Identity Theft fraud is one of the fastest growing crimes in America, and the Washington, D.C. Metropolitan area is not immune. The Montgomery County Office of Consumer Protection and Department of Police Financial Crimes Section are jointly providing the following safety tips to the public in an effort to help limit the potential for victimization by identity theft or fraud:

CREDIT REPORT

Federal laws entitles you to receive one free copy of your credit report every 12 months from each of the three nationwide credit reporting companies (Experian, Equifax, Transunion). Your credit report can be ordered online from annualcreditreport.com. This is the ONLY authorized website for obtaining free credit reports. After reviewing your report, immediately contact your bank or credit card company if you notice an error or discrepancy.

SHRED ALL DOCUMENTS

Protect your personal information by shredding all documents that contain financial or personal information. If you do not own a shredder, Montgomery County holds free shredding services yearly. For more information, please contact the Montgomery County 311 Call Center at 240-777-0311 or via the internet at www.montgomerycountymd.gov/.../paper-shredding.html.

WALLETS/PURSES

1. Limit the amount of information that you carry in your wallet or purse.
2. Keep social security numbers, PINs, and passwords out of your wallet or purse.
3. Write “ask for ID” on the back of your credit or debit cards.
4. Keep your wallet or purse securely on your person.

MAIL

1. Install a locked mailbox at your residence to deter mail theft.
2. Use a post office box or a commercial mailbox service to ensure security of your mail.
3. When you are away from home for an extended time, have your mail held at the post office or ask a neighbor or friend to collect it daily.
4. When ordering new checks, pick them up at the bank or request that the checks be mailed with a signature requirement for receipt.
5. Suspects often remove mail from mail boxes and look for outgoing checks. The suspects then alter and cash the checks at area banks. Be sure to drop outgoing mail at your local post office or in a U.S. Postal Service mailbox. The Montgomery County Police Department recommends not using the “flag” on your mailbox as an alert that there is mail waiting in the box.

SCAMS

Criminals often target unsuspecting victims by contacting the potential victim and claiming that the victim has won a lottery, owes money for taxes, has unpaid utility bills, or that a loved one has been arrested. Methods of contact can be via the phone, the internet, or in person. It is important to remain calm in these situations and ask plenty of questions. Remember that scammers are trained professionals that have a response for most questions that you might ask. Keep in mind that:

1. Legitimate government agencies and companies will never threaten to arrest you, deport you, or turn your residential/business utilities off immediately.
2. Legitimate government agencies and companies do not request payment via a re-loadit card, gift card, money order, or similar method.

3. Check the phone number that the caller is calling from and make a note of it. Many scammers use “spoofed” telephone numbers that actually appear like they are calling from a government agency or utility company. Before providing any information or money, contact the agency or company yourself. Do not call the number provided to you by the scammers or the call ID. Rather, research the number by looking at an old account statement. If in doubt, contact your local police department or utility company to verify the information or account.
4. Pull out your last utility statement and ask the caller to tell you the account number and amount due, but never provide this information to them.
5. NEVER give out your personal information, such as your credit card number, social security number, date of birth, etc.

ATM MACHINES

1. Check the ATM before using the device. Look for loose pieces or tape or glue marks which might indicate the presence of a skimming device. Report these immediately to the bank.
2. Beware of shoulder surfers. These are people around you that might be looking over your shoulder to obtain your PIN number.

ELECTRONIC DEVICES

Electronic devices such as cell phones and tablets are stolen at an alarming rate. Remember these tips:

1. Record the serial numbers of your devices.
2. Use strong passwords consisting of a combination of letters, numbers, and special characters.
3. Secure wireless internet routers with a password.
4. Ensure that your electronic devices have up-to-date security software.
5. Do not respond directly to emails or texts from people or companies that you do not know.
6. Avoid clicking on internet links that are contained in emails, even if it might be from a company that you currently do business with as these links can be “spoofed”. Instead, log into the company’s website yourself.
7. When disposing of your old electronic devices, be sure to wipe the data clean.
8. If you receive a phone call or email from a person/company stating that they have information that your computer has a problem and that they can fix the problem for a fee, hang up. Legitimate companies do not and cannot monitor your computer legally without your permission. Once you allow them access, however, they can download your personal information or install malware - programs that report information back to them without your knowledge.

HELPFUL NUMBERS/WEBSITES

- Montgomery County Office of Consumer Protection – (240) 777-3636 or www.montgomerycountymd.gov/OCP
- Montgomery County Police Department – (301) 279-8000 or www.mymcpnews.com
- Equifax – (888) 766-0008
- Experian – (888) 397-3742
- TransUnion – (800) 680-7289
- PEPCO Customer Service – (202) 833-7500 / www.pepco.com
- WSSC Customer Service – (301) 206-9722 / www.wsscwater.com
- Washington Gas Customer Service – (703) 750-1000 / www.washgas.com
- Federal Trade Commission – (877) 382-4357 / www.ftc.gov