Financial Education
Protecting Your Identity

Help keep your identity safe by practicing online security and limiting access to your personal information.

Identity theft is when someone steals your personal information or identity to commit fraud. This could be things like your name, Social Security number, credit card number, or bank account information. Thieves can use this kind of information to rent apartments, take out loans, open accounts in your name, or put charges on your existing accounts without your permission.

Identity theft, fraud, and data breaches affect tens of millions of people in the U.S. each year. This is why it's important to be cautious with your identifying information—both online and in the real world.

CHECK YOUR CREDIT REPORT

Check your credit report at all three nationwide credit reporting companies (Equifax, Experian, and TransUnion) each year using the free website annualcreditreport.com. If you see anything in your report that's incorrect or suspicious, contact the credit reporting company and the company that furnished the information immediately. If you're concerned about past or future identity theft, you can also freeze or put a fraud alert on your credit file. See Module 7: Understanding Credit Reports and Scores for more information.

You can also opt out of receiving offers for credit or insurance, known as prescreened offers. This can help prevent credit or insurance offers that are meant for you from falling into other people's hands—these offers can then be used to take out fraudulent loans in your name. Remove your name from mailed pre-screened offers by opting out at (888) 567-8688 or online at optoutprescreen.com. Choose the "5-year" removal option to stop prescreened offers for five years—or make a request by mail if you want to opt-out permanently. Choose the "forever" removal option. Even if you opt out of these offers, you can still apply for credit when you want it by contacting the lender directly or applying online.

LIMIT ACCESS TO YOUR INFORMATION

- Don't carry your Social Security card or number in your wallet or purse. Keep it somewhere safe at home.
- Remove your name from many direct mail marketers' lists by registering with the Direct Marketing Association using the online form at dmachoice.thedma.org. This will create fewer opportunities for thieves to steal your information.
- Remove yourself permanently from most telemarketers' lists by registering your cell phone or landline number with the Do Not Call Registry at (888) 382-1222 or at donotcall.gov.
- Never give your personal information to someone who calls you and asks for it, even if they say they're from your financial institution. If you want to confirm if the call was legitimate, hang up and call that financial institution back using a phone number you trust, like the one on your bank statement or the back of your credit card.
- Use a shredder, scissors, or your hands to tear all papers with identifying information or account numbers into tiny pieces before throwing them out. Also, cut up any old or cancelled credit cards or debit cards.
- Only give out your Social Security number when it's absolutely necessary. Often when someone asks for it, you are not required to give it to them.
- Protect information like your mother's maiden name, which is often used as a way to verify identity with financial institutions. Be cautious of where this might appear online, so don't put it on your social media account.

PRACTICE ONLINE SECURITY

There are many things you can do to safeguard your personal information online.

- **Commit all passwords to memory**. Never write them down (not even on a post-it by your computer!) or carry them with you.

    - Make sure passwords are long and include upper- and lower-case letters and numbers. Don't include any words that can be found in a dictionary or names and dates that can be associated with you (your children's names or birthdates, for example).
    - The best practice is to have a different password for each account. If you find it too hard to keep track of so many different passwords, have separate, longer, harder-to guess passwords for your financial accounts.

- Don't give out your financial or personal information over the Internet, unless you have initiated the contact or know for certain with whom you are dealing.

- Never share identity information online unless the site is secure with an encryption program, so no one can intercept your information. **If secure, the website address will start with https, not http**. There will also be a lock symbol near the web address (🔒). A secure website is not necessarily a legitimate one. Don't let your guard down just because you see the "https" and lock symbol.

- Don’t use public WiFi when sending financial or personal information. And if you’re using a public computer, like at your local library, never give the browser permission to save your password, always log off any website you signed into, and close the browser before you leave the computer.

- Passcode protect your phone and tablet. Many people use apps on their mobile devices that save their passwords and log them in automatically, giving thieves easier access to personal information. Using a passcode helps ensure that someone else can’t get into sensitive information stored on your device.

- Don't reply to emails asking for personal banking information, even if they have a company logo! **Financial institutions will never ask for personal information via email**.