

How do you protect yourself from Identity Theft?

Identity Theft



With regard to banking, read on to cut the line on Phishing, learn how protect yourself from identity theft, and what to do if you become a victim of either.

How to Protect Yourself

Use the tips below as guidelines for keeping your banking activity safe:

Online Banking Safety

Don't leave your computer unattended after you've signed in to online banking. Always exit your online banking session when you've completed your transactions. Keep your online banking password private. Never give your online banking password to others or allow others to access your online banking records. If you access your account information from any computer other than your own (such as your computer at work) be sure the system is private (not shared).

Telephone Banking Safety

Bank employees will never ask you to tell them your secret code or online banking password over the telephone. If someone calls you claiming to be a bank representative and asks for your secret code, don't give it out. Ask them for identification and call your bank immediately to report the incident.

Check Card Safety

Review your monthly statement or your account activity online to confirm all transactions are yours. Report any errors or unknown charges immediately. After you've handed your card to a merchant for a purchase, make sure that the card is actually yours when it's given back (and not the card of someone else). Keep your charge slip and destroy any carbons. If you lose your card, report it to your bank immediately.

What is "phishing"?

The term "phishing" comes from the way in which internet scammers "phish" for your personal financial information. This involves sending fraudulent emails that appear to be from a legitimate company that you recognize and do business with, such as a financial institution, credit union, or credit card company, in order to trick you into surrendering private information that can be used to initiate fraudulent transactions or complete an identity theft. In many cases, the fraudulent email will warn you of a serious problem with your account that needs immediate attention, and will threaten to suspend or close your account if your personal information is not updated within a given time frame. The email then directs you to click on a link to a phony website where you are asked to update personal information, such as your Social Security number, passwords, credit card information, bank account

numbers and contact information. Any email you receive that appears to be from your bank and requests updated personal information, such as your Social Security number, account number, secret codes, or passwords, is fraudulent. The link contained in the email is NOT to your Bank's website, even though it may imitate your bank's style and graphics.

If you have already replied to a phishing email and given out personal account information. Besides your bank, who else should you contact if you think you have been a victim of phishing?

Equifax
800-525-6285
P.O. Box 740250
Atlanta, GA 30374
Experian
888-397-3742
P.O. Box 1017
Allen, TX 75013
TransUnion
800-680-7289
P.O. Box 6790
Fullerton, CA 92634

Dumpster Diving

They rummage through trash looking for bills or other paper with your personal information on it.

Skimming

They steal credit/debit card numbers by using a special storage device when processing your card.

Phishing

They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

Changing Your Address

They divert your billing statements to another location by completing a change of address form.

Old-Fashioned Stealing

They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.

Pretexting

They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.