# Anti-Phishing

Phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information such as passwords, account numbers, or credit card details by masquerading as a trustworthy person or business in an apparent official electronic communication, such as an email 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 email 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 email address. All of these features are designed to assure the recipient that the email is from a legitimate business source when in fact, the information submitted will be sent to the perpetrator.

If you become aware of actual phishing incidents using your credit union's name, logo or graphics, attempting to solicit information from your members (also known as "spoofing") you should take the following actions as appropriate:

- Post a prominent alert notice on your homepage and login screen
- Contact members directly by mail and/or email providing them with the information noted above
- Monitor member's accounts for unusual activity and trends
- Flag and monitor the accounts of members who report that they have fallen victim to a phishing or a similar email 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

The following is a list of recommendations you should share with your members to help them avoid becoming a victim of a phishing scam:

- 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:
  - Include upsetting or exciting (but false) statements in their emails to get people to react immediately
  - Ask for confidential information such as usernames, passwords, credit card numbers, social security numbers, account numbers, etc.
  - 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 webpage 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 over the telephone.
- Always make sure that you are using a secure website when submitting credit card or other sensitive information via your web browser. To make sure you are on a secure web server, check the beginning of the web address in your browser's address bar - it should be "https://" rather than just "http://."
- Consider installing a web browser toolbar 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 card, and debit card statements to make sure that all transactions are legitimate. If anything is suspicious, contact your financial institution(s) and card issuers.
- Make sure that your browser is up to date and security patches are applied.
- Always report "phishing" or “spoofed” emails 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
  - Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: ic3.gov

What to do if you have given out your personal financial information

Phishing attacks are growing quite sophisticated and difficult to detect, even for the most technically savvy people. 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 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 statement containing unauthorized use is mailed to you.
- Report the theft of this information to your financial institution as quickly as possible.

Some phishing attacks use viruses 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, PayPal, your email ISP, online financial institution accounts, online trading accounts, e-commerce accounts and everything else for which you use an 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: 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**: 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 (800) 255-0056 and ask the operator to call the Auto Disclosure Line at (800) 685-1111 to request a copy of your report.

  **Experian**: 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: (800) 972-0322.

  **Trans Union**: 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: (877) 553-7803.

- Notify your financial institution(s) and ask them to flag your account and contact you regarding any unusual activity:
  - If any accounts were setup 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 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) 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.

You should report incidents of phishing and other email fraud attempts that target your credit union to the link provided in the NCUA website: Internet/Email Fraud Alert

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

Corporate Central Credit Union is committed to maintaining the privacy of our members. We maintain any information you provide over the Internet according to our usual strict security and confidentiality standards. For security of our website and to ensure that the website remains available to all users, Corporate Central Credit Union employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information.

If you have any questions about the way your information is used in connection with our website or about Corporate Central Credit Union's privacy statement, please contact us at (800) 242-4747 or (414) 425-5555.

**EMAIL "PHISHING"**
Phishing (pronounced "fishing") is a scam to steal valuable information such as credit card and social security numbers, user IDs, and passwords. Phishing, also known as "brand spoofing," is when an official-looking email is sent to potential victims pretending to be from their ISP, credit union, bank or a retail establishment. Emails can be sent to people on selected lists or on any list and the scammers expect some percentage of recipients will actually have an account with the real organization.

**LAND LINE TELEPHONE "VISHING" & INTERNET PHONES "VISHING" (VoIP)**
Vishing, (Voice phISHING) also called "VoIP phishing for the Internet phones," is the voice counterpart to phishing. Instead of being directed by email to a website, an email message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's card number or other personal or financial information. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number or another area code within or outside the United States.

In either case, because people are used to entering card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed and the entire operation can be brought up and taken down in a short time, compared to a land line telephone.

**TEXT MESSAGE "SMISHING"**
Smishing (SMS phISHING) is the mobile phone counterpart to phishing. Instead of being directed by email to a website, a text message is sent to the user's cell phone or other mobile device with some ploy to click on a link. The link causes a Trojan to be installed in the cell phone or other mobile device.

**NEW! MAIL LETTER "PHISHING"**
This new scam occurs when the phisher is creating a letter and sending it through the mail to individuals to respond to the letter by calling a phone number. The phisher outlines in the letter that the individual must respond for their own protection. This scam is used in conjunction with other channels to steal valuable personal and financial information of the individual receiving the letter.

**Loss Prevention Recommendations:**
Educate your membership on "Phishing, Smishing and Vishing."

- Post warnings on your website, in newsletters and in branch lobbies
- Post a notice on your credit union's website, stating that you will NEVER solicit personal or private information via email
- If a message is received by someone claiming to be your financial institution asking for confidential information NEVER respond unless you initiated the request
- Educate your members if they have doubts about who's on the phone, call back the number of record at your financial institution or card company
- Advise your members to be wary of any message received from an unknown sender
- Educate your members to not open unsolicited emails or text messages
- Advise your members to not click on any links provided in unsolicited emails
- Encourage your members to monitor financial accounts on a regular basis
- If your member has a landline or Voice over the Internet Phone (VoIP), recommend your member to create a password protected account
- Educate your members to deploy "blockers" on emails, text messaging, phone numbers, both landline and VoIP. In addition, consider "extra" caution when using "text messaging." Your member may want to disable the "text messaging" feature on their mobile device if they are not using it. Don't display your wireless phone number or email address in public. This includes newsgroups, chat rooms, websites, or membership directories.
- Educate your members if they open an unwanted message to send a stop or opt out message in response
- Educate your members to check the privacy policy when submitting their wireless phone number or email address to any website. Find out if the policy allows the company to display or sell your information.
- Encourage your members to contact their wireless or Internet Service Provider about unwanted messages

If a member is a victim of Phishing, Smishing or Vishing, take appropriate steps:

- Block and reissue the compromised credit/debit cards or the account that is at risk
- If not blocking the at-risk card number or account, utilize an authorization strategy to prevent fraud exposure
- Have your member report the incident to the credit bureau
- Encourage your member to order a credit report
- Report suspicious internet sites and emails to the government and for additional protection tips visit ic3.gov or the Federal Government's Consumer Information Center at consumer.gov/Tech.htm
- Work with your Internet Service Provider or telephone carrier to shut down fraudulent websites or telephone numbers
- Use tools provided by a reputable Internet brand protection service to conduct regular comprehensive internet monitoring
- Monitor all web links to ensure proper authorization, content, privacy and security
- Ensure that appropriate written contracts are in place with all authorized third parties
- Ensure that proper disclosure notices are posted on your credit union's website
- Take appropriate action against cyber squatters and other unauthorized operators to ensure continued control of domain names and web-linking relationships
- If you can determine the Internet Service Provider hosting the imposter/spoofed website, contact the Internet Service Provider to request that the website be immediately disabled and all information pertaining to it be preserved for law enforcement

- Maintain a comprehensive and up-to-date domain portfolio
- Register key brand names as well as the credit union's name
- Register names under all relevant domain names, including all top-level domains and country codes
- Confirm the domain names that your credit union has purchased. Confirm you have purchased .MOBI. to prevent it from being used by the scammer.
- Use reputable domain name registration authority

A good resource for this topic is Anti-Phishing Working Group at antiphishing.org/index.html

If you have been victimized by a spoofed email or website, you should contact your local law enforcement, US Postal Inspector or the FBI.