Identity THEFT

KIT cares about your safety. Now that you can access your KIT account online, you need to be especially aware of how to protect yourself from cyber-thieves! Visit KIT online at www.kitfcu.org

KIT is your full service financial institution. Call today for more information regarding any of our services. 1-888-459-9286

Identity Theft Member Information

KIT FEDERAL CREDIT UNION

Fact...
Identity thieves raid mailboxes for credit card offers and statements. Always remove your mail from your mailbox in a timely manner. Never use your mailbox for outgoing mail.

Don't Become the next victim...

Keep Your Online Transactions Safe

*Avoid sending sensitive information, such as your account number, through UNSECURED e-mail.
*Passwords or PIN numbers should be used when accessing an account online.
*General security over your personal computer such as virus protection and physical access controls should be used and updated periodically.
*Read mail only from senders that you know and trust.
*Do not open suspicious attachments.
(If it's a friend, verify it first).

How To Guard Against Identity Theft

*Guard you social security number. Do not give out your PIN or credit card numbers over the phone unless you initiated the transaction.
*Be very careful with receipts. Make sure you have them when you leave the store or ATM and do not throw them into public trash cans.
*Destroy pre-approved credit card offers before you throw them out. A home shredder is the best thing to use on financial statements, receipts and old cancelled checks that you are discarding.
*Account for all new checks for your checkbook when you receive them in the mail.
*Block your ATM transaction with your body to prevent someone from learning your PIN.
*Commit all passwords and PIN numbers to memory so no one can see them in writing.
*Be creative when you select a password. Don't be obvious like using the last four digits of your social security number, phone number, address, birth date or any format that could easily be decoded by thieves.
*Remove mail promptly from your mailbox. Never use your mailbox for outgoing mail. Identity thieves raid mailboxes for credit card offers and financial statements.
*Protect your identification and credit cards from pickpockets. Close your wallet and keep your purse shut and close to your body.
*Limit the number of I.D. and credit cards that you carry. If they are stolen, you'll have fewer to replace.
*If your social security number is used as your driver's license number or appears on another I.D. card, ask the issuer for a new card with a different account number. If your social security number is printed on your checks, reorder checks without it. Also, if your driver's license number is printed on your checks, consider removing it.
*Keep your birth certificate and social security card in a safe deposit box. Carry these items with your only on the days that you need them.
*Review your credit report each year. If someone is applying for credit in your name and you haven't noticed any warning signs, a copy of your credit report may help point this out. You can obtain a free credit report once a year from easy of the credit report agencies—Experian, Equifax and Trans Union. Online at **www. AnnualCreditReport.com or toll free at 877-322-8228**

What To Do If You Are A Victim

1 Contact your credit card company and your financial institution and close your accounts. The FBI suggests that you put passwords (not your mother's maiden name) on any new accounts you open.

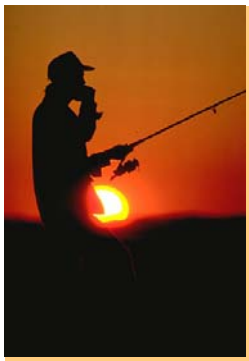
2. Call the three major credit bureaus (numbers shown below) to tell them your identity has been stolen. Request that a "fraud alert) be placed on your file and that no new credit be granted without your approval.

EQUIFAX: 800-525-6285
EXPERIAN: 888-397-3742
TRANS UNION: 800-680-7289

3. Call the Social Security Fraud Hotline: 800-269-0271.

4. Contact the Federal Trade Commission (FTC) theft hotline: 877-438-4338 www.consumer.gov/idtheft

5. You should not only file a report with the police, but also get a copy of the report in case you need proof of the crime later for credit card companies, etc.



Phishing Scams

What Is Phishing?

Phishing attacks are 'spoofed' e-mails and fraudulent web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, social security numbers, etc. By hijacking the trusted brands of well-known financial institutions, online retailers and credit card companies, phishers are able to convince up to 4% of recipients to respond to them.

How to Avoid Phishing Scams

*Be suspicious of any e-mail with urgent requests for personal financial information. KIT will NEVER send you an email asking for your account number, password, or other sensitive information. If you receive such an email that appears to be from KIT, phone us IMMEDIATELY!

*Don't use the links in an email to get to any web page, if you suspect the message might not be authentic.

*Always ensure that you are using a secure website when submitting credit card or other sensitive information via your web browser.

*Regularly log into your online accounts and check your financial institution credit and debit card statements to make sure that all transactions are legitimate.

*Make sure that your browser is up to date and security patches applied.

*Always report "phishing" or "spoofed" emails by forwarding the email to the following groups:

The anti-phishing network at:
www.antiphishing.com
The Federal Trade Commission at:
www.consumer.gov/idtheft
*The Internet Fraud Complaint Center of the FBI by filing a complaint on their website**:**
www.ifccfbi.gov

WARNING

Spyware is software installed on a computer without the user's knowledge, often through a virus or when a user downloads a free program.

It is designed to let a hacker eavesdrop, collect personal or confidential information and perhaps track and record a user's activities. Some spyware can obtain such information as passwords or credit card numbers. It also often bombards computer users with unwanted ads.

AVOID THE RISK of banking online n public computers like those in hotels, libraries or internet cafes where spyware might have been installed.

How To Get Your

FREE CREDIT REPORT

THE FACT ACT: Fair and Accurate Credit Transactions Act, passed by Congress, allows all individuals the right to check their credit report once every year.

You can obtain a free credit report once a year from each of the credit report agencies—Experian, Equifax and Trans Union.

ONLINE AT
www.AnnualCreditReport.com
TOLL FREE AT
877-655-8228

Pharm-ing

Is a Twist of Phishing

Security experts are now concerned about a new internet-related fraud known as "Pharming". Pharming attempts to fool online users through a virus that alters the behavior of internet browsers, this, redirecting users to a fictitious site when they attempt to log on to their financial institution's web site.

This can be done by changing—or "poisoning" - some of the address information that internet service providers (ISPs) store to increase the speed of web browsing. Some ISPs and companies have a software bug on their computer servers that permits fraudsters to hack in and change those addresses.

Fast Fact…

IDENTITY THEFT: Average ID theft victims spend 607 hours resolving their case with $1,495 in out-of-pocket expenses.

Source: Federal Trade Commission—Identity Theft Resource Center