



IDENTITY THEFT

To steal your identity, criminals need your personal information, which includes: your Social Security number, birthdate, address, bank account and credit card numbers, passwords, and *anything used to answer security questions*.

PROTECT YOURSELF: NEVER GIVE OUT PERSONAL INFORMATION UNLESS YOU HAVE INITIATED THE CONTACT.

HOW IDENTITY THEFT HAPPENS

LOW TECH - OFFLINE

1. Lost or stolen property
2. In-home service provider and unsecure personal information
3. Stolen mail
4. Credit card taken out of customer's sight
5. Bribing employees
6. Shoulder surfing/Dumpster diving

HIGH TECH - ONLINE

1. Security breach
2. Unsecure Wi-Fi
3. Skimming
4. Phishing
5. Social media
6. Inadequate privacy settings



PROTECT YOURSELF - OFFLINE

EXPERTS RECOMMEND:

- Don't leave valuables unsecured at home if there are strangers/service providers who visit.
- Lock your valuables while at work.
- Leave your Social Security card at home.
- Keep important documents in a safe at home or a safety deposit box at the bank.
- Protect your family's Social Security and Medicare cards and numbers.
- Know how your child's school shares and protects information.
- Photocopy important identification (driver's license, credit cards, and passports, etc.) on a personal copier.
- Check account statements regularly. Look for charges you didn't make. Be alert for bills that don't arrive when you expect them and follow up.
- Be cautious with your mail. Incoming or outgoing mail should never sit in your mailbox for an extended amount of time.
- Shred documents with personal and financial information.
- Review medical Explanation of Benefits statements and report any fraudulent services.



OPT-OUT

STOP CREDIT CARD OFFERS BY:



888-567-8688



www.optoutprescreen.com

This removes your name from the list sold by major credit reporting agencies for a period of five years or permanently.

You will be asked to provide your Social Security number.

MEDICARE FRAUD

BE SUSPICIOUS OF ANY HEALTH CARE PROVIDER WHO:

- Asks for your Medicare number in exchange for free equipment or services.
- Advertise "free" consultations to people with Medicare.
- Call or visit you and say they represent Medicare or the federal government; or
- Use telephone or door-to-door selling techniques.

Visit [Stop Medicare Fraud](http://StopMedicareFraud.gov) for more information. (www.stopmedicarefraud.gov)

PROTECT YOURSELF - ONLINE

With an increasing mobile lifestyle, it's important to keep tabs on and know exactly what you're sharing online.



Public
Wi-Fi



EXPERTS RECOMMEND:

- Never open an email from an online sender you don't know.
- Don't open email attachments unless you know who sent it and what it is.
- Don't use public Wi-Fi for sensitive transactions.
- Never email or text any financial or account information.
- Avoid using the same password for multiple accounts and websites.
- Create a strong password that is hard to guess but easy to remember.
- Password protect all of your devices - smartphone, tablet, computer, etc.
- Properly wipe any device before selling or recycling it.
- Be cautious about posting personal identifying information.
- Never give out personal information to someone unless you have initiated the contact.
- Use privacy settings to restrict access.
- Manually manage location services on your phone.
- Know privacy policies.

CHECK EVERY FOUR MONTHS



You are entitled to a free report from each of three credit reporting agencies every year. Order a free report every fourth month. You will be asked for your Social Security number when you request your free credit report.

To protect your Social Security number, choose the option on the form that allows you to redact all but the last four digits of your number from the

report you will receive.

[Request your free report](#) thru Annual Credit Report.com or call 877-322-8228.

IF YOU'VE BECOME A VICTIM

Visit the [federal government one-stop resource](http://www.identitytheft.gov) (www.identitytheft.gov) to help you report and recover from Identity Theft. The FTC will help you develop a recovery plan, including what to do right away; how to place a fraud alert and get your credit reports; and how to file a report with your local police department.

RESOURCES

[Federal Trade Commission](http://www.ftc.gov)

877-438-4338

(www.identitytheft.gov)

[OnGuardOnline](http://www.ftc.gov/onguardonline)

(www.ftc.gov/onguardonline)

[Identity Theft](http://www.idtheftcenter.org)

[Resource Center](http://www.idtheftcenter.org)

888-400-5530

(www.idtheftcenter.org)

[Stop.Think.Connect.](http://www.stopthinkconnect.org)

(www.stopthinkconnect.org)

[IRS Identity Protection Specialized Unit](http://www.irs.gov/individuals/identity-protection)

800-908-4490

(www.irs.gov/individuals/identity-protection)

[IRS Form 14039](http://www.irs.gov/pub/irs-pdf/f14039.pdf)

(www.irs.gov/pub/irs-pdf/f14039.pdf)

[Identity Theft Affidavit](http://www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf)

(www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf)

[IRS Taxpayer Guide to Identity Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft-1)

(www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft-1)



Identity theft can happen to anyone. That's why it's important to keep your personal information to yourself - offline and online. One of the best ways to protect yourself is by never providing personal information to someone unless you have initiated the contact!

An [electronic copy of this handout](#) is available through the QR code below or on our website (www.mi.gov/ce). While you're there, [schedule a presentation](#) (www.mi.gov/ce) for one of our other seminars.

For questions, contact Attorney General Bill Schuette's Consumer Programs team at 877-765-8388 or agcp@mi.gov.

