ONLINE SAFETY

- Don't give out your personal information, banking information,credit card numbers via e-mail or phone
- When making online purchases, check to make sure the seller is reputable
- When purchasing online, check to see if insurance is available
- Contact police to make a report if your identity is stolen
- Use false age (if any) in social networking—by giving your real age, people saying "happy birthday' on your wall will reveal to everyone your exact date of birth

Online Precautions are critical

Helpful Links:

- www.ftc.gov/idtheft
- http://www.lookstoogoodtobetrue.com

CREDIT REPORTING AGENCIES:

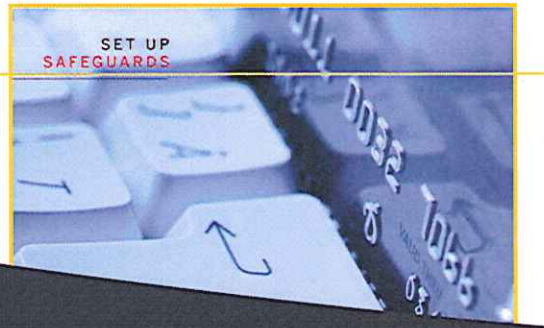
Equifax - www.equifax.com
1-800-685-1111

Experian – www.experian.com
1-888-EXPERIAN (888-397-3742)

Trans Union –
www.transunion.com
1-800-916-8800

it won't happen to me...

- NOBODY PLANS TO BE A VICTIM OF IDENTITY THEFT
- IDENTITY THEFT CAN HAPPEN TO ANYONE, EVEN SOME POLICE OFFICERS HAVE BEEN VICTIMS, NO ONE IS IMMUNE TO THIS GROWING CRIME
- PLAN AHEAD, SET UP SAFE-GUARDS TO HELP PREVENT IDENTITY THEFT



THIS PUBLICATION IS PROVIDED FREE OF CHARGE BY
ARDMORE POLICE DEPARTMENT

ARDMORE POLICE DEPARTMENT

Second Floor
Ardmore City Hall
23 South Washington
Ardmore, Oklahoma 73401

non-emergency 223-1212
Ardmore CrimeStoppers 580-504-4LAW

IN AN EMERGENCY, DIAL 911

PROTECT YOUR IDENTITY

FROM IDENTITY THEFT

ARDMORE POLICE DEPARTMENT
ARDMORE, OKLAHOMA

My Identity Has Been Stolen, What do I do now?

Alert your bank and credit card companies

Check your credit report regularly (a credit monitoring service can do this for you at a cost and can put your status on high alert for you)

Contact the credit reporting agencies and have anything that is not yours removed. (some credit monitoring services will do this for paying members — before signing up, make sure the company provides this service)

Report possible fraud to local police who forward data to police where suspect is operating.

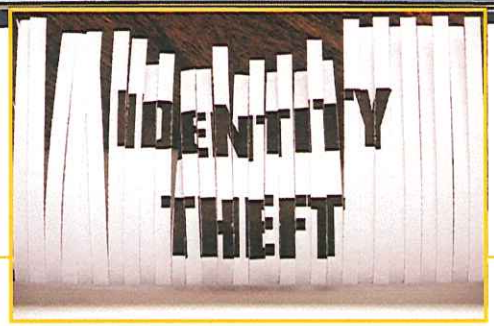
Report to ic3.gov FBI website for Internet Fraud & enter complaint.

Report to uspsoig.gov/investigation.htm Inspector General for US mail and enter complaint if the US Postal Service (mail) is involved.

Report to Internet source from which you contacted the suspect - website of auction, merchandiser, other. Some have systems for protection and possible recovery.

METHODS OF IDENTITY THEFT

- *PHISHING* IS USING A LURE TO GET PEOPLE'S INFORMATION SUCH AS "YOU'VE WON $10K, JUST ENTER YOUR BANKING INFORMATION FOR DIRECT DEPOSIT, OR "YOUR ACCOUNT HAS HAD UNAUTHORIZED ACCESS, PLEASE CONFIRM YOUR BANK ACCOUNT AND ADDRESS SO WE CAN CORRECT THE SYSTEM"
- PHISHING CAN BE DONE THROUGH E-MAIL✉, TELEPHONE ☎, TEXT MESSAGE, POSTAL SERVICE MAIL📪, OR IN- PERSON REQUESTS FOR ASSISTANCE
- REQUESTS FOR ASSISTANCE OFTEN CONSISTS OF AN EMERGENCY, SUCH AS A SPOUSE TEXTING FOR BANK ATM PIN OR PERSON STRANDED NEEDING MONEY TO GET HOME
- TRASH PICK-UP (COLLECTING INFORMATION FROM YOUR DISPOSED TRASH)
- MAIL SCAMS 📪 (OFTEN SAYING YOU CAN HELP SOMEONE OR YOU'VE WON SOMETHING)



PREVENTION

- PASSWORD PROTECT ANY INFORMATION YOU HAVE ON YOUR COMPUTER
- PASSWORD PROTECT YOUR SMARTPHONE
- USE UP-TO-DATE VIRUS AND SPYWARE PROTECTION SOFTWARE
- IF USING WIRELESS ROUTER, SECURE IT (PASSWORD PROTECT LOG-IN)
- SHRED DOCUMENTS WITH PERSONAL INFORMATION BEFORE THROWING AWAY
- DO NOT CLICK ON SPYWARE, "YOU ARE NOT PROTECTED", OR OTHER POP-UPS THAT ARE NOT INTERNAL (NOT THE VIRUS PROTECTION YOU USE)
- DO NOT ANSWER E-MAILS CONCERNING YOUR BANK ACCOUNT OR RECENT PURCHASE, CALL YOUR BANK OR SERVICE PROVIDER WITH NUMBERS YOU HAVE ON FILE, NOT THE NUMBERS THEY PROVIDE IN E-MAIL OR CALL