



Protect yourself from fraud

Identity theft is the use of someone else's personal information for financial gain without that person's knowledge or permission. Identity theft can be detrimental as it could lead to financial ruin.

Protect yourself from fraud



Identity Theft 101:

Fraudsters only need one of these three pieces of critical information to execute the crime:

- Social Security Number (SSN)
- One-time passcodes or login credentials
- Driver's license

Often, these fraudsters will try to access your information through **phishing**, the use of deception to dupe individuals into sharing their personal information over the internet.

How scammers operate:

Often, online attacks target people by getting them to share personal information through:

- Impersonating a reputable entity (e.g. financial institution, credit card company, etc.)
- Programming ransomware (viruses, data usurpers) into links and downloadable attachments
- Creating a sense of urgency/fear, using social engineering to exploit emotions or prompting quick action to lower your defenses and get information

Don't take the bait! 3 steps to avoid being phished:

1. Stay aware

- > Monitor and review your transactions
- > Review your credit reports regularly
- > Be mindful of requests to debit your account
- > Enroll in a credit file monitoring program

2. Be skeptical

- > Review emails and texts cautiously
- > Check for spelling errors, unusual URLs, and generic greetings (e.g. Dear Customer)
- > Make a call to the company phone number if you are unsure
- > Do not trust unsecured networks- use a VPN and only connect to public Wi-Fi in an emergency.

3. Safeguard your information

- > Utilize password best practices-use a mix of case types, symbols, numbers, and letters. Don't use the same password for each website, and make sure to change passwords every 30-60 days.
- > Do NOT give out passwords, PINs, or even one-time passcodes you receive over text message over the phone
- > Store your card information in a digital wallet on your smartphone
- > Store personal documents in a safe and shred sensitive documents you no longer need

Protect yourself from fraud



What to do if your identity has been stolen:

1. If you think you might have received a fraudulent request and have provided information, please contact GTE Financial Member Services IMMEDIATELY at: 813.871.2690 or toll-free at 1.888.871.2690
2. If you have received a questionable email or have visited a website you believe may be phony, or know you've been a victim of a scam, please report it immediately to GTE Financial at CyberCrime@gtefinancial.org
3. Report identity theft to the U.S. Federal Trade Commission (FTC) at ftc.gov/idtheft or by calling 877.438.4338
4. You can report scams, fraud, and suspicious activity to the FTC at ftccomplaintassistant.gov or 877.382.4357
5. If you believe you're a victim of identity theft, you should contact all 3 major credit bureaus

Built-in protection with GTE products:

Stay one step ahead of identity theft with sophisticated security. We offer a wide range of products and services that work overtime to keep your finances safe, including:

- > Go Premium with GTE Secure™
- > GTE Mastercard® with Total Identity Monitoring
- > The GTE Mobile App, which offers control over your personal banking
- > Security and balance alerts in online banking

Visit gtefinancial.org/fraud to learn more!

Federally Insured by NCUA.