Avoiding Frauds and Scams

Barbara Martin-Worley
Director, Consumer Fraud Protection
18th Judicial District Attorney's Office

Serving Arapahoe, Douglas, Elbert and Lincoln Counties

Common Scams

You Have
Won
$50,000.00

Extortion Scams

Have two things in common:

- You are given a very short period to respond
- There is a threat or penalty if you do not respond

Prevent Becoming a Victim

- Never talk to strangers on the telephone – they are not calling to wish you a good day. They are invading your privacy.

- Use an answering machine, voice mail or Caller ID to screen calls.

- Never give any personal information, including credit card numbers, bank account, or Social Security Numbers, passwords or pin numbers, driver's license number, etc., to anyone who calls you, UNLESS YOU INITIATE THE CALL.

Cyber Crimes

- Email/websites
- Social networking sites
- On-line classified ads
- Mobile devices

Cyber Crimes

Craigslist Scams

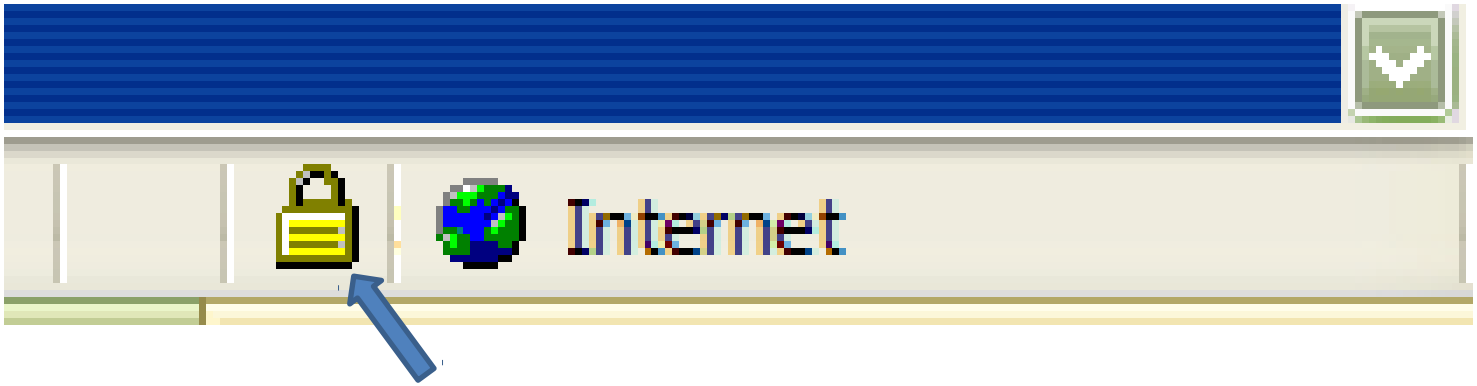
- Never do business without vetting the buyer; seller.
- Deal with local advertisers.
- Meet in person first, in a public setting, before agreeing to a purchase or service.
- Be wary if the advertiser is unable to meet in person.
- Never wire or send money in advance.

Cyber Crime Prevention

Electronic Communications:

- Know who you are communicating with.
- Watch what is posted on social networking sites about you or your family.
- Use electronic funds transfer & direct deposit.
- Password protect online business transactions.
- Update virus protection software regularly.
- Confirm you are on a secure website before making on-line purchases.
- **Always log off each time you are finished.**

Is Website Safe?



Stop Unwanted E-Mail

- Register at www.dmachoice.org
- Registration is free and good five years

Risks on Social Media

There are strangers who “friend” you, but they really aren’t your friend.

Risks on Social Media

- These are “friends” who try to get you to click on videos or other attachments, or download a document to “fix” a problem. By doing so, these attachments can infect your computer with viruses and other malware.

- Sometimes, these attachments allow such “friends” to steal your personal information off of your computer.

Risks on Social Media

Be careful of what you post on Facebook:

- Photo's that show house numbers or street names in the background
- Personal information about you or other family members that a stranger can use to steal identity, such as:
- Names of family members, birthdates, addresses

Protection

- Adjust website privacy settings
- Only select “friends” who you trust, because once you select a friend, they can access any information that you allow to be viewed by all friends.
- If you don’t know a friend well, only give them limited access to your profile
- Be careful what you click on, on others’ sites

Cell Phone Safety

Most common method of infecting phone with malware is by downloading apps and games.

Cell Phone Safety

Risk Factors:

- Not researching origin of apps before downloading

Signs:

- Apps that don't include privacy policies
- Apps that show up on phone that you didn't download
- Texts From unknown sources

Cell Phone Safety

- Read all privacy policies before downloading apps.
- Adjust settings to block unwanted numbers.
- Routinely upgrade apps – includes the additional benefit of providing updated security patches.
- Contact mobile phone carrier or manufacturer to resolve a security breach.