Ask how the merchant handles returned merchandise and complaints. Find out if it offers full refunds or only store credits.

c. You can also research a company through the Better Business Bureau, or a government consumer protection agency like the district attorney's office or the Attorney General. Remember, anyone can create a Web site.

3. **Read the Web Site's Privacy and Security Policies:**

a. Every reputable online Web site offers information about how it processes your order. It is usually listed in the section entitled "Privacy Policy." You can find out if the merchant intends to share your information with a third party or affiliate company. Do they require these companies to refrain from marketing to their customers? If not, you can expect to receive "spam" (unsolicited email) and even mail or phone solicitations from these companies.

b. You can also learn what type of information is gathered by the Web site, and how it is, or is not, shared with others. The online merchant's data security practices are also often explained in the Privacy Policy, or perhaps a separate Security Policy.

(1) Look for online merchants who are members of a seal-of-approval program that sets voluntary guidelines for privacy-related practices, such as TRUSTe (www.truste.org), Verisign (www.verisign.com), or BBBonline (www.bbbonline.org).

4. **What's Safest: Credit Cards, Debit Cards, Cash, or Checks?**

The safest way to shop on the Internet is with a *credit card*. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. When it has been determined that your credit was used without authorization, you are only responsible for the first $50

5. **Never Give Out Your Social Security Number:**

a. Providing your Social Security number is not a requirement for placing an order at an online shopping site. There is no need for the merchant to ask for it. Giving out your Social Security number could lead to having your identity stolen.

6. **Disclose Only the Bare Facts When You Order:**

a. When placing an order, there is certain information that you must provide to the web merchant such as your name and address. Often, a merchant will try to obtain more information about you. They may ask questions about your leisure lifestyle or annual income. This information is used to target you for marketing purposes. It can lead to "spam" or even direct mail and telephone solicitations.

b. Don't answer any question you feel is not required to process your order. Often, the web site will mark which questions need to be answered with an asterisk (*). Should a company require information you are not comfortable sharing, leave the site and find a different company for the product you seek.

10. **Keep Your Password Private:**

a. Many online shopping sites require the shopper to log-in before placing or viewing an order. The shopper is usually required to provide a username and a password.

b. Never reveal your password to anyone. When selecting a password, do not use commonly known information, such as your birthdate, mother's maiden name, or numbers from

your driver's license or Social Security number. Do not reuse the same password for other sites, particularly sites associated with sensitive information. The best password has at least eight characters and includes numbers and letters.

11. **Check the Web Site Address:**

a. The address bar at the top of your device's screen contains the web site address (also called the URL, or Uniform Resource Locator). By checking that address, you can make sure that you are dealing with the correct company.

b. Don't click on any link embedded within a potentially suspicious email. Instead, start a new Internet session by typing in the link's URL into the address bar and pressing "Enter" to be sure you are directed to a legitimate Web site.

12. **Don't Fall for "Phishing" Messages:**

a. Identity thieves send massive numbers of emails to Internet users that ask them to update the account information for their banks, credit cards, online payment service, or popular shopping sites. The email may state that your account information has expired, been compromised or lost and that you need to immediately resend it to the company.

b. Some emails sent as part of such "phishing" expeditions often contain links to official-looking Web pages. Other times the emails ask the consumer to download and submit an electronic form.

c. Remember, legitimate businesses don't ask for sensitive information via email. Don't respond to any request for financial information that comes to you in an email. Again, don't click on any link embedded within a suspicious email, and always call the retailer or financial institution to verify your account status before divulging any information.