NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: December 2005 **LETTER NO.: 05-CU-20**

TO: Federally Insured Credit Unions

SUBJ: Phishing Guidance for Credit Unions And Their Members

REF: Letter to Credit Unions #04-CU-12 Phishing Guidance for Credit Union Members

DEAR BOARD OF DIRECTORS:

In our Letter to Credit Unions #04-CU-12 Phishing Guidance for Credit Union Members, we highlighted the need to educate your membership about phishing activities. As the number and sophistication of phishing scams continues to increase, we would like to emphasize the importance of educating your employees and members on how to avoid phishing scams as well as action you and/or your members may take should they become a victim.

Appendix A of this document contains information you may share with your members to help them from becoming a victim of phishing scams. Appendix B contains information you may share with your members who may have become a victim of phishing scams.

Background

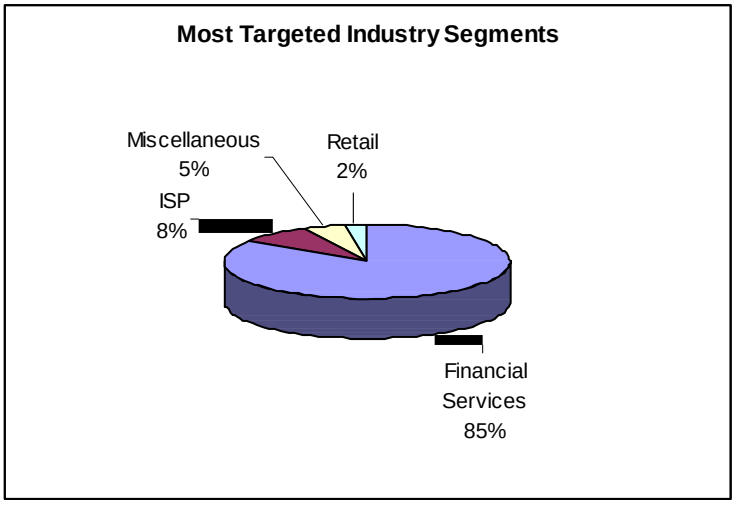
Phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords, account, credit card details, etc. by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message. Often the message includes a warning regarding a problem related to the recipient's account and requests the recipient to respond by following a link to a fraudulent website and providing specific confidential information. The format of the e-mail typically includes proprietary logos and branding, such as a "From" line disguised to appear as if the message came from a legitimate sender, and a link to a website or a link to an e-mail address. All of these features are designed to assure the recipient that the e-mail is from a legitimate business source when in fact, the information submitted will be sent to the perpetrator.

Phishing can take many forms such as:

- Deceptive Phishing;
- Malware Phishing;
    - key loggers and screen loggers
    - session hijackers
    - web trojans
    - hosts file poisoning
    - system reconfiguration attacks
    - data theft
- Domain Name System (DNS) Phishing (commonly referred to as Pharming);
- Content-Injection Phishing;
- Man-in-the-Middle Phishing; and
- Search Engine Phishing.

Each of the above phishing techniques is described in detail in the Identity Theft Technology Council's[1] (ITTC) whitepaper, *Online Identity Theft: Technology, Chokepoints and Countermeasures*. The whitepaper also includes specific action credit unions may take to reduce the chance of being phished as well as steps to take should your credit union become a target of phishing. The whitepaper is available for download from Anti-Phishing Working Group's (APWG)[2] website at: http://www.antiphishing.org/Phishing-dhs-report.pdf.

As of August 2005, the APWG reported that the financial services industry continued to be the most targeted industry sector staying steady at nearly 85% of all attacks. In addition, the APWG is seeing a wide diversity of brands being spoofed and very small financial institutions all over North America and Western Europe are steadily appearing as phishing targets.



[1] Members of the Identity Theft Technology Council represent a public-private partnership between the U.S. Department of Homeland Security (DHS), Science and Technology Directorate (S&T), SRI International, the Anti-Phishing Working Group, and private industry.

[2] The Anti-Phishing Working Group is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem. Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are more than 1300 companies and government agencies participating in the APWG and more than 1900 members.

Prevention and Mitigation

Credit union member education and staff training are important tools you can use to combat e-mail frauds such as phishing. Appendix A to Part 748 of the NCUA Rules & Regulations contains guidelines designed to ensure the security and confidentiality of member information; protect against any anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member; and ensure the proper disposal of member information. Credit unions should consider implementing the following measures as appropriate:

- Implement a policy that your credit union will not solicit confidential or sensitive member information via e-mail and inform members of the policy on a periodic basis.

- Provide a notice[3] to your credit union members describing your security policies and practices including the role the member can play in protecting his or her own information.

- Include a security-related page[4] on your website to educate members about phishing and other fraudulent activities.

- Adopt a policy to personalize e-mails to members using their names in the message, and inform members of this policy[5].

- Keep abreast of advances in technology designed to protect member information and reduce e-mail fraud, and take advantage of those that are effective and practical for your credit union. For example, if your credit union provides high-risk Internet based services, you should consider using multifactor authentication techniques (see NCUA Letter to Credit Unions #05-CU-18 Guidance on Authentication in Internet Banking Environment for detailed information on multifactor authentication).

---

[3] This notice should include information to make members aware of fraudulent activities and scams that can be carried out using e-mail, the Internet, and other communication channels. The notice should also describe what the member should do if they suspect they are the targets of one of these schemes. The security policies and the notification to customers should include specifics regarding what information you will not request from members via e-mails, telephone, or other communication methods. With this information, your members will be more alert to suspicious e-mails. This notice may appear on monthly statements, the credit union's website, and other periodic communications.

[4] The page might include information about known frauds and instructions on what members should do if they identify or suspect one. An effective practice is to place a prominent link or button on each page of your website that will direct the reader to the security page.

[5] Perpetrators often use mass-mailing programs to send "spam' e-mails to many recipients using a non-personalized greeting such as "Valued Member" or "To Whom It May Concern". Instruct members not to respond to such e-mails and to notify you if they receive any e-mails purporting to be from your credit union that do not include this personalization.

- Apply system (hardware and software) patches and upgrades on a timely basis.

- Maintain information security procedures in accordance with current industry best practices and regulatory guidance (see Additional References section).

- Keep website certificates[6] current and educate members how to verify that the pages they are viewing are actually those of your credit union.

- Design educational popup messages[7] to appear occasionally when a member logs in or views certain pages.

- Train security and service staff regarding your policies and procedures for protecting member information, including those concerning phishing and other forms of e-mail fraud, so they are sensitive to member comments and informed of the appropriate actions to take.

Incident Response

If you become aware of actual phishing incidents using your credit unions' name, logo, graphics, etc. attempting to solicit information from your members (also known as "spoofing"), you should consider taking the following actions as appropriate:

- Post a prominent alert notice[8] on your website's homepage and login screen.

---

[6] If an organization wants to have a secure web site that uses encryption, it needs to obtain a site, or host, certificate. Some steps you can take to help determine if a site uses encryption are to look for a closed padlock in the status bar at the bottom of your browser window and to look for "https:" rather than "http:" in the URL. By making sure a web site encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to gather your information. If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure web site, your browser will check the certificate for the following characteristics: (1)the web site address matches the address on the certificate; and (2)the certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority. There are two ways to verify a web site's certificate. One option is to click on the padlock in the status bar of your browser window. However, your browser may not display the status bar by default. Also, attackers may be able to create malicious web sites that fake a padlock icon and display a false dialog window if you click that icon. A more secure way to find information about the certificate is to look for the certificate feature in the menu options. This information may be under the file properties or the security option within the page information. You will get a dialog box with information about the certificate, including the following: (1)Who issued the certificate-You should make sure that the issuer is a legitimate, trusted certificate authority (you may see names like VeriSign, thawte, or Entrust); (2)Who the certificate is issued to-The certificate should be issued to the organization who owns the web site. Do not trust the certificate if the name on the certificate does not match the name of the organization or person you expect; and (3)Expiration date-Most certificates are issued for one or two years. One exception is the certificate for the certificate authority itself, which, because of the amount of involvement necessary to distribute the information to all of the organizations who hold its certificates, may be ten years. Be wary of organizations with certificates that are valid for longer than two years or with certificates that have expired.

[7] Possible messages subjects include how to identify a phishing attack, how to avoid the consequences, how to report attacks to you, and how to get to the security section of the website.

[8] The notice should relate the details of the phishing incident so the reader will be able to recognize it and know not to respond to it or other e-mail requests of this type. The notice should also reiterate your credit union's security

- Contact members directly by mail and/or e-mail providing them with the information noted above.

- Monitor member accounts for unusual activity and trends.

- Flag and monitor closely the accounts of members who report that they have fallen victim to a phishing or similar e-mail scam.

- Alert your staff to the incident so that they are sensitive to the situation and report activity such as unusual address change requests, account transactions, or new account activity.

- Encourage members who believe that they have been a victim of the phishing scam to follow the recommendations published in the brochure, *You Can Fight Identity Theft*, outlining steps members should take to reduce the risk of identity theft.

A "camera-ready" version of the brochure is available on the NCUA Website at http://www.ncua.gov/Resources/Documents/LCU2001-09ENC.pdf for downloading and copying. For credit unions that do not have access to the Internet, limited copies of the brochure can be obtained directly by contacting:

National Credit Union Administration
Office of the Chief Financial Officer – Division of Procurement and Facilities Management
1775 Duke Street
Alexandria, VA 22314
Telephone: (703) 518-6340

You should report incidents of phishing and other e-mail fraud attempts that target your credit union to the link provided in the NCUA Website **("Internet/E-Mail Fraud Alert")**.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

/s/
JoAnn M. Johnson
Chairman, National Credit Union Administration Board

policies and practices and indicate how to identify legitimate communications from your credit union. Finally, the notice should include a point of contact should the member need more information or wish to report that they have been a victim of the scam.

Additional References

Following are further sources of information regarding phishing and other e-banking-related frauds that may assist you in developing policies, education programs, and credit union members' assistance plans:

National Credit Union Administration

- NCUA Letter to Credit Unions #05-CU-18 *Guidance on Authentication in Internet Banking Environment*
- NCUA Letter to Credit Unions #04-CU-12 *Phishing Guidance for Credit Union Members*, issued September 2004
- NCUA Letter to Credit Unions #04-CU-06 *E-Mail and Internet Related Fraudulent Schemes Guidance*, issued April 2004
- NCUA Letter to Credit Unions #04-CU-05 *Fraudulent E-Mail Schemes*, issued April 2004
- NCUA Letter to Credit Unions #03-CU-12 *Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions*, issued August 2003
- NCUA Letter to Federal Credit Unions #02-FCU-11 *Tips to safely Conduct Financial Transactions Over the Internet – An NCUA Brochure for Credit Union Members*, issued July 2002

Federal Financial Institutions Examination Council IT Examination Handbook

- *Information Security Booklet, December 2003*
  http://ithandbook.ffiec.gov/

Federal Trade Commission

- *How Not to Get Hooked by the 'Phishing ' Scam*, July 2003
- *ID Theft: When Bad Things Happen to Your Good Name*

Anti-Phishing Work Group

- *Online Identity Theft: Technology, Chokepoints and Countermeasures*, October 2005
  www.antiphishing.org/Phishing-dhs-report.pdf

Appendix A

The following is a list of recommendations you could share with your members to help them ***avoid*** becoming a victim of phishing scams.

- Be suspicious of any email with urgent requests for personal financial information unless the email is digitally signed (you can't be sure it wasn't forged or 'spoofed'). Phishers typically: (1)include upsetting or exciting (but false) statements in their emails to get people to react immediately; (2)ask for confidential information such as usernames, passwords, credit card numbers, social security numbers, account numbers, etc.; and (3)do not personalize the email message (while valid messages from your credit union should be).

- Don't use the links in an email to get to any web page if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.

- Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone.

- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just http://.

- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites.

- Regularly log into your online accounts and don't wait for as long as a month before you check each account.

- Regularly check your financial institution, credit, and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your financial institution(s) and card issuers.

- Ensure that your browser is up to date and security patches applied.

- Always report "phishing" or “spoofed” e-mails to the following groups:
    - forward the email to reportphishing@antiphishing.com;
    - forward the email to the Federal Trade Commission at spam@uce.gov;
    - forward the email to the "abuse" email address at the company that is being spoofed;
    - when forwarding spoofed messages, always include the entire original email with its original header information intact; and
    - notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/.

Appendix B

What To Do If You've Given Out Your Personal Financial Information

Phishing attacks are growing quite sophisticated and difficult to detect, even for the most technically savvy people. And many people are getting onto the Internet and using email or Web browsers for the first time. As a result, some people are going to continue to be fooled into giving up their personal financial information in response to a phishing email or on a phishing website. If you have been tricked this way, you should assume that you will become a victim of credit card fraud, financial institution fraud, or identity theft. Below is some advice on what to do if you are in this situation:

- Report the theft of this information to the card issuer as quickly as possible:
  - Many companies have toll-free numbers and 24-hour service to deal with such emergencies.

- Cancel your account and open a new one.

- Review your billing statements carefully after the loss:
  - If they show any unauthorized charges, it's best to send a letter to the card issuer describing each questionable charge.

- Credit Card Loss or Fraudulent Charges (FCBA):
  - Your maximum liability under federal law for unauthorized use of your credit card is $50.
  - If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use.

- ATM or Debit Card Loss or Fraudulent Transfers (EFTA):
  - Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
  - You risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you.

- Report the theft of this information to the bank as quickly as possible.

Some phishing attacks use viruses and/or Trojans to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames, passwords, Social Security Numbers, etc. In this case, you should:

- Install and/or update anti-virus and personal firewall software.

- Update all virus definitions and run a full scan.

- Confirm every connection your firewall allows.

- If your system appears to have been compromised, fix it and then change your password again, since you may well have transmitted the new one to the hacker.

- Check your other accounts! The hackers may have helped themselves to many different accounts: eBay account, PayPal, your email ISP, online bank accounts, online trading accounts, e-commerce accounts, and everything else for which you use online password.

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. If you have given out this kind of information to a phisher, you should do the following:

- Report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and do the following:
    - Request that they place a fraud alert and a victim's statement in your file.
    - Request a FREE copy of your credit report to check whether any accounts were opened without your consent. You can find information about obtaining free credit reports on the Federal Trade Commission's website at: http://www.ftc.gov/bcp/conline/edcams/freereports/index.html.
    - Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft.

- Major Credit Bureaus:
    - Equifax - www.equifax.com:
        - To order your report, call: 800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241.
        - To report fraud, call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241.
        - Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.
    - Experian - www.experian.com:
        - To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen TX 75013.
        - To report fraud, call: 888-EXPERIAN (397-3742) and write: P.O. Box 9530, Allen TX 75013 TDD: 1-800-972-0322.
    - Trans Union - www.transunion.com:
        - To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022.
        - To report fraud, call: 800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803.

- Notify your financial institution(s) and ask them to flag your account and contact you regarding any unusual activity:
    - If bank accounts were set up without your consent, close them.
    - If your ATM card was stolen, get a new card, account number, and PIN.

- Contact your local police department to file a criminal report.

- Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information.

- Notify the Department of Motor Vehicles of your identity theft:
    - Check to see whether an unauthorized license number has been issued in your name.

- Notify the passport office to be watch out for anyone ordering a passport in your name.

- File a complaint with the Federal Trade Commission:
    - Ask for a free copy of "ID Theft: When Bad Things Happen in Your Good Name", a guide that will help you guard against and recover from your theft.

- File a complaint with the Internet Fraud Complaint Center (IFCC)
    - http://www.ifccfbi.gov/index.asp.
    - The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet.
    - For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation.

- Document the names and phone numbers of everyone you speak to regarding the incident. Follow-up your phone calls with letters. Keep copies of all correspondence.