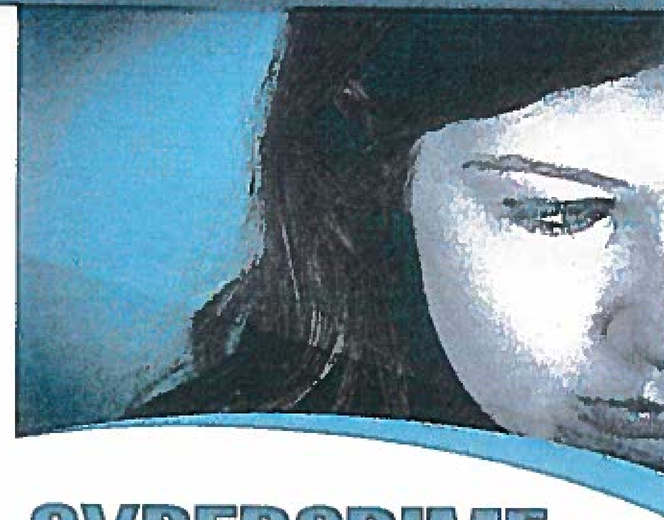
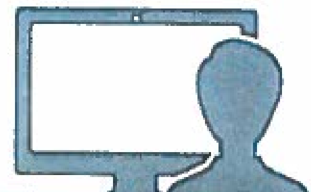
CYBERCRIME Prevention





The average annual cost per victim (including direct, indirect, and opportunity costs) of cybercrime targeting organizational victims in the United States was $11.6 million in 2012 (up 26% from the year before). While any estimate for overall losses stemming from clandestine activity is necessarily hindered by a lack of data, best estimates currently put annual net U.S. losses attributable to cybercrime in the neighborhood of $100 billion.

REAL ESTATE SCAMS

In real estate scams, perpetrators attempt to sell or rent property that does not exist or property that they do not own to victims.

Tips to Avoid Victimization

- Never wire money. It is the same as sending cash.
- Beware of below-market rate rental offers.
- Do not provide a security deposit or first month's rent before meeting the landlord or signing a lease.
- Use caution if a property owner claims to be outside of the United States or away on business.

ROMANCE SCAMS

Romance scams occur when individuals use the promise of love and romance in order to manipulate victims into sending money or other things of value.

Tips to Avoid Victimization

- When an online suitor requests money or material assistance, it is time to terminate the relationship.
- Check to see if the pictures used occur on any other websites.
- Look for frequent misspellings and poor grammar.
- Don't reply to messages asking for personal or financial information.
- Don't agree to deposit a check and wire money back.

WORK-AT-HOME SCAMS

Work-at-Home scams involve the promise of the opportunity to work from home at one's own pace in order to make often substantial amounts of money, but these offers are often bogus.

Tips to Avoid Victimization

- Contact the Better Business Bureau to determine the legitimacy of the company.
- Be suspicious when money is required up front for instructions or products.
- Don't provide personal information when first interacting with your prospective employer.
- Do your own research into legitimate work-at-home opportunities, using the "Work-at-Home Sourcebook" and other resources available at your local library.

COPS U.S. Department of Justice

NW3C National White Collar Crime Center

This project was supported by Cooperative Agreement Number 2013-CK-WX-K027 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, companies, products, or services should not be considered an endorsement by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

Photo Credits: [illegible]

ADVANCED FEE FRAUD

Advance Fee Fraud occurs when a victim is asked to pay a fee in order to receive something of value but nothing of value is ever delivered.

Tips to Avoid Victimization

- Be wary if you receive an email asking you to send personal or identifying information in order to receive something else in exchange.
- Be skeptical of any individuals representing themselves as officials or humanitarians asking for help that requires you to supply money.
- Do not pay up-front fees for a "prize" or something that should be considered free.

AUCTION FRAUD

Auction fraud is classified as fraudulent transactions that occur in the context of an online auction site such as eBay.

Tips to Avoid Victimization

- Pay attention to user ratings. Try to learn as much about the seller/buyer as possible.
- Use a well-known auction service and if possible pay with a credit card or third party escrow service, such as PayPal.
- Be cautious if asked to supply personal information (such as social security number or driver's license information).
- Be wary if asked to wire money rather than pay through another means.

COMPUTER CRIMES

Computer crimes are defined as (1) crimes that target computer networks or devices directly or (2) crimes facilitated by computer networks or devices.

Tips to Avoid Victimization

- Maintain the most up-to-date anti-virus malware protection available and make sure the patches and periodic software updates are up to date on your machine.
- Never respond to email solicitations from a source you are not familiar with and never open an attachment from a suspect source.
- Back-up contents of your hard drive as frequently as possible.
- If dealing with ransomware, do not pay the perpetrators.

CREDIT/DEBIT CARD FRAUD

Credit/debit card fraud involves the unauthorized charging of goods or services or cash withdrawals to a victim's credit or debit card.

Tips to Avoid Victimization

- Call the credit card company and inquire.
- Scrutinize all credit or debit card statements when they arrive.
- Be sure to shred any credit card or bank statements when you are through with them.
- Notify your card issuer if your address changes or if you will be traveling.
- Never give your account number to anyone on the phone unless you've made the call to a company you know to be reputable.

HEALTH-RELATED FRAUD

Any kind of health-related or health insurance-related fraud that someone can fall victim to online.

Tips to Avoid Victimization

- Affordable Care Act is only available through www.healthcare.gov or by calling 1-800-318-2596.
- Do not give your personal information to anyone contacting you regarding the Affordable Care Act.

Tips to Avoid Affordable Care Act Scams

- Never sign blank insurance claim forms.
- Never give blanket authorization to a medical provider to bill for services rendered.
- Don't do business with door-to-door or telephone salespeople who tell you that services of medical equipment are free.

IDENTITY THEFT

Identity theft is the illegal use of an other person's identifying information (such as a name, birth date, social security and/or credit card number).

Offline Tips

- Protect your personal identifying information, especially your social security number.
- Be sure you know who you are sharing personally identifiable information with over the phone.
- Be careful when disposing of electronic devices and documents containing personal information.
- Avoid leaving mail in your box for long periods.

Online Tips

- Use complex and varying passwords.
- Beware of emails from unknown sources.
- Use caution when accessing public Wi-Fi.
- Utilize security software on your electronic devices.