Please take a few moments to think about the answers to the following questions. Be honest. This activity can help you identify those areas where you're most vulnerable for identity theft.

OPEN YOUR WALLET. DOES IT CONTAIN:
- Your Social Security card?
- A driver’s license with a SSN (Social Security Number) on it?
- A health insurance card with a SSN on it?
- A list of SSNs for family members?

If you carry these items, you're vulnerable.
- Do you review all statements or online banking to check to make sure each charge is legitimate? **If not, you're vulnerable.**
- Do you use a cross-cut shredder to destroy credit card offers, statements with account numbers on them and other papers that contain your personal information? **If not, you're vulnerable.**
- Do you use the last four digits of your SSN as your personal identification number (PIN)? **If you do, you're vulnerable.**
- Do you have an easy-to-remember password, such as your child’s or pet’s name? **If you do, you're vulnerable.**
- Do you check your credit report annually for signs of ID theft (such as unfamiliar accounts)? **If not, you're vulnerable.**

CONTENTS OF YOUR WALLET:

<table>
<thead>
<tr>
<th>ITEM</th>
<th>ACCOUNT/ID NUMBER</th>
<th>PHONE # TO CALL IF LOST/STOLEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver’s license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof of car insurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debit card(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail card(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roadside assistance card(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health insurance/medical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT:** Keep this list in a safe place or keep account numbers in a separate location.
Technology brings us all kinds of convenience and entertainment. It also creates new ways for crooks to take advantage of consumers. The scams and the lingo change all the time. Here's an abbreviated technology fraud dictionary to keep you in the know.

**Pharming**
This secretly plants a virus or malicious program in your computer and hijacks your web browser. Pharming crimeware misdirects users to fraudulent sites or proxy servers. When you type in the address of a legitimate website, you're sent to a fake site without knowing it. If you give your password or account information on the fake site, thieves will use your account fraudulently.
Pharming can occur four ways:
- Static domain name spoofing (misspellings: vwestcu.org vs. westcu.org)
- Malicious software, or malware (viruses and Trojans redirect you to the false site)
- Domain hijacking (hacker hijacks legitimate site and redirects all traffic)
- DNS poisoning — most dangerous (you enter correct URL, but poisoned server redirects)

**Phishing**
In this scam, you receive an email prompting you to reveal personal details — your Social Security number, passwords or credit card information — by clicking on a link to a bogus webpage mimicking a legitimate company. These emails and linked sites used to have an amateurish look that was easy to spot; now, they often are indistinguishable from the real thing.
A clear tip-off that it’s fake: Typically the greeting is generic and not addressed to you by name. Another characteristic is a sense of urgency or alarm and that your account is about to be closed. Delete the message and report it to your financial institution immediately. Also, report suspicious activity to the Federal Trade Commission.

**Pretexting**
Sometimes referred to as "social engineering," it occurs when someone tries to get personal or private information without authority to do so. The scammer may ask for private information while impersonating an accountholder by phone, mail, email or even by phishing — using a phony website or email to collect data. Be especially wary of callers who claim to be calling on behalf of a survey firm and then ask you for some personal information.

**Smishing**
This is phishing via SMS (short message service) and it’s targeted at mobile phone users who use text messaging. One of the first known Smishing attacks looked like this: “We’re confirming you’ve signed up for our dating service. You will be charged $2 a day unless you cancel your order.” The message included a web link that routes you to the main phishing page, where you’re prompted to download a program. The program you download turns out to be a virus called Trojan Horse which turns your computer into a zombie controlled by hackers. Hackers can then use this access to get into your larger network to steal personal account information and perform other malicious activities.
Be cautious about unregistering from a service when you’re sure you didn’t make a formal arrangement with the sender.
COMPUTER “HOUSEKEEPING” TIPS
• Install and update current virus protection software.
• Install firewall software to partially guard against spyware, which can capture account numbers and passwords, slow down your computer, cause pop-up ads to appear, and report surfing behavior to advertisers. Resource: onguardonline.gov.
• Install spyware detection and removal software. A sampling of good programs includes:
  - Ad-Aware SE
  - McAfee VirusScan
  - Microsoft's Windows Defender
  - McAfee Stinger
  - MalwareBytes
  - Spybot Search & Destroy
  - Spyware Blaster
  - Spyware Doctor

NOTES
• Beware of look-alikes such as No-Adware.
• Check spyware removal program ratings at download.cnet.com ($0-$40).
• Install a spam blocker.
• Beware of peer-to-peer file sharing services — many include spyware.
• Run the latest patches and fixes from Windows Update to keep Windows and any other regularly used software up-to-date.
• Use a secure browser to scramble communications.
• Set browser security level to at least medium. [Tools: Macro: Security: Medium]
• Secure your wireless network. Disable the broadcasting of the SSID (Service Set Identifier) after you configure your router. Make sure your wireless router has an encryption feature or turn it on if it was turned off before delivery.

GENERAL USAGE TIPS
• Use strong passwords — a combination of letters (upper and lower case), numbers and symbols—at least eight characters long.
• Turn off your wireless network when you’re not using it. Public “hot spots” are not secure.
• Don’t use public computers to access financial accounts.
• Avoid emailing personal and financial information.
• Password - protect tax returns.
• Don’t click on links to webpages within email messages you weren’t expecting. Contact the company directly — call, or retype weblink.
• Don’t download files or open attachments from strangers.
• Avoid automatic log-in; always log off when done.
• Lock your computer when you leave the workstation. Lock your laptop with security cable; don’t leave a laptop in your car.
• Securely erase the hard drive before disposing of the computer. Reformat hard drive, or use hard drive erase utility. Conduct a search on how to do this for your particular operating system or personal computer. Consider “shredding” software to delete files.
**Minimize your risk**

**Steer clear ...**
- Use “strong passwords” that include upper and lower case letters, numbers, and symbols. Memorize a sentence and then use the first letter of each word—including numbers and symbols—as your password (e.g., “My #2 dog is a Lab/Poodle mix” becomes M#2diaL/Pm).
- Never use easily recognizable passwords (e.g., mother’s maiden name, birth date, last four digits of SSN or consecutive numbers).
- Never authorize payment over the phone unless you initiated the call.
- Never access sensitive personal information, or accounts, from a public computer or using a public Wi-Fi network.
- Never give personal information to callers (even the IRS). A call from the “IRS” is likely a scam.

**Get in the habit ...**
- Whether you’re at home or traveling, expect occasional challenge questions when conducting online transactions to verify your identity and protect your accounts from crooks.
- Check your credit report annually at AnnualCreditReport.com, as well as your child’s at IDTheftCenter.org.
- Review statements monthly (more often online).
- Safeguard wallets, purses, checkbooks and account statements—at home and at work.
- Mail bills from a locked mailbox or the Post Office.
- Shred (cross cut) preapproved credit card offers, statements, bills and personal documents.
- Guard against shoulder surfers. Cover the keyboard as you punch in your PIN.
- Don’t carry your Social Security card in your wallet unless you need it that day.

**Be proactive ...**
- Go paperless! Use electronic deposit of paychecks, dividends, pension, Social Security payments and tax refunds. Use online BillPay—it’s safer than mailing checks.
- Lock down your smartphone. Go to settings and set a PIN or passcode. Install Lookout a software that allows you to lock the phone remotely. Turn off GPS.
- Keep a list—in a safe place—of account numbers, expiration dates and numbers to report theft. Don’t keep that list in your wallet.
- Dry up junk mail: (1) Get off prescreened credit card lists by calling -- 88.5opt.out or go to optoutprescreen.com; and (2) Register with Direct Marketing Association’s Mail Preference Service at dmachoice.org.

**Shop safely online ...**
- Shop only with companies you know.
- Pay only with credit card, or with third-party intermediary.
- For online transactions, use Verified by Visa and/or MasterCard’s Secure Code.
- Use a separate credit card for online purchases to track purchases easily.
- Use a secure browser (look for closed padlock or unbroken key at bottom of browser window—not the payment page). URL must change to “https://”.
- Keep a paper trail, never send financial information via email and understand privacy policies.
RESOURCES

CREDIT REPORTING AGENCIES

<table>
<thead>
<tr>
<th>Agency</th>
<th>Website</th>
<th>Order Reports</th>
<th>Fraud units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equifax</td>
<td>Equifax.com</td>
<td>800.685.1111</td>
<td>800.525.6285</td>
</tr>
<tr>
<td>Experian</td>
<td>Experian.com</td>
<td>888.397.3742</td>
<td>888.397.3742</td>
</tr>
<tr>
<td>TransUnion</td>
<td>Transunion.com</td>
<td>800.888.4213</td>
<td>800.680.7289</td>
</tr>
</tbody>
</table>

FREE CREDIT REPORTS

AnnualCreditReport.com (877.322.8228)
Annual Credit Report Request Service | PO Box 105281 | Atlanta, GA 30348-5281

GET OFF MAILING LISTS

Direct Marketing Association dmachoice.org
Opt Out optoutprescreen.com (888.5OPT.OUT)

IDENTITY THEFT RESOURCES

Federal Trade Commission ftc.gov (877.IDTHEFT)
OnGuard Online onguardonline.gov
ID Theft identitytheft.gov

ORGANIZATION CONTACTS

Better Business Bureau bbbonline.org
Privacy Rights Clearinghouse privacyrights.org
callforaction.org

PROTECT YOUR COMPUTER

download.cnet.com/windows
killdisk.com
lavasoft.com
onguardonline.gov

REPORT THEFT OR FRAUD

Federal Trade Commission ftc.gov/ bcp/edu/microsites/idtheft
Internet Crime Complaint Center IC3.gov
Treasury Inspector General www.treasury.gov
FTC 877.438.4338
Social Security Fraud 800.269.0271