Consumer Federation of America

PROTECT YOURSELF FROM FRAUD WHEN YOU'RE BUYING ONLINE

You know the saying, "On the Internet, no one knows you're a dog." Sometimes it's hard to be sure who you're dealing with online. Follow these tips to avoid becoming a victim of fraud when you're buying online.

1. **Check out unfamiliar sellers – Shopper complaints can keep you away from the bad guys.** While you'll find many familiar companies online, including ones that you do business with in person, on the Internet you can make purchases from companies and individuals from all over the world. If you're not familiar with the seller, it's a good idea to look for information about complaints at the Better Business Bureau, www.bbb.org, and check the seller ratings on auction or price comparison sites. There are also many online sites where consumers share information about problems with companies and give feedback that can help you decide whether you want to do business with them.

2. **Pay the safest way – Credit cards offer extra protections.** Even if the seller has no history of serious complaints, that does not guarantee that your purchase will be trouble-free. If you pay with a credit card, you have the right to dispute the charges if the goods or services aren't delivered or were falsely described. It's safe to provide your credit card number online because you also have the right to dispute the charges if someone fraudulently uses it. While you can also dispute unauthorized debits, but you don't have the right to dispute debits if the goods or services were misrepresented or never arrived. Note: Some debit card issuers will voluntarily credit the money back in that case, so be sure to ask if you become a victim. Some payment services such as PayPal offer "buyer protection" in case something goes wrong. Read how to qualify for these protections before using the services.

3. **Know A Secure Browser – Look for shttp/https where the "S" is for secure.** Some websites use a security feature that turns your account number into code so no one else can read it. If shttp or https appears at the beginning of the website URL (at the top of your computer screen), you know the site is protecting your account number. There may also be a symbol on your screen such as a padlock that closes. Never provide financial account numbers by email, since it's not secure.

4. **Never pay using a money transfer service – You could be transferring cash to a crook.** Crooks ask consumers to send them payment using a money transfer service such as Western Union or MoneyGram because they can get the cash fast and it's hard to trace. Legitimate sellers don't ask consumers to send payment that way. Money transfer services should only be used to send money to people you have met in person and know well, not to strangers.

5. **Keep records of your purchases – Always save or print order documents.** Be sure to save your order information and other documentation in a special folder in case there are questions or problems later. To protect yourself from losing the information to a computer snafu, print it.

6. **Watch out for "phishing" and "smishing" – Legitimate companies will never request confirmation of account information by email or texting.** Identity thieves posing as well-known companies often send emails and text messages (called "phishing" if it is an email or "smishing" if it comes as a text message on your phone) asking consumers to confirm personal information such as their account numbers. No one who already has your account information would need to contact you to confirm it. Never click on the link or call the number that may be provided. Instead, immediately delete these messages, since they may also contain viruses that can infect your computer or mobile phone.

7. **Check out CFA's "Buyer Beware" video at** www.consumerfed.org/fraud.