ACCOUNT HIJACKING & IDENTITY THEFT

- How to recognize it
- How to prevent it

Guarding Against Account Hijacking

It is the fastest growing form of identity theft, and it can have the most devastating effect on us. It is called ***Account Hijacking,*** and some 2 million people are victimized yearly.

Account hijacking occurs when a criminal obtains your personal banking information and uses it to take over your bank accounts. It can take weeks or months to discover. Fortunately, there are steps you can take to protect yourself.

STEP 1 PROTECTING YOURSELF UNDERSTAND THE THREAT

Often, the account hijacker uses one or more methods to obtain your personal data. You should be particularly aware of two:

- **Hijacking by Phishing** deceives customers into providing their user names, passwords, and account numbers via deceptive e-mails, fake Web sites, or both. The classic phishing attack involves a deceptive e-mail that purports to be from a legitimate financial institution. The e-mail typically tells the customer that there is some sort of problem with the customer's account, and instructs the recipient to click on the included hyperlink to "fix" the problem. In reality, the fake Web site is simply collecting customer user names and passwords in order to hijack accounts.
- **Hijacking with Spyware** works by inserting malicious software, often referred to as "spyware," on a person's personal computer. Spyware can be loaded when a user opens a seemingly innocuous e-mail attachment or clicks on a pop-up advertisement. The spyware collects selected information (e.g., user names, passwords, and

account numbers) and forwards that information to the fraudster.

STEP 2 PROTECTING YOURSELF
FORTIFY YOUR SYSTEM

Here are some basic safety measures you can implement immediately:

- **Password Protection—**If your password is easy for you to remember, the chances are good it is also easy for an Internet hacker to figure out. Experts advise a combination of letters and numbers…and avoiding pet names, your home address, and similar easy-to-crack codes.
- **Anti-Virus Software—**Your computer's anti-virus software is like a vaccine—it works at first, but you need to keep it up-to-date to guard against new strains.
- **Anti-Spyware—**Anti-spyware programs are readily available, and every computer connected to the Internet should have the software installed… and updated regularly.
- **"Phishing Awareness"—**If you receive an unexpected email, or one that you consider suspicious, delete it. Remember: your bank will never email you and ask you to go to another site to "verify information."

QUICK FACTS ABOUT ACCOUNT HIJACKING

- An estimated 2 million people are hit with account hijacking each year; most say it was from a phishing email.
- Overall account fraud totals more than $2.4 billion annually, $1,200 per victim.
- People who monitor their accounts online (rather than just with mailed statements) can detect hijacking earlier. In one report, victims' losses were one-eighth of those who detected the crime via paper statements due to early detection.

STEP 3

PROTECTING YOURSELF
VIGILANCE PAYS

Chances are you will never be victimized by account hijacking identity theft. But if you are victimized, early detection is critical.

- **Check your statements regularly.** If something seems irregular, contact your banker to discuss it. A recent study showed that customers who *monitor their accounts online* discover problems sooner.
- **Check your credit report at least annually.** You are entitled to one free credit report annually from each of the three major credit bureaus. If a hijacker is misusing your credit, clues are likely to show up here. For a free report: **www.annualcreditreport.com.**

Your bank is taking substantive measures to protect the safety and security of your accounts. By acting today to strengthen security at your end of the Internet highway, hijackers will have an even tougher time. Stop by your bank to learn more.

UNITY
National Bank

www.unitybanktexas.com

713.387.7400

© FINANCIAL EDUCATION CORPORATION