ACCOUNT HIJACKING

Protect your account from **unauthorized access.**

Account hijacking is the fastest growing form of identity theft, and the effects can be devastating. Be vigilant and protect your accounts from unauthorized access.

Account hijacking is a process through which an individual's email account, computer account, or any other account associated with a computing device or service is stolen or hijacked by a hacker. The hacker then uses the stolen account information to carry out malicious or unauthorized activity, which can sometimes take weeks or months to discover.

The Federal Deposit Insurance Corporation (FDIC), a government entity charged with insuring financial institution deposits, defines account hijacking as any unauthorized access to and misuse of asset accounts through phishing and hacking.

"Phishing" involves theft of personal financial information from individuals through deception on the Internet. "Smishing" is a similar phish for personal financial information that is completed by sending a single message over a cell phone in the form of text or voice mail. "Hacking" is unauthorized use of a computer or computer networks aided by spyware, which is illegal software that collects personal information.

Victimizing millions of Americans over the last decade, account hijacking methods are getting increasingly sophisticated, requiring financial institutions and account holders to take more precautions to protect their financial data.

You can detect potential account hijacking sooner by frequently monitoring your financial institution and debit card accounts online rather than waiting for your paper statement to arrive in the mail.

About 30% of a group of 294 survey respondents reported having had at least one email or social networking account accessed by an unauthorized party, according to a study conducted by researchers from Carnegie Mellon University and Google.*

* Source: "Google Study Finds Widespread Account Hijacking", Thomas Claburn, InformationWeek, Feb., 2014

Take Measures To Protect The Security Of Your Accounts

You can fortify your system and protect yourself from account hijacking:

- Choose your passwords carefully and change them often. Passwords should be changed at least every 90 days, if not more frequently. Don't use a password that could be easily guessed, such as your children's names, your home address or phone number.
- Install firewall and anti-spyware software on your computer. A firewall is software designed to help prevent unauthorized access to your computer. Anti-spyware software prevents destructive programs from stealing sensitive information.
- Always install the latest updates or "patches" to stay one step ahead of hackers.
- Don't respond to phishing emails. Delete suspicious emails that request personal or financial information. Internet fraudsters can make emails look legitimate by stealing logos and other graphics from businesses you know and trust.
- Stay on top of your accounts. Keep track of your balance and account activity on a regular basis. Studies show that individuals who monitor their accounts online discover many problems sooner.

Stay watchful and review your credit report annually

You are entitled to one free credit report from each of the three credit reporting agencies each year. If a hijacker is misusing your credit, clues are likely to show up here. These reporting agencies are:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
800.685.1111	888.397.3742	800.888.4213

SHERWOOD STATE BANK
SSB A COMMUNITY BANK
FDIC