#

Scams are in the Air…This Valentine's Day

February 2011

With Valentine's Day around the corner, many of us single people return to thoughts of finding love online. But while your head is in the online clouds, you should know - *and sorry to sound like a parent* - that cyberscammers may be there with you looking to take advantage of your vulnerable heart.

From fake online dating profiles used to fool you, to phony eCards with links to malware, be aware of cybercrooks who will pull on your heart strings to try and get what they want—your money and sensitive information.

To help you stay safe on Valentine's Day and year-round, here is a look at some of the top romance scams and threats, followed by safety tips in honor of your heart:

Be Aware Online Daters - Romance Scams & Threats

1) Online Dating Scams—Millions of people use online dating sites to broaden their networks and meet potential mates, but not everyone on these sites are sincere—some are scammers hoping to lure you in with false affection, with the goal of gaining your trust, and eventually, your money.

In a typical scam, the cybercrook will create a fake online dating profile, complete with attractive photos. Then, they reach out to you one-on-one via email, chat, text or phone, trying to establish a relationship and gain your trust. Once trust is established, they may ask for money for a plane ticket to visit, or give you a sob story. For instance, the scammer may say that they have a life threatening illness, or need money to pay rent. Either way, they play on your emotions to get what they want.

- **Military Ploy—**In this version of an online dating scam, the cybercrook pretends to be a soldier and strikes up a relationship with a female online dater. Once a relationship is established—perhaps over weeks or months—the scammer asks the victim to apply for military leave so he can visit, and fill out official-looking military paperwork, for a fee, which he promises will be refunded. Some scammers even ask for money for medical supplies, or claim they need help to take care of a child.

- **Mail Order Bride Scams—**Traditional mail order bride services, where men pay to meet a foreign bride, have gone digital. New online sites offer users access to potential mates from around the world, for a monthly membership fee. The trouble is these sites provide fertile ground for scammers, who setup profiles and begin corresponding with users in the hopes of extracting money. The "bride" may say she needs money for

tickets or a visa to come visit, and then never appears, or fakes a family emergency and asks the victim for monetary help.

2) Love Exploits—These threats have you looking for love in all the wrong places—like dangerous websites designed to steal your information. One recent example of this is the Koobface worm, which targeted Match.com users by sending messages that appeared to be from other users, inviting them to look at photos and videos on a Match.com look-a-like site. When users tried to log in to the malicious site, it recorded their usernames and passwords and attempted to install a Trojan.

Another recent love exploit was the "KamaSutra PowerPoint" threat, which arrives via spam, offering recipients a tantalizing PowerPoint show of sexual positions. The PowerPoint slide deck itself is safe (although it contains images you would likely not want your co-workers, family members or roommates to see on your screen), but once downloaded, it stealthily installs malware on your computer.

3) Valentine's Day Spam & eCards–Scammers know that the holidays are the perfect time to send out themed messages and eCards, knowing they will grab your attention. Spam messages with subject lines such as "The Perfect Valentine's Day Gift" may contain a link to a dangerous website that asks for personal information. And, a message that appears to be an eCard from a loved one could actually download malware on your machine when you click on the link, leaving you with an infection, rather than affection.

Although these romance scams are quite common, there are some easy steps you can take to avoid becoming a victim.

In Honor of Your Heart - How To Stay Safe

- When signing up for online dating, go with a well-known dating site and get referrals from friends on which sites they use

- Once signed up to a dating site, stay incognito for a while. That way, if you run into someone who's dishonest or makes you uncomfortable, you stay safe

- Design your dating profile with care—think about the image you want to project and NEVER, under any circumstance, post personal information, such as your full name, address and phone number

- Vet potential dates by checking to see that their profile information matches other online information, such as their LinkedIn or Spokeo profile

- When meeting a date for the first time, make sure to meet in a public place and DO NOT give them your personal address. Trust your instincts—if there are red flags, you are not imagining things. End the date

- If a potential date asks you for a loan or any financial information, immediately report them to the dating site
- NEVER EVER click on links in emails or eCards from people you do not know
- When you receive an eCard, check the destination address of the link to make sure it is going to a legitimate eCard site – if you don't trust it, DO NOT click it
- To help protect you from malware, use a comprehensive security software, such as McAfee Total Protection, and keep it up-to-date

#