Credit Union Connections

LINCOLN MAINE Federal Credit Union

A Member-Owned Financial Cooperative

Important information for Lincoln Maine Federal Credit Union Members Summer 2017

Online Banking Upgrades Coming Soon!

Our Online Banking upgrade is scheduled to launch August 7, 2017! You will be required to re-register in Online Banking, which can be done simply by clicking on the *Register Here* link, located next to the Online Banking log in at lincolnmainefcu.com.

Features include:

- Member to Member Transfers
- Family & Friends – allows people who are not on an account to be able to transfer to it
- eAlerts
- Secure Messaging
- Graphs of Transaction History

Some things you should know:

- The upgrade to Online Banking will occur on August 7 at 10:00 am. The site will be down approximately one hour. Mobile banking will be unavailable during this time.
- You must have a valid email address on file with the credit union in order to register.
- Scheduled transfers and related accounts will all transfer to the new Online Banking site.
- In order to access Mobile Banking you must complete the registration process by clicking on the *Register Here* link, located in the Mobile App.

Our priority is to have a smooth and seamless transition process for all of our members. If you have any questions or need help in the registration process, please call us at 207-794-8623.

Same-Day ACH Payments: What This Change Means for You

When making a payment, have you gotten used to some lag-time between the transaction and the money clearing your account? This will be going away – for example, if you pay your cable bill by telephone in the morning, the funds could be cleared from your account before 5:00 p.m. the same day.

On September 15, the Federal Reserve will start processing same-day ACH (Automated Clearing House) payments. This is an option that allows funds to move more quickly than in the past, further modernizing current payment systems. Retailers can opt to convert the checks you write to ACH by using the same system that is used for bill payments. Payments you schedule via websites, telephone or mobile apps where you provide your account number could be affected by this change.

Three Tips to be Prepared

1. Don't Assume Funds Will Clear the Day After Purchase

Habits can be hard to break. Get in the habit now of planning for funds to clear at the time you check out.

2. Check Your Share Draft Balance

Keeping a low balance can have a negative impact in the event a same-day ACH payment overdraws your account and incurs a fee. Even with overdraft protection, keeping your account balance at a level that supports your spending is the best way to keep your account in the green.

3. Ask Questions

We are here to help! Leading up to and after this change occurs, watch your statements for additional announcements. And as always, please contact us by phone, email, or stop into our branch to ask any questions that you may have!

Products & Services

Visa® Check Cards
Direct Deposit
Payroll Deduction
On-Line Bill Pay Services
Teller-Phone℠
Home Banking
CUe-Statement℠
Visa Credit Cards
And much more!

Lincoln Hours

Lobby
Monday-Thursday
8:30 a.m.-4:00 p.m.
Friday
8:30 a.m.-5:00 p.m.
Saturday
9:00 a.m.-11:30 a.m.

Drive Up
Monday-Thursday
8:00 a.m.-4:00 p.m.
Friday
8:00 a.m.-5:00 p.m.
Saturday
9:00 a.m.-12:00 noon

Addresses

Lincoln Office
171 West Broadway
P.O. Box 220
Lincoln, ME 04457-0220
(207) 794-8623
Fax (207) 794-8187

Lee ATM
2789 Lee Road
Lee, ME 04455

Howland ATM
61 Lagrange Road
Howland, ME 04448

lmfcu@lincolnmainefcu.com
www.lincolnmainefcu.com

Holidays

Independence Day
Tuesday, July 4

Labor Day
Monday, September 4

Let's NOT Go Phishing!

Do you know what to look out for in phishing email scams? Often sent by email, these scams seek to infect computers with malware or steal personal information, but often, even savvy surfers of the web can be fooled.

What is "Phishing"

"Phishing" has received a lot of attention in the press recently. It is a way that fraudsters try to acquire personal, sensitive information such as login names, passwords, credit and debit card information, birth dates, and social security numbers, to access financial resources for malicious purposes. Phishing scams often appear to come from a familiar, trusted resource through your email. While the attempts sometimes obviously look like spam, a well-crafted email can contain the logo of the entity the fraudster is trying to mask their identity through and can be difficult to identify.

How Can I Protect Myself?

Email communication is becoming more and more common, but there are a few ways you can avoid falling victim to a phishing scam. Here are four steps you can take to protect your personal information in a phishing scam:

1. Watch for Misspelled URLs

Appearing in the address bar, these can be off by as little as one character, or may have a subdomain added to the main address that drives to the spoofed website.

2. Think Before You Click the Link

Again, this can be tricky to watch for, but if you hover your mouse over a link in an email *without clicking on it*, you can see the web address. If it looks suspect, do *not* click the link and contact customer service for the company the email appears to have originated from.

3. Start Using Multi-Factor Authentication

We know – *not another password!* You may have seen some companies requiring a second security step, such as a PIN or a fingerprint, which is required in addition to your login and password to access an account. While it may seem like a bother, this protects you. In the event your passwords were stolen in a phishing scam, having the additional step in place adds a level of security that prevents a thief from accessing any information using only the password.

4. Ask Us at Lincoln Maine FCU

If you ever receive an email that looks like it is from us, but something feels off or suspicious about it, please do not hesitate to visit your nearest branch to discuss what you saw. Our staff will be able to help you clarify whether or not the email originated from our credit union, or will be able to report the fraudulent activity in the event it has occurred.