

FRAUD ALERT!

ACCOUNT HIJACKING & IDENTITY THEFT

- *Your credit union wants you to know how to recognize and prevent this most prevalent of all identity theft crimes.*

Guarding Against Account Hijacking

Account hijacking is the fastest growing form of identity theft, with millions victimized every year.

Account hijacking occurs when a criminal obtains your personal financial information and uses it to take over your accounts. It can take weeks or months to discover.

Fortunately, there are steps you can take to protect yourself.

Understanding the Threat

Often, the account hijacker uses one or more methods to obtain your personal data. You should be particularly aware of two of them, **phishing** and **spyware**.

HIJACKING BY PHISHING deceives people into providing their user names, passwords, and account numbers via deceptive e-mails, fake (spoofed) 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 you that there is some sort of problem with your account, and instructs you to click on the included hyperlink to “fix” the

problem. In reality, the spoofed Web site is simply collecting user names and passwords in order to hijack your account.

HIJACKING WITH SPYWARE works by inserting malicious software, often referred to as “malware” or “spyware,” on a person’s computer. Spyware can be loaded when you open a seemingly innocuous e-mail attachment or click 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.

Fortifying Your System

When it comes to account hijacking, an ounce of prevention is worth a pound of cure! Here are some basic safety tips you can implement immediately:

- ✔ **Password**— Experts advise a combination of letters and numbers...and avoiding pet names, your home address and similar easy-to-crack codes.
- ✔ **Virus Protection**—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.

- ✔ **Firewalls**—This protective wall between the outside world and your computer can help prevent unauthorized access to your computer. Updates are called patches, and you should check regularly with your software company to be sure you have the latest patches.
- ✔ **Spyware**—Anti-spyware programs are readily available, and every computer connected to the Internet should have the software installed...and updated regularly.

Safe Online Transactions

Technology, accountability and ongoing communication help your credit union insure that your online experience is safe and secure.



We NEVER send emails requesting personal information.

Your credit union will never ask you to “verify” information through an email...never ask you to click on a special site to do so. If you receive something like this that appears to be from your credit union, do not answer it. It is likely a ***phishing scam***. Delete it. Then call your credit union to inform them.

Maintaining Your Vigilance

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 credit union to discuss it. *An encouraging note: a recent study showed that people 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 credit union is taking substantive measures to protect the safety and security of your accounts against account hijacking and other forms of identity theft. By acting today to strengthen security at your end of the Internet highway, hijackers will have an even tougher time. Stop by your credit union soon to learn more!

