Department of
CITIZEN SERVICES
Aging • Children's Services • Consumer Affairs

MINIMIZE YOUR RISK FOR IDENTITY THEFT

Con artists want to steal your identity for a number of purposes: to steal money, obtain access to credit, obtain health care and even commit crimes.

To reduce your risk of becoming a victim, never give out personal information over the telephone, through the mail, or on the internet, unless you have initiated the contact, know who you're dealing with, and how the information will be used.

Personal Safety

- Keep all personal information in a safe place.
- Provide your social security number to others only when absolutely necessary.
- Do not carry credit cards, social security card, passport, and other forms of personal identification that you don't regularly use.
- Take your receipts from all bank machines, gas pumps, and retail stores.

Mail Safety

- Promptly remove mail from your mailbox after it is delivered. For even greater protection, use a locking mailbox, or a PO Box for mail delivery.
- Shred all mail that contains personal information, such as: pre-approved credit applications, credit card receipts, bills and medical statements.
- Pay attention to credit billing cycles. If bills don't arrive on time, contact your creditor. A missing bill could mean that a thief has hijacked your account and changed the billing address.
- Do not send checks from your home mailbox. Instead, put outgoing mail in an official mailbox or take it to the post office.

Internet Safety

- Install virus protection and security software from a reputable company. Update that software regularly, using the directions given by the company when you purchased the software.
- Beware of e-mail or pop-up messages that instruct you to click on a hyperlink or downloading software to do any of the following:
    - Update your security software. Before doing so, make sure the message is from the company from whom you purchased the software and that the instruction is consistent with information provided by the company at purchase. ID thieves often use this ploy to

obtain access to your computer files that contain personal financial and other information.

- Verify your account information. Banks and other creditors rarely make such requests. If you are unsure whether the request is legitimate, call the creditor using contact information on your bills (not from the questionable message).

- Only make purchases from secure websites. Look at the website's URL to see if it begins with "https" (the s stands for secure). Some merchants also use third-party payment entities (such as PayPal) for secure transactions.
- Password-protect your credit and other financial accounts and chose passwords and security questions that only you will know.

Social Media Safety

- Read privacy and security policies closely to know what information the site sells or gives to others. Use the highest level privacy setting available on the site.
- Provide the least amount of information necessary to register for and use the site.
- Never include personal information (e.g. address, social security number, birth date) in your screen name or in posts.
- Be cautious about accepting invitations to connect from unfamiliar contacts.
- Verify e-mails you receive from and through social network sites. One recent Facebook scammer asked customers to re-set their passwords in order to get access to other personal information. In another scam, users lost money after receiving e-mails from imposters claiming to be friends or relatives who were in trouble in another country and needed money to get home or for bail.

Exercise Common Sense

- When in doubt: don't open it, download it, or link to it
- Don't give out any personal information that you have any doubts about sharing.

To obtain this factsheet in an alternative format, please contact the Office of Consumer Affairs at 410-313-6420(voice/relay) or email us at consumer@howardcountymd.gov.