Internet Escrow Scams

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

Buying and selling items online has become more common in recent years. Annually, people post millions of items for sale on online classified websites, and exchange billions of dollars via online payment services to purchase them. But unlike most advertisements printed in your local newspaper, online advertisements could be posted by someone in another state—or another country—and it can be difficult to verify an advertisement's legitimacy. Some scam artists pose as real companies to make consumers feel more comfortable buying an item from someone they can't see face-to-face, in what is known as an escrow scam.

It can happen like this:

"Jenna" needed a new computer for school. She searched an online classifieds website and found the laptop she wanted at an unbeatable price. She emailed the seller, who claimed to live in another state and said that eBay would handle the transaction. The seller claimed eBay would hold Jenna's money in escrow and allow her to try the laptop before releasing her money to the seller. Jenna received an email with eBay's logo that instructed her to purchase eBay gift cards and reply with the redemption codes to pay for the laptop. Jenna became suspicious and examined the email more closely. She noticed that the email came from escrow@ebay01.net, which she knew could not possibly be a real email address for the company. She blocked the person from contacting her and did not pay any money.

Overview of Internet Escrow Scams

Legitimate escrow services are supposed to protect buyers from fraudulent activity and can be useful for people making purchases over the Internet or at long distances. Escrow services usually hold the buyer's money until he or she receives the purchased item and verifies that its condition is as promised. If the buyer has a problem with the item or never receives it, the escrow service can refund the buyer's money.

Criminals who commit escrow scams warp this model to convince consumers that their money will be protected, while requesting that consumers send money by unconventional methods. While escrow scam artists sometimes set up their own fake escrow services, many scam artists misuse the names of well-known companies—such as eBay, PayPal, Amazon.com, or Apple—to perpetrate the scam. They send official-looking emails, often using the legitimate company's logo and email format, that instruct the buyer to send money via gift cards or wire transfers, which are practically untraceable. Then, once the victim sends the money, he or she never receives the item and never hears from the scam artist again.

Tips to Avoid Internet Escrow Scams

The criminals who commit this type of scam prey on people's skepticism and caution, and attempt to take advantage of people who would otherwise be wary of sending money to someone they do not know personally. You can take steps to protect yourself from escrow scams when purchasing something from another person online, including:

- **Check the sender's email address.** While an email might look like it came from eBay or PayPal, it is easy for a scam artist to use a company's logo to create a legitimate-looking email message. When in doubt, check to make sure the email actually came from the company. For example, an email might look like it came from PayPal, but the email address is actually paypal@xyzescrow.com. If the email address doesn't check out, delete the email and block the sender from contacting you without clicking on anything in the email or opening any attachments. Emails from scam artists sometimes contain viruses that can infect and damage your computer.

- **Be cautious when opening links.** If an email contains links that appear to go to the company's website, double check that they do not reroute to a fraudulent site. Hover over the link with your cursor and check the destination address. If it is not the company's website, do not click on the link. This method is not foolproof—scam artists can alter the link to make it look like the destination is reputable when it is not. When in doubt, use your browser to go directly to the company's website.

- **Don't trust the information in emails.** If you have questions about how the escrow service operates, take the extra step of going directly to the company's website to locate its contact information. For example, you should call the company's customer service telephone number listed on its website—not the phone number listed in a suspicious email. Scam artists will sometimes list a fake toll free number in their emails in the hopes that consumers will never speak with an actual company representative about the transaction. If you want to contact the company via email, locate an email address on its website rather than replying directly to the email you received.

- **Be wary of unusual payment methods.** Most major companies require buyers to send payment via a credit card or bank account transfer through a secured website. A reputable site will never require buyers to send information in an email exchange or wire money to an individual. If an email from a well-known company asks you to send money in an unconventional way, check the company's website to see if that method is usually how it does business. In general, it is best to avoid paying for items or services via wire transfer or gift card—these methods of payment are difficult to trace and often used by scammers. It is nearly impossible to recover the money if the transaction turns out to be a scam.

Reporting Escrow Scams

If you have been targeted by an escrow scam, you should report the matter to the criminal authorities, who have jurisdiction to investigate and prosecute online crime. These authorities include your local and county law enforcement officials, as well as the following federal criminal investigative agencies:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
(763) 569-8000
www.ic3.gov (Internet Crime Complaint Center)

United States Postal Inspection Service
Criminal Investigation Service Center
1745 Stout Street, Suite 900
Denver, CO 80299-3034
(877) 876-2455
postalinspectors.uspis.gov

United States Secret Service
Minnesota Electronic Crimes Task Force
300 South Fourth Street, Suite 750
Minneapolis, MN 55415
(612) 348-1800
www.secretservice.gov