Internet Banking Security

The Internet has made it easier for criminals to deceive individuals into revealing confidential information and clicking on links or attachments that will compromise the security of their computers which ultimately have an impact on Internet banking security. These criminals have continued to use increasingly sophisticated, effective, and malicious methods to fraudulently gain unauthorized access to consumers' Internet banking accounts.

At LA Financial Federal Credit Union we understand that security measures are a top priority and of utmost importance for Internet banking. LA Financial Federal Credit Union has implemented a significant level of security features to mitigate the risk of fraudulent Internet activity however we strongly encourage both our consumer and business members using Internet banking and cash management services to be aware of current threats to the security of their Internet banking accounts, and to implement internal preventative and monitoring controls to reduce the risk of compromised access and account takeover.

LA Financial Federal Credit Union is required under *Regulation E: Electronic Fund Transfers* to provide certain protections to our members relative to electronic fund transfers (EFT). As applicable to Internet access, this regulation covers transactions initiated through LA Financial Federal Credit Union's Internet banking and cash management channels, to either order, instruct, or authorize the financial institution to debit or credit an account. Transactions may include but are not limited to ACH payments, external transfers, and bill payments. For specific applicability and provisions, please refer to LA Financial Federal Credit Union's EFT disclosure which is included with this notification.

LA Financial Federal Credit Union will **NEVER** request a member's personal information (debit card number, account number, social security number, personal identification number or password) through email or by phone. If you ever receive an unsolicited phone call or email claiming to be from LA Financial Federal Credit Union requesting your personal and confidential information, please **DO NOT** respond. Contact us immediately by calling 800-894-1200.As an additional monitoring control, you should review account statements and online account transaction history to ensure all transactions are correct and authorized.

Fraudsters will commonly use a type of Internet piracy called "phishing." In a typical Phishing case, you'll receive an e-mail that appears to be from LA Financial Federal Credit Union. In some cases, the e-mail may appear to come from a government agency, including the FDIC. The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the Credit Union's web site. In a phishing scam, you could be **redirected to a fictitiousweb site** that may look exactly like the Credit Union's site. In other situations, it may be the Credit Union's actual web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your login authenticationcredentials. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth. ***If you provide the requested information, you may find yourself the victim of identity theft which can lead to malicious activity such as Internet banking account takeover.***

LA Financial Federal Credit Union is required through its regulators to conduct regular periodic risk assessments of their Internet banking products and services to identify security threats, and controls in place related to internal and external security, changes in member functionality offered through Internet banking, and actual incidents of security breaches, ID theft, or fraud experienced internally or within the industry. As a proactive measure, we strongly suggest to our business or commercial members to also perform a periodic risk assessment and controls evaluation related to security of their Internet banking / cash management environment. Special attention should be directed to high risk transactions which involve access to personal financial information or the movement of funds to other parties such as ACH, wire transfers, and bill payment.

LA Financial Federal Credit Union has implemented strong preventative and monitoring controls within its Internet banking, bill payment, and cash management systems however in order to enhance our member's internal security we recommend our members implement their own controls to mitigate risks. Examples of controls you may want to consider implementing to mitigate the risks of account takeover and fraudulent account activities are as follows:

- Maintain up-to-date operating system security patches and have installed updated virus/spyware protection software. Viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus and anti-spyware software will help to keep your computer safe from malicious software that could install itself or may try to install itself on your computer.
- Install a Firewall, either software or hardware. A firewall will prevent attacks on your computer through the Internet using established rules to determine if a requested connection is malicious or not.
- Implement intrusion detection/prevention software or services
- Safekeeping and confidentiality of Internet banking authentication credentials
- For business members, implement dual control for initiating and approving high risk Cash Management transactions such as ACH origination and wire transfers
- Daily account activity monitoring via Internet banking account transaction history review
- Review and monitor your checking account, debit card, and credit card statements for unauthorized transactions.
- Refrain from opening unsolicited email and attachments
- Refrain from providing authentication credentials to callers claiming to be representing the financial institution and from responding to emails requesting information or re-directing you to a website.
- Prior to disposing, shred all confidential information on hardcopy and on electronic media.

If you notice any suspicious or unauthorized account activity, experience a breach in security of personal information, your login credentials or computer security have been compromised, or for more information please contact our Fraud and Risk Management Department at info@lafinancial.org or call 800-894-1200.