S.C.R.A.M. GAZETTE

Faking it—Scammers' tricks to steal your heart and money

Not everyone using online dating sites is looking for love. Scammers create fake online profiles using photos of other people — even stolen pictures of real military personnel. They profess their love quickly. And they tug at your heartstrings with made-up stories about how they need money — for emergencies, hospital bills, or travel. Why all of the tricks? They're looking to steal your money.

As if all that isn't bad enough, romance scammers are now involving their victims in online bank fraud. Here's how it works: The scammers set up dating profiles to meet potential victims. After they form a "relationship," they come up with reasons to ask their love interest to set up a new bank account. The scammers transfer stolen money into the new account, and then tell their victims to wire the money out of the country. Victims think they're just helping out their soulmate, never realizing they're aiding and abetting a crime.

Here are some warning signs that an online love interest might be a fake. They ask you to:

chat off of the dating site immediately, using personal email, text, or phone
wire money using Western Union or Money Gram
set up a new bank account

Did you know you can do an image search of your love interest's photo in your favorite search engine? If you do an image search and the person's photo appears under several different names, you're probably dealing with a scammer. And if the person's online profile disappears a few days after they meet you, that's another tip-off.

Here's the real deal: Don't send money to someone you met online — for any reason. If your online sweetheart asks for money, you can expect it's a scam.

Unfortunately, online dating scams are all too common. There may be tens of thousands of victims, and only a small fraction report it to the FTC. If this happens to you, please report it at ftc.gov/complaint — click on Scams and Rip-Offs, then select Romance Scams.

How to Recognize a Scam Artist

The relationship may not be what you think, especially if your sweetheart:

wants to leave the dating site immediately and use personal email or IM
claims love in a heartbeat
claims to be from the U.S., but is traveling or working overseas
plans to visit, but is prevented by a traumatic event or a business deal gone sour
Scammers also like to say they're out of the country for business or military service.

What You Can Do About It
You may lose your heart, but you don't have to lose your shirt, too. Don't wire money to cover:

travel
medical emergencies
hotel bills
hospital bills for a child or other relative
visas or other official documents
or losses from a temporary financial setback
Don't send money to tide someone over after a mugging or robbery, and don't do anyone a favor by making an online purchase or forwarding a package to another country. One request leads to another, and delays and disappointments will follow. In the end, the money will be gone along with the person you thought you knew.

Attention Grandparents: Watch out for phony debt collectors

My grandma kept an eye out for cheaters. (No, not that kind.) Back in the day, if a salesman knocked on her front door, she waved them off. Before caller ID, she hung up on telemarketers. But a call from a phony debt collector? She might have fallen for that one. Especially if the debt collector said she was responsible for her grandchild's debt.

Here's what's happening: A fake debt collector calls you. They want to collect on a debt your grandchild (supposedly) failed to pay. They ask you to wire money, send a prepaid card or give your credit card number – immediately. And if you won't – or can't – pay? That's when the threats begin:

"Your grandchild will be arrested."
"He'll lose his job."
"We'll suspend her driver's license."

Unless you co-signed a loan, you're never responsible for someone else's debt. In fact, debt collectors can't legally tell you that someone – anyone – else even has a debt.

If you get one of these calls, stop. Don't be rushed into sending money. Don't verify any personal or financial information. And hang up if the caller threatens you. Debt collectors can't do that. It's not legal. Once you're off the phone, report the call to the FTC.

Want more? Read our tips on how to avoid family emergency scams. And check out Pass It On, our campaign that encourages older adults to talk to others about avoiding scams.

Niles Police
7000 W. Touhy Ave
Niles, IL 60714
847-588-6500
www.nilespd.com
Connect with US!
www.nilespd.com

CRIMINALS CONTINUE TO DEFRAUD AND EXTORT

Data from the FBI's Internet Crime Complaint Center (IC3) shows ransomware continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses.[1] CryptoWall and its variants have been used actively to target U.S. victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between $200 and $10,000. Many victims incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

These financial fraud schemes target both individuals and businesses, are usually very successful, and have a significant impact on victims. The problem begins when the victim clicks on an infected advertisement, email, or attachment, or visits an infected website. Once the victim's device is infected with the ransomware variant, the victim's files become encrypted. In most cases, once the victim pays a ransom fee, he or she regains access to the files that were encrypted. Most criminals involved in ransomware schemes demand payment in Bitcoin. Criminals prefer Bitcoin because it's easy to use, fast, publicly available, decentralized, and provides a sense of heightened security/ anonymity.

If you believe you have been a victim of this type of scam, you should reach out to your local FBI field office. You may also file a complaint with the IC3 atwww.IC3.gov. Please provide any relevant information in your complaint.

Tips to protect yourself:

- *Always use antivirus software and a firewall.* It's important to obtain and use antivirus software and firewalls from reputable companies. It's also important to continually maintain both of these through automatic updates.
- *Enable popup blockers.* Popups are regularly used by criminals to spread malicious software. To avoid accidental clicks on or within popups, it's best to prevent them from appearing in the first place.
- *Always back up the content on your computer.* If you back up, verify, and maintain offline copies of your personal and application data, ransomware scams will have limited impact on you. If you are targeted, instead of worrying about paying a ransom to get your data back, you can simply have your system wiped clean and then reload your files.
- *Be skeptical.* Don't click on any emails or attachments you don't recognize, and avoid suspicious websites altogether.

If you receive a ransomware popup or message on your device alerting you to an infection, immediately disconnect from the Internet to avoid any additional infections or data losses. Alert your local law enforcement personnel and file a complaint at www.IC3.gov.

GIFT CARD SCAMS

While it is very popular to purchase, spend, and give others gift cards, the FBI would like to warn consumers of the potential for fraud. The online presence of the Secondary Gift Card Market has grown significantly in recent years. The Secondary Gift Card Market provides a venue for consumers to resell unwanted gift cards. However, criminal activity has been identified through sites facilitating such exchanges.

There are both online and in-store venues for reselling gift cards. Kiosks and pawn shops are an option for consumers who prefer to handle a transaction in person. Secondary Gift Card Market websites exist to exclusively buy and sell gift cards.

Some of the various types of gift card scams reported to the IC3 are as follows:

- Victim sells a gift card on an auction site, receives payment for the sale, and sends the PIN associated with the gift card to the buyer, who disputes the charge after using the gift card.
- Victim purchases an item on an auction site and is advised by the seller to purchase gift cards to pay for the transaction. After purchasing thousands of dollars in gift cards, the victim finds out the auction transaction is a scam.
- A Secondary Gift Card Market site agrees to pay a victim for a discounted merchant gift card. The victim sends the code on the gift card, and the payment for the transaction was reversed. Thus, the buyer uses the gift card code to purchase an item and stops payment to the seller.

Consumers should beware of social media postings that appear to offer vouchers or gift cards, especially sites offering deals too good to be true, such as a free $500 gift card. Some fraudulent offers may pose as Holiday promotions or contests. The fraudulent postings often look as if a friend shared the link. Oftentimes, these scams lead to online surveys designed to steal personal information. Never provide your personal information to an unknown party or untrustworthy website.

Tips to Prevent Gift Card Fraud:

Consumers can take several steps to protect themselves when buying and selling gift cards in the Secondary Gift Card Market, as listed below:

- Check Secondary Gift Card Market website reviews and only buy from or sell to reputable dealers.
- Check the gift card balance before and after purchasing the card to verify the correct balance on the card.
- The re-seller of a gift card is responsible for ensuring the correct balance is on the gift card, not the merchant whose name is on the gift card.
- When selling a gift card through an online marketplace, do not provide the buyer with the card's PIN until the transaction is complete. Online purchases can be made using the PIN without having the physical card.
- When purchasing gift cards online, be leery of auction sites selling gift cards at a discount or in bulk.
- When purchasing gift cards in a store, examine the protective scratch-off area on the back of the card for any evidence of tampering.

If you believe you have been a victim of a gift card scam, you may file a complaint, providing all relevant information, with the IC3 at www.IC3.gov.