



SPECIAL EDITION: Fraud Protection

Leader

First Quarter 2010

Phishing, Vishing, Smishing - what does it all mean?

Fraudulent acts can be committed through many methods, including mail, phone and internet. How can you protect yourself from becoming a victim of identity theft? Let's discuss the three most popular forms of "electronic" fraud—phishing, vishing and smishing.

What is Phishing?

The number of phishing scams is rising at a shocking rate: so much so, that phishing now represents the largest form of online identity theft. Websites frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online.

A phishing attempt is usually in the form of an email that appears to be from your financial institution or credit card provider. The email encourages you to click an embedded link that takes you to a fake login page designed to capture your details. It is an attempt by fraudsters to 'fish' for your personal and financial details.

Scam artists send fake emails claiming that your information has been compromised, due to your account being deactivated or suspended. They will then ask you to confirm the authenticity of your information like a credit card number, personal identification number (PIN), passwords or other personal information, such as mother's maiden name. While some emails are easy to identify as fake, others may appear to be from a legitimate source.

Fake emails often direct you to counterfeit web sites carefully designed to look real. These websites may look familiar to you, but are in fact used to collect personal information for possible illegal use. These emails attempt to convey a sense of urgency such as 'Your account will be closed or temporarily suspended if you don't respond,' or, 'You'll be charged a fee if you don't respond.'

Ok, that was phishing. But what in the world is vishing?

Vishing uses Voice over Internet Protocol (VoIP) technology where a scam artist poses as a "real" company, such as your financial institution, and attempts to trick members into providing their personal and financial details over the phone.

A typical vishing attack uses an automatic dialer and a modem to call phone numbers in a particular region. When the phone is answered, an automated recording alerts the consumer that their credit card has had illegal activity and that they should call the recorded phone number immediately. When the member calls the number, it is answered by a computer-generated voice that tells them they have reached 'account verification' and instructs them to enter their 16-digit credit card number. Once a member enters their credit card number, the 'visher' has all of the information necessary to place fraudulent charges on their card. Those responding are also asked for the security number found on the back of the card. The call can then be used to obtain additional details such as PIN number, expiration date, date of birth, account number, etc.

We've covered phishing and vishing. So what is smishing?

Smishing or SMiShing is a scam where the user is tricked into downloading a Trojan horse, virus or other malware onto their cell phone or mobile device. SMiShing is short for "SMS phishing." SMS is also popularly known as texting. *(continued on page 2)*

From the President



Jean M. Yokum
President/CEO

The number of high tech financial scams has increased dramatically over the past few years. Criminals are finding new and unique ways of tricking consumers into

divulging their personal information.

The security of our members' personal/private information is a top priority at LFCU. Unfortunately, we continue to see a number of members falling

prey to various scams involving the internet, text mail, counterfeit checks, and identity theft. If a person claiming to represent Langley FCU calls, emails or texts you and starts asking you questions about your accounts and account numbers, remember our general rule - we will never contact you and ask for personal information like that.

To better protect you, we have decided to make this edition of The Leader the "Security Issue." We trust you will find the newsletter educational and even keep it as a reference or guide. I also encourage you to visit the Educa-

tion Center on the LFCU website to use our interactive 'Identity Theft Coach'. You'll receive valuable information about further steps you can take to protect your identity.

Although today's frauds and scams are tough to detect, we hope you do everything you can to protect your assets in this New Year. As always, your credit union appreciates your membership and hope 2010 is your best year ever!

Phishing, Vishing, Smishing - what does it all mean? (continued)

An example of a Smishing message: A cell phone user receives a SMS message stating 'We're confirming you've signed up for our service. You will be charged \$2/day unless you cancel your order: www.smishinglink.com.' Fearful of incurring additional rates on their cell phone bill, they visit the link highlighted in the message. Once they arrive at the URL, they are prompted to download a program which is actually a Trojan horse or virus that then allows the device to be controlled by hackers.

How to be safe online:

- Avoid unknown websites and be suspicious of emails from any company asking for personal or financial information.
- Do not click any links inside an email. Instead, go directly to the valid company's site, log on from there or call the company directly.
- If you want to find your online banking site, always type its URL into your browser.
- Ensure that any website site visited is secure when submitting sensitive information such as credit card numbers. One indication is if the URL starts with <https://> rather than <http://>. Another indication is a padlock icon at the bottom of the screen, which when clicked, displays a security certificate.
- Do not open attachments in emails unless you are absolutely sure that is the file you are waiting to receive.
- Keep your PC operating system up to date and update your anti-virus software frequently.
- Use a personal firewall and software to detect and remove spyware.
- Use one of the many available anti-phishing toolbars that can alert you when you encounter a known Phishing Site.
- Don't use the same password for all of your online accounts.
- Don't store online account information and passwords in files held on your computer.



Tips to prevent vishing:

LFCU has some of your personal details. So, always be suspicious of any caller who appears to be ignorant of basic personal details like first and last name, etc. (although it is unsafe to rely on this alone as a sign that the call is legitimate). If you receive such a call, do not give any information. Report any suspicious calls to LFCU immediately.

Do not call and leave any personal or account details on any telephone system that you are directed to by a message or e-mail.



When a telephone number is given, you should first call the phone number on the back of your credit card or on your statement to verify whether the given number actually belongs to the financial institution or credit card company.



Keeping your mobile device safe:

Be sure your device has security software to address viruses and other malware.

Be as vigilant about security for your mobile devices as you are for desktop computers.

Reduce those bothersome solicitation calls

The Federal Trade Commission (FTC) launched the National Do Not Call Registry in June, 2003, to give Americans a choice about getting telemarketing calls at home. According to a recent Harris Interactive poll, 92% of people who reported placing a number on the registry said they are receiving fewer calls.

To register a telephone number on the National Do Not Call Registry, or to file a complaint, consumers should visit www.donotcall.gov or call 1-888-382-1222 (TTY: 1-866-290-4236). If you are registering a phone number online, you will be asked to provide a valid email address to which a confirmation of the registration will be sent. A registration is not complete until the consumer clicks on the link in this email. If you are registering by phone, you must call from the phone number you wish to register.

If you think you put your number on the National Do Not Call Registry, and you're still getting telemarketing sales calls, the Federal Trade Commission recommends that you:

- Check to see that your number is on the registry. You can verify that your number is on the registry two ways: online at www.donotcall.gov (click on "Verify A Registration"), or by calling 1-888-382-1222 (TTY 1-866-290-4236) from the phone number you wish to verify. Follow the prompts.
- Understand that some calls are not covered. Once your number has been on the registry for 31 days, most telemarketing calls will stop. However, you still may get:
 - calls from — or on behalf of — political organizations, charities, and telephone surveyors;
 - calls from companies with whom you have an existing business relationship. A company may call you for 18 months after you make a purchase or three months after you submit an inquiry or application;
 - calls from companies you've given permission to call.
- File a complaint. If your number has been on the registry for at least 31 days, and a telemarketer calls, you can complain to the FTC. Visit www.donotcall.gov or call 1-888-382-1222 (TTY 1-866-290-4236). You'll need to provide the date of the call and the phone number or name of the company that called you.



What is Skimming?

Skimming is a method used by perpetrators to capture your account information from your credit or debit card. Your card is swiped through a special 'skimming device'. The information contained in the magnetic strip on the card is then read and stored on the skimmer or an attached computer.

How do skimmers operate?

At ATM machines, a skimming device is inserted into the ATM card slot. The device scans the card and stores the information. While a member keys in their PIN, the wireless skimming device transfers the data to the fraudsters. This information is then used for online shopping or to make counterfeit credit cards.

Tips to protect yourself from Skimming:

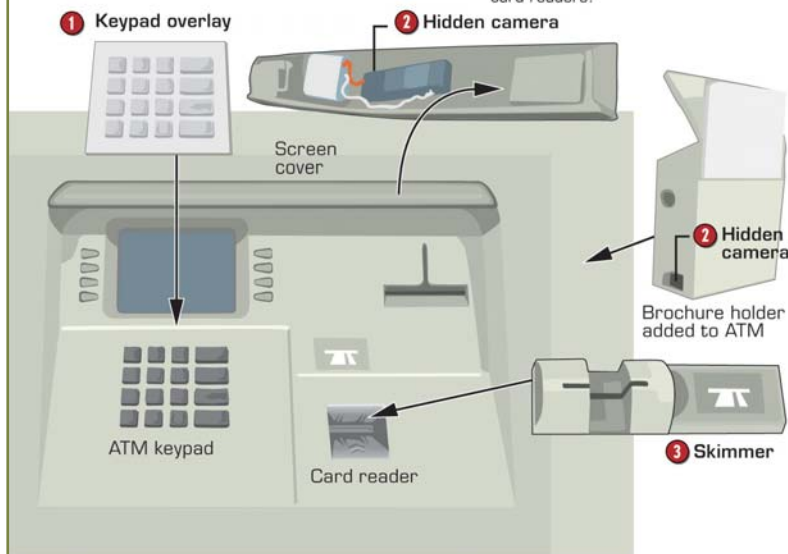
- Sign on the reverse of your new credit card as soon as you receive it.
- Collect your receipts / charge slips at ATMs, restaurants and shopping outlets.
- Check your statement regularly.
- Look for unusual devices connected to the 'swipe' area at ATMs or machines that take credit/debit cards. Telltale signs that an unauthorized swiping device may be attached to an ATM or other card reader include:

- The card reader will most likely have a loose fit, and possibly its size is not proportional to the real façade. It will most likely have a bulky, protruding fit.
- The card reader could have a different coloration than the rest of the machine.

card 'skim' scheme

ATM cardholders have been warned for years about the dangers of card skimmers. The technology is now so compact that many consumers might not notice it. Here are some elements of a typical skim operation.

- 1 Keypad overlays capture PIN numbers on a memory chip.
- 2 Hidden cameras can also copy customers' PIN numbers.
- 3 Skimmers are placed over the card reader to copy the card's magnetic stripe. These are often legal credit card readers.



Reprinted with permission of the Baltimore Sun Media Group. All Rights Reserved.

Fraud Prevention--Don't Be Fooled

- LFCU will never call you and ask for your account number.
- LFCU will never send you an email directing you to a website to 'verify' your personal or account information or any transaction.
- LFCU will never send you a text message directing you to call a phone number to 'verify' your personal or account information or any transaction.
- LFCU staff members will never ask for your password or PIN number to any service.

In the event you have provided credit, debit or ATM card information to a caller or website and you suspect your account information has been compromised, it is important to act quickly. Use the following phone numbers to report this information:

LFCU DEBIT / CREDIT CARDS: Call Cardholder Services toll-free 24-hours a day at (800) 449-7728.

LFCU ATM CARDS: Call the LFCU Contact Center (757) 827-5328 or (800) 588-3279 during business hours or call Cardholder Services toll-free 24-hours a day at (800) 449-7728.

FOREIGN FRAUD: If you are planning to travel abroad, check the LFCU Stop Fraud section of the website for a list of countries where your Langley credit, debit or ATM card usage may be affected.

If someone claiming to represent LFCU contacts you by email or telephone, email our Security Center by visiting our website at www.langleyfcu.org/stopfraud/ and click on the 'email our Security Center' towards the bottom of the page or call the LFCU Contact Center for verification before providing personal information.

How to check your credit report

It's a good idea to obtain a free copy (one per year) of your credit report through one of the three major credit bureaus and check for unauthorized activity. Below are the three major credit bureaus. You can request your report by calling or visiting online:

- Equifax 1-877-322-8228 or www.equifax.com
- Experian 1-888-397-3742 or www.experian.com
- TransUnion 1-800-680-7289 or www.transunion.com

\$50,000 ANNUAL COLLEGE GRANT PROGRAM

Langley Federal Credit Union invites local graduating high school seniors to enter the Education Exchange® 2010 College Grant Program, which will award \$50,000 in college grants to qualified students. Sponsored by ACCEL/Exchange Network, this annual program honors hardworking, academically talented students nationwide.

The Education Exchange® Grant Program is open to all college-bound, high school seniors graduating in 2010. Applicants are judged based on exceptional scholastic achievement, community involvement, qualities of character and leadership, essay responses and financial need. A total of 34 college grants will be awarded nationally – four \$5,000 grants and 30 \$1,000 grants.

To receive an Education Exchange® 2010 application form, which includes complete rules and eligibility requirements, visit any Langley Federal branch location. The entry deadline is March 15, 2010. Grants will be awarded in July 2010.

Protect yourself with Passwords

Creating a unique online password helps ensure your account security. Here are a few tips to make the process easier:

- Longer passwords are more secure than shorter passwords.
- Be mindful of passwords that are 'case sensitive' (uppercase and lowercase letters). Having your caps lock on may produce an invalid login if your password includes any lowercase letters.
- The best passwords contain a mixture of numbers and letters.
- Words are easier to remember than random letters. Try picking a memorable word and adding a few numbers before and/or after it.
- Some sites also utilize Security Images in order to log in. In this instance, make sure that your Security Image and Password are not the same.
- Never tell anyone your password.



\$250,000 Share Insurance Protection Extended to 2013

The Helping Families Save Their Homes Act of 2009, signed into law May 20, 2009, includes a provision extending \$250,000 share insurance coverage provided by the National Credit Union Share Insurance Fund through Dec. 31, 2013. Previously, this level of coverage was set to expire Dec. 31, 2009. The NCUSIF is managed by the National Credit Union Administration, the independent federal agency that supervises federal credit unions and is backed with full faith and credit of the U.S. government.

More information about NCUA insurance coverage is available online via the Share Insurance Tool Kit at <http://www.ncua.gov/Resources/ShareInsuranceToolkit.aspx>.



FREEDOM.

This tax season, enjoy more free time when you let our team prepare your 2009 tax return.

Our tax preparers weren't trained yesterday to file your taxes today. Take advantage of your credit union membership and let Langley Financial Services Tax Service help you through the tax process this year. We offer:

- Fast & Accurate Turnaround
- No Additional Cost to E-file
- Full Staff of Experienced Enrolled Agents

The LFS Tax Service Office is located at:
The LFCU Coliseum Branch
1055 West Mercury Boulevard, Suite 400
Hampton, Virginia

Appointments are also available at LFCU's Yorktown & Chesapeake Branches.

Call 838-7561 to schedule your appointment today!

SPECIAL OFFER

LFCU Member Discount

10% OFF

TAX SERVICES



Present this coupon for a 10% discount on tax preparation services.

Discount is limited to current year individual tax returns only.

IRA Contribution Designation

When making your annual Individual Retirement Account (IRA) contribution, whether by mail or in person, the IRA account holder must designate in writing (with signature) which year (2009 or 2010) the contribution will be applied. Contributions for tax year 2009 can be accepted through April 15, 2010.

Fight back the attack of the fees. . .

Get 6.99% APR* on balance transfers. Plus, no balance transfer fee.



Don't let credit card fees get the best of you. Fight the fees with LFCU's Switch & Save offer! Consolidate your debt by transferring your non-LFCU high interest credit card balances to your LFCU Credit Card through March 2010. You'll receive a special 6.99% APR* on transferred balances until January 2011. Plus, there are no transfer fees. So why stress over multiple credit card payments and potential rate hikes? Cut your credit card interest today!

Apply by completing the Switch & Save application found on the LFCU website at www.langleyfcu.org, at any branch location or by calling the Contact Center at (757) 827-5328 or (800) 588-3279 during business hours.

If you're not currently an LFCU Credit Card holder, apply online at www.langleyfcu.org.

*6.99% APR applies to transferred balances only. To receive the promotional rate - the balance transfer cannot be less than \$100 for each card balance transferred. If it is less, then the regular APR for your account shall apply. New purchases, cash advances and balance transfers after March 31, 2010 will be at the regular rate. Your APR will be determined based on credit worthiness and will range from 10.99% to 14.50% APR. Maximum balance transfer for promotional rate is \$20,000 or up to your available credit limit, whichever is less. Special rate is valid only for balance transfers from other credit card companies, financial institutions, or department store credit cards. The promotional rate for balance transfers will not apply for checks made payable to you, cash or to make payments toward amounts you owe Langley Federal Credit Union. You will need to make sure to continue to make your monthly payments to the issuer/merchant until you receive a statement from the issuer/merchant reflecting the balance transfer payment, as transfers may not be immediate. Langley FCU will not be responsible for any finance charges or late fees incurred due to your non-payment. Any balance transfers or convenience checks processed after the promotional period will incur finance charges at the standard rates. Payments will be applied to any balance at the lower rate before being applied to balances at the card's standard rate. Effective February 22, 2010, if your payment exceeds the minimum payment due each billing period, we will apply the excess payment to balances with the high APR before applying the excess payment to balances with the lower APR. The promotional APR for balances transferred will remain in effect through the January 2011 credit card statement cycle - after which time, new purchases, cash advances and transfers will carry your card's standard rate of 10.99% or 14.50% APR. Transfers must be made by March 31, 2010.

Use your MasterCard for another "priceless" opportunity



Every time you use your MasterCard Credit or Debit card between January 2 and February 15, 2010, you will automatically be entered for a chance to win a trip to the Arnold Palmer Invitational in March 2010. For more information, visit www.langleyfcu.org.

Register Now for LFCU's Annual Meeting

Join Langley Federal Credit Union at our 74th Annual Meeting at the Hampton Roads Convention Center in Hampton, April 28, 2010 at 6:00 PM.

Come out for a celebratory, informational evening with your fellow members, learn what LFCU has done this year and what you can look forward to next year. Refreshments will be served, and of course you will have a chance to win one of our fabulous door prizes! **TICKETS WILL BE MAILED & REQUIRED FOR ADMISSION.**

If you would like to attend, please complete the reservation form by March 31st and submit to any branch or mail to: Langley Federal Credit Union, Attn: Marketing Department, P.O. Box 7463, Hampton, Virginia 23666. The event is for LFCU Members only. If you require special assistance, please plan to arrive early.

ANNUAL MEETING REGISTRATION FORM & TICKET REQUEST

Member Name _____ Account # _____

Member Name _____ Account # _____

Member Name _____ Account # _____

Member Name _____ Account # _____

Street Address _____

City _____ State _____ Zip _____

Phone # _____

Constellation Club Scholarship Applications Available

LFCU's Constellation Club helps teach children through age 18 the importance of financial responsibility and the rewards of saving. As a Constellation Club member, your child has an opportunity to win both monetary and scholarship rewards for saving. Applications for these awards will be in each of our branches and on-line this month. Call 757-827-LFCU or visit www.langleyfcu.org for more information.

Annual Award Opportunities:

Little Dippers (through age 10)

- Ten Virginia Air & Space Center Summer Science Camp Scholarships
- Five \$50 Share Deposits

Shooting Stars (ages 11 through 18)

- One NASA Space Camp Scholarship (Huntsville, AL)
- Five \$100 Share Deposits
- Four \$5,000 Galaxy Graduate College Scholarships (awarded to graduating high school seniors)

Requirements:

Constellation Club members need to have maintained a "B" average or above (current school year) and made at least one deposit each quarter during the course of their membership (2009 only). Constellation Club Accounts need a minimum annual deposit total of \$50 for Little Dippers or \$100 for Shooting Stars. Deadline for application is February 28, 2010, and awards will be presented at our Annual Meeting in April.

Free Member Education Seminars

DATE	TIME	TOPIC
January 14 th	6:30 p.m. - 8:00 p.m.	Tax Update Seminar
January 23 rd	8:30 a.m. - 3:00 p.m.	Homeownership Seminar
January 28 th	6:30 p.m. - 7:30 p.m.	Long Term Care
February 11 th	6:30 p.m. - 8:00 p.m.	Budgeting In Tough Economic Times
February 25 th	6:30 p.m. - 7:30 p.m.	Understanding Your Credit Score

Seminars are free and held at LFCU's Member Education Center in the Oyster Point Branch, 11742 Jefferson Avenue, Suite 110, Newport News, Virginia. Register by calling Kitty Simon, Director of Member Education, at 757-825-7112 or online at www.langleyfcu.org/community/seminars. For complete course descriptions, please visit www.langleyfcu.org.

HOLIDAY CLOSINGS

- ▲ Monday, January 18th - Martin Luther King Day
- ▲ Monday, February 15th - Presidents' Day

BOARD OF DIRECTORS

Richard A. Biege.....Chairman
 Peter A. Morley (CMSgt. USAF-Ret.).....Vice Chairman
 Jean M. Yokum.....Treasurer
 George R. Hayes.....Secretary
 William E. Griffith, Jr.....Assistant Secretary
 Buena E. Crawford.....Director
 Bruce R. Hoogstraten.....Director
 R. Lester Wingrove, Jr.....Director
 Joyce M. Wright.....Director



James L. Frost (Lt. Col. USAF-Ret.).....Director Emeritus

BRANCH LOCATIONS

- ◆ ABERDEEN
409 Aberdeen Rd., Hampton
- ◆ AIR FORCE
Building 467, LAFB, Hampton
- ◆ CHESAPEAKE CROSSROADS
4107 Portsmouth Blvd., Ste 114, Chesapeake
- ◆ CITY CENTER
721 Lakefront Commons, Newport News

- ◆ COAST GUARD
USCG Tracen, Building 46, Yorktown
- ◆ COLISEUM
1055 W. Mercury Blvd., Hampton
- ◆ DENBIGH
12644 Jefferson Ave., Newport News
- ◆ EAGLE HARBOR
13478 Carrollton Blvd., Unit A, Carrollton
- ◆ HAYES
3140 George Wash. Mem. Hwy., Hayes
- ◆ NASA
Bldg. 1310 LaRC, Hampton
- ◆ OYSTER POINT
11742 Jefferson Avenue, Newport News
- ◆ POQUOSON
415 Wythe Creek Rd., Poquoson
- ◆ STONEYBROOK
15463 Warwick Blvd., Newport News
- ◆ WARWICK
11107 Warwick Blvd., Newport News
- ◆ WILLIAMSBURG CITY
1222 Richmond Road, Unit 16, Williamsburg
- ◆ WILLIAMSBURG NEW TOWN
5220 Monticello Avenue, Williamsburg
- ◆ WILLOW OAKS
225 Fox Hill Road, Suite D5, Hampton

- ◆ YORKTOWN
4822 George Washington Mem. Hwy., Grafton

For a complete list of Credit Union Service Centers, visit www.cuservicecenter.com.

GENERAL INFORMATION

PHONES, LOCAL

Contact Center.....757-827-LFCU
 Phone Loans.....757-827-EASY
 CHIPS.....757-827-9434
 Mortgages.....757-825-7108
 Langley Financial Services, LLC.....757-898-0089

PHONES, TOLL-FREE

Main.....800-826-7490
 CHIPS.....800-233-2819
 Phone Loans.....800-588-EASY

MAILING ADDRESS

P.O. Box 7463, Hampton, VA 23666

WEBSITE

www.langleyfcu.org

CORE VALUES

Ethics · Accountability · Loyalty · Passion · Honesty



CREDIT UNIONS

Federally insured by NCUA.