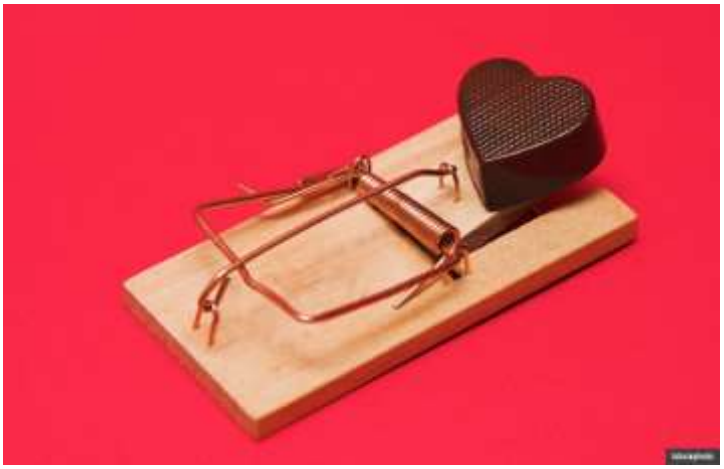
Don’t Fall for Online Romance Scams

Con artists use Valentine’s Day as way to steal your heart and your money

by **Sid Kirchheimer**, **AARP**



Cupid isn't the only one taking aim at you this time of year. Valentine's Day provides a bonanza of opportunities for scammers to hit their targets.

At online dating sites, crooks impersonate exciting new love interests, who before long need some money from you. All too often they get it: Their average take is $10,000. But it's not just those who seek a cyber-sweetheart that get swindled. Even sober non-romantics can be taken in by the scammers' holiday-themed hoaxes this time of year. So be on your guard. Here's what to look out for:

Don't let your heart get scammed. Watch out for these Valentine's Day hoaxes.

"Gotcha" greetings. Opening an electronic greeting card sent to your computer is "one of the easiest ways to invite malware onto your machine," says Brenda Moretto, of online security company McAfee.

Don't click on links or follow instructions to download software that you supposedly need to view a card. Doing either can unleash malicious programs that turn your computer into a spam-sending "botnet" or give cyber-crooks remote access to your personal information, online bank accounts and passwords.

Legitimate e-card notifications include a confirmation code that allows you to open the greeting at the card company's website. If there's no card at that site, the message was a scam. Ignore any messages sent by strangers, or bearing titles like "webmaster@hallmark.com," "friend" or "secret admirer." And be careful even if a message has a friend's name — scammers can also impersonate them.

Sale-related spam. Expect an in-box littered with offers for deals on chocolates, jewelry, roses and other Valentine's Day-themed products. But be skeptical unless the offer is from a company you've done business with and which has your contact information. Links within emails can download malware, direct you to a scammer-run

“online-romance-valentines-day-scams”, AARP, Inc. Viewed February. 5, 2018.
https://www.aarp.org/money/scams-fraud/info-02-2013/online-romance-valentines-day-scams.html

website to glean your credit card without delivering anything, or lead you to a copycat website selling cheap counterfeits.

How can you spot scam websites?

- Start by carefully reading the Web address. For instance, look at the difference between these two addresses: "www.tiffany.com" and "www.tiffanyco.mn" (a Mongolian site exposed by Scam Alert). If it looks fishy, don't click.
- Hover your mouse over the link (without clicking) to see its full address.
- Copy and paste (again, without clicking) the link into a Microsoft Word document. Then right click on the pasted link and select "Edit Hyperlink" from the menu that appears, which should open a pop-up window that shows the address to which the link directs.
- Copy and paste the link to http://browsingprotection.f-secure.com/swp/ to check the safety of the website.

Search-word dangers. No doubt, your own Internet surfing for gifts can take you to dangerous waters. For each holiday — and their popular presents — cyber-scammers have found ways to tweak search engine results of gift-related search words. You get led to rogue rip-offs. Before clicking anywhere, use the bulleted "spot a scam" strategies — and use common sense. Don't trust advertisements touting unbelievable bargains or vendors whose names you don't recognize.

Problematic presents. Online and otherwise, even legitimate vendors may deliver less than expected. So save the love for your sweetie — and ask sellers tough questions. "While you think you're ordering from a local florist, you may actually be on the phone with someone hundreds or thousands of miles away," says Steve Bernas of the Better Business Bureau in Chicago. Last year, florist complaints were up 47 percent.

Interested in jewelry? Check out the Federal Trade Commission's consumer information on buying jewelry. It has tips on terms and how to spot fake appraisals.

Sweet on a canine? Before you bite on that street-corner offer, realize that Valentine's is peak season for dognapping and puppy-selling scams. These scams persist in ads in local newspapers and Craigslist, as well as emails and scammer websites.

Social media rogue romantics. Scammers are increasingly using social media websites to try to trick you into taking surveys that could set the stage for identity theft. Beware of applications that masquerade as romantic "wall" postings.

"online-romance-valentines-day-scams", AARP, Inc. Viewed February. 5, 2018.
https://www.aarp.org/money/scams-fraud/info-02-2013/online-romance-valentines-day-scams.html