Online Dating

“Romance” scams have damaged consumers the most out of any kind of internet fraud. Anyone can be the victim of an online dating scam, regardless of age!

Safe Practices

- Generally, be skeptical of information provided in online profiles (be very cautious of situations that seem too good to be true).
- Be wary of online profiles that are quick to ask for personal information.
- Search his/her name in a search engine (Google, Bing, Facebook etc.) and investigate his/her background. Determine if the information you find matches up with the information provided on the dating website.
- Run his/her profile picture through a reverse-image search engine (like Tin Eye or Google Images) to see if there is a secondary name tied to that picture.
- Run his/her email address through a database of known online scammers (such as romancescams.org or Scamalytics).
- Investigate the company he/she works for, determine if the company exists and if he/she actually works there (overseas embassies can confirm if foreign companies exist).
- Do NOT send money through a wire transfer service to anyone you met online and haven’t met in person. If you are being scammed, you have a very low chance of getting your money back.
- Be skeptical of repeat requests for money.
- Do not stop using the dating website as the primary form of communication, even if your suitor insists.
- If the person claims to know a mutual friend or acquaintance, ask them specific questions about him/her, and ask the friend to verify.
What to do if you are a victim?

- Immediately **cut off all contact** with the suspected scammer.
- **File a police report!**
- **Find out** if the online dating website itself is **legitimate**.
- If the online dating website itself is legitimate, **alert any authorities** or administrators of the website.
- If you have given the scammer information about your location or that of any loved ones, and there may be a chance he/she would try to cause physical harm, **take necessary security precautions** (e.g. warn friends to be more vigilant, change locks, etc.).
- If you believe that the suspected scammer has enough information to acquire a credit card, loans, or other credit in your name (for example, your Social Security Number), alert the 3 major credit bureaus (Experian, TransUnion, and Equifax) and **file a fraud victim statement**, or **place a “security freeze” on your credit reports**.
- If you have given financial details (for example, credit card information) to the suspected scammer, **immediately alert your bank**.
- If you have provided other sensitive account information (for example, usernames and passwords) to the suspected scammer, immediately **alert** all websites and organizations that she/he may be able to access in your name, and **change any login information that you control**.

If you believe you are a victim of an online dating scam, submit a complaint to the Internet Crime Complaint Center of the Federal Bureau of Investigation at **www.ic3.gov**.

For more information, visit us at **www.penncase.org**

Penn CASE is a student organization at the University of Pennsylvania