Centier BANK

Protect Your Information

TOP 5 TIPS

1 Identity Theft

Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain. According to the US Postal Inspector, identity theft is America's fastest growing crime. Unfortunately, identity theft can happen to anyone and can lead to financial loss, negatively impact credit scores, and cause emotional distress for its victims. The best and most effective way to protect yourself from identity theft is to educate yourself on how to recognize and prevent it.

Signs of Identity Theft:

- Unexplained withdrawals or charges on credit card statements or bank accounts
- Missing bills or statements from your mailbox
- Receiving bills for services you didn't use
- Debt collectors call you about debts that are not yours
- Unfamiliar accounts on your credit report
- Website login username or passwords that suddenly do not work
- Inability to file a tax return because of duplicate filing

2 Cyber Attacks

Cybercriminals use many techniques in an attempt to manipulate your emotions to access your personal information. They will impersonate financial institutions and other government agencies, and use fear, flattery, guilt and other methods to trigger and coax you into providing information that could compromise your security.

Phishing: A tactic in which scammers pose as a trusted entity, typically via email and/or text, sending a message that includes links that make it possible for your device to be accessed or hacked.

Spoofing: A tactic in which scammers disguise their phone number or email address to appear as though the communication is coming from a local number or trusted entity.

3 Scams & Fraud

A **scam** is an intentional attempt to deceive or mislead you with the goal of personal gain, usually monetary.

As identity theft scams grow more widespread and elaborate, it is important for consumers to stay informed on the latest scams and fraudulent tactics being used by criminals.

Take a look at some of the common scams being used today:

Bank Impersonation Scams

If someone claiming to be your bank calls you asking for account information, hang up and call the number provided on the back of your Debit Card or visit a branch for assistance.

Package Delivery Scams

Do not click on links sent to you via email or text to check the status of your package deliveries. Log in via the store or account website in a new browser window to check safely.

Government/ IRS Scams

The government will not call to threaten you or ask for money.

Person to Person Payment (P2P) Scams

Only use P2P services to send money to people you know. Many of these transactions are irreversible and not meant for commercial use.

Sweetheart Scams

Never transfer money from your bank account, buy gift cards, or wire money to an online love interest.

Fake Check Scams

Do not accept payment in the form of check or cash checks from people you don't know.

Gift Card Scams

No legitimate business or government entity will call or text you requesting payment in gift cards.

Prize Scams

Never pay money to claim a prize. Don't click on links in texts that claim you have a reward or prize.

4 Best Practices

Protect Your Private Information:

- Keep your social security number, Medicare and other account information in a safe place.
- Never give out private information via email, text, or incoming calls.
- Only discuss sensitive information when you place the call to a trusted number.

Don't Take the Bait:

- Do not open or respond to text messages from unknown numbers.
- Don't click on links in emails or texts unless you are certain you know what it is.
- Do not respond to any request to verify your information (account numbers, SSN's, passwords).

Tighten up Your Password Practices:

- Don't store passwords in or near your device.
- Change your passwords often.
- Don't use family members, dates of birth, pets, etc. as passwords.
- Keep passwords strong, using at least 8 characters, including a mix of lower and uppercase letters, numbers and symbols.

Avoid Oversharing on Social Networks:

- Limit your exposure online by not including your home address, date of birth, or other personally identifying facts.
- Review and utilize your privacy settings often.
- Don't accept requests from suspicious or unknown accounts.

Guard Your Gadgets:

- Use firewall, virus, and spyware protection software for computer, tablets and smart phones.
- Do not download anything that is not from a trusted source.
- Do not access banking or other sensitive information sites while using public Wi-Fi.

5 Resources

- **Federal Trade Commission** - reporting the incident
- **Indiana Attorney General's Office** - freezing credit reports
- **Postal Inspector** - leaders in the fight against identity theft
- **Police Department** - documenting and reporting
- **Attorneys** - legal help
- **Local Banks** - protecting your financial accounts

If you believe you have been a victim of Identity Theft, below are some important contact numbers:

Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

Please remember to contact all your financial institutions, credit card issuers, creditors, and local law enforcement. Keep records of all correspondence.

For more information, contact or visit us today. We're here to answer your questions and provide help.