ATM Security ALERT

Beware of ATM “Skimmers”

Alert Summary

Bayou Federal Credit Union is aware of reports of ATM tampering, aimed at capturing your card number and PIN. Thieves have been known to affix “skimmer” devices and/or cameras to ATMs to illegally capture your card information.

The typical ATM skimmer is a device smaller than a deck of cards that fits over the existing card reader. Most of the time, the attackers will also place a hidden camera somewhere in the vicinity with a view of the number pad in order to record personal-identification-numbers. Some criminals may install a fake PIN pad over the actual keyboard to capture the PIN directly, bypassing the need for a camera.

Acton Required

You should always be vigilant when using ATMs. Pick a location that is well-lit, and avoid using an ATM if suspicious people are hanging around. As for avoiding ATM “skimmers”, here are some tips:

- **Check for Tampering**
  When you approach an ATM, check for some obvious signs of tampering at the top of the ATM, near the speakers, the side of the screen, the card reader itself, and the keyboard. If something looks different, such as a different color or material, graphics that aren't aligned correctly, or anything else that doesn't look right, don't use that ATM.

- **Wiggle Everything**
  Even if you can't see any visual differences, push and pull at everything

- **Protect the PIN**
  Even if you don't notice a skimmer and swipe your card, covering your hand when you enter your PIN can block a camera that may have been installed. If the keyboard doesn't feel right—too thick, perhaps—then there may be a PIN-snatching overlay, so don't use it.

- **Location**
  Criminals frequently install skimmers on ATMs that aren't located in overly busy locations since they don't want to be observed installing malicious hardware or collecting the harvested data. Stop and consider the safety of the ATM before you use it.

As always, monitor your financial accounts closely and report any discrepancies. Find more helpful information on identity theft and cybersecurity at www.ftc.gov.

Bayou Federal Credit Union 2-4-2016

Data Security: How Your Credit Union is Looking Out for You

NAFCU
National Association of Federal Credit Unions

As data breaches at merchants continue to permeate the news, we want you to know that Bayou Federal Credit Union is ready to help if your personal or financial data is ever compromised.

We take service to our members seriously and will do everything we can to ensure that action is taken – quickly – to help you avoid becoming a victim of identity or account theft. Your credit union is subject to strong data security standards established by Congress and federal regulators. While data breaches can happen anywhere, we are ready with a plan designed to ensure the safety and confidentiality of your sensitive data.

Unfortunately, merchants and retailers aren't subject to these federal requirements. Many of them follow their own data security standards, but, as the crush of data breaches over the last couple of years has shown, these self-imposed merchant standards are no substitute for a stronger federal standard.

When it comes to protecting your personal information, every measure counts. When your debit or credit card data is breached at a merchant, the cost of card replacement or account reimbursement to you is typically paid by your credit union and not the retailer where the breach occurred. Unfortunately, this can become a very expensive proposition for the credit union, as we are often never reimbursed for these costs by merchants—as there is no liability requirement on them to pay for data breaches that occur on their watch.

We want you to know that in the event of any breach affecting your accounts, this credit union will always do what we can to make you whole. In the meantime, credit unions around the country are leading the effort to get Congress to pass legislation ensuring merchants and retailers meet a national standard for protecting any of your financial data they collect when you make a purchase and are held liable for breaches that occur on their end. We hope you will support us in this effort.

While we can't control what happens at merchants and retailers, we want you to know that Bayou Federal will do everything we can to assist you and your family if a breach does occur when you use your debit or credit card. You can always feel free to reach our member service department at (225) 925-8800 or (800) 349-2900.

Sincerely,

Carrie R Hunt

Carrie Hunt
Senior Vice President of Government Affairs and General Counsel
National Association of Federal Credit Unions
3138 10th Street North
Arlington, Virginia 22201
800-336-4644 • 703-842-2234
fax: 703-522-0594
www.nafcu.org

Data Breach ALERT

9-5-2014
Home Depot Stores
reportedly experience credit and
debit card data breach

Alert Summary

Bayou Federal Credit Union is aware of recent reports of a Home Depot credit and debit card breach. The company has not confirned details of a breach, but says it is investigating a breach at this time. Some reports are claiming the data breach may involve all of the more than 2200 Home Depot stores nationwide.

Acton Required

There is no need to take any action regarding your Bayou Federal credit card or debit card at this time. You may continue to use your cards.

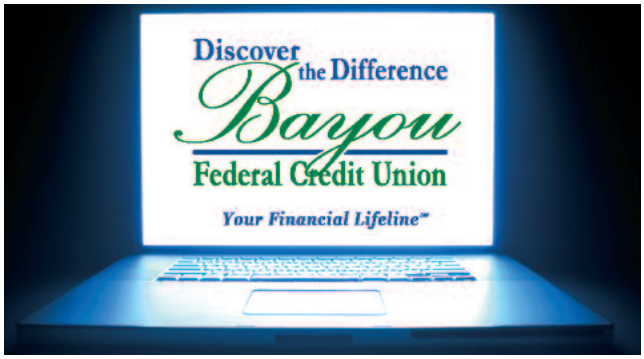
If your card is identified as part of this breach or any other one, we will contact you regarding the replacement of your card.

Bayou Federal takes any threat to the security of your personal or financial information very seriously. We will continue to be vigilant on this matter and will post more information if needed.

As always, monitor your financial accounts closely and report any discrepancies. Find more helpful information on identity theft and cybersecurity at www.ftc.gov.

Online Banking Security

Important Information For Members of Bayou Federal Credit Union



Cyber-fraudsters want to steal your money!

Bayou Federal has substantive safeguards in place to help protect you, but we need your help to be most effective.

1. Understand the threats. Here are a few of the most common:

PHISHING - This is an attempt to steal your personal information through fraudulent e-mails or smart-phone texts. Often very believable, their messages lure you to a site that asks you to "verify" personal financial details, such as account numbers, social security numbers, and even PIN numbers. Remember, Bayou Federal will NEVER e-mail or text you requests for personal financial information...we already have it, and we keep it safe and secure for you.

Spyware - This is the term for software that you may unknowingly download onto your personal computer, phone, or tablet. Once there, the spyware tries to collect personal information and send it back to the criminal. Your best defense against spyware is up-to-date security software that you purchase from a reputable seller.

Card Skimming - Some criminals try to collect personal information by placing a device on an ATM, called a skimmer. These devices are usually affixed right to the front of the ATM, and can capture your card information and PIN when you try to use the machine. Using ATMs you know and trust, as well as examining the machine closely, can help you stay safe from these illegal devices. If something on or around the ATM doesn't look right or normal, avoid the machine and use another.

Bayou Federal invests substantially in security measures to help protect your personal financial information. But many account hijacking attempts come as a result of hacking into personal computers or devices, then using information found there to access financial information. Here are some precautions you can take:

1. **Strong passwords -** experts advise a combination of letters and numbers, but not something easily guessed like birthdays or home addresses.
2. **Anti-Virus Protection -** Make sure the anti-virus software on your computer, phone, or tablet is up-to-date, and it scans e-mails as they are received.
3. **E-Mail Safety -** E-mail is usually not encrypted, so be wary of sending account numbers or other sensitive information in this way.
4. **Sign Off and Log Out -** Always log off from our Virtual Branch secure online banking area once you're done, and the same goes for other sites in which you may input personal information.

PERSONAL SECURITY TIPS:

- **Be wary of messages from an unknown sender**
- **Don't open unsolicited emails or text messages**
- **Don't open any links from unsolicited emails or texts**
- **If you have responded to a phishing scam and provided any requested financial information, contact Bayou Federal immediately and;**

1. **Report the incident to the 3 major credit bureaus**
2. **Order a credit report**
3. **Report the incident to the Federal Trade Commission**
4. **File a complaint with the Internet Crime Complaint Center at www.ic3.gov**

As always, monitor your financial accounts closely and report any discrepancies. Find more helpful information on identity theft and fraud at **www.ftc.gov.**

Bayou Federal Credit Union:
(225) 925-8800 • (800) 349-2900
www.bayoufcu.org • cuinfo@bayoufcu.org

Online Security ALERT

Major Security Flaw Found in Internet Explorer

Millions of PCs Could Be Exposed to Attacks

Alert Summary

According to the Department of Homeland Security, a major security flaw has been found in Microsoft's Internet Explorer that can allow hackers to hijack online sessions. This is a browser-based vulnerability and does not affect the operating system.

The United States Computer Emergency Readiness Team (US-CERT) advises to stop using Internet Explorer, versions 6 through 11, if users are unable to apply workarounds published by Microsoft. DHS urges users and administrators to "consider employing an alternative Web browser until an official update is available."

Alert Details

The exploit was first identified by security firm FireEye, which outlined the vulnerability in an April 26 blog post. The company says the exploit is significant because the vulnerable browsers "represent about a quarter of the total browser market." US-CERT, in an April 28 statement, says the vulnerability "could lead to the complete compromise of an affected system." CERT says it's unaware of a practical solution to this problem. But it recommends the use of the Microsoft Enhanced Mitigation Experience Toolkit to help prevent exploitation of this vulnerability.

Microsoft encourages you to take steps that protect your PC such as enabling a firewall, applying all software updates, and installing antivirus and antispyware software. They also have some tips and actions you can take to help protect against this specific vulnerability. To lean more, visit microsoft.com/security.

As always, monitor your financial accounts closely and report any discrepancies.
Find more helpful information on identity theft and fraud at www.ftc.gov.

Bayou Federal Credit Union 4-30-2014

Online Security ALERT

April, 2014

BAYOU FEDERAL'S COMPUTER SYSTEMS AND ONLINE SERVICES REMAIN SECURE:

"Heartbleed" Bug Not an Issue Here

Alert Summary

The Heartbleed bug--a flaw in the Open Secure Socket Layer (OpenSSL) technology used to establish secure links between servers and users--may have exposed millions of usernames, passwords and other information. Undetected for more than two years, the bug affects two-thirds of encrypted websites.

Bayou Federal Credit Union has taken appropriate measures to secure our site and online functions. We urge all members to remain vigilant by watching their accounts for any unusual or unauthorized activity. It's also a good idea to change your passwords frequently, no matter which bugs or viruses are currently identified as threats. In addition, maintaining up-to-date virus protection on your computer can help guard against malware and other threats.

Alert Details

Tech giants Cisco (CSCO, Fortune 500) and Juniper (JNPR) have identified about two dozen networking devices affected by Heartbleed, including servers, routers, switches, phones and video cameras used by small and large businesses everywhere. The companies are also reviewing dozens more devices to determine whether they're impacted by the bug as well. Many other companies could have been affected as well.

That means for two years now, someone could have been able to tap your phone calls and voicemails at work, all your emails and entire sessions at your computer or iPhone. You also could have been compromised if you logged into work from home remotely. And you'll probably never know if you were hacked.

Experts say the best defense right now is to change passwords to any sites with which you communicate personal or financial information. Keeping a close eye on account balances and such is also always a good idea. Most companies, like Bayou Federal, are aware of the threat and have taken steps to patch systems or guard against any vulnerabilities. We will continue to monitor this and all internet security threats and keep our members informed.

As always, monitor your financial accounts closely and report any discrepancies.
Find more helpful information on identity theft and fraud at www.ftc.gov.