Credit Union Connections

LINCOLN MAINE Federal Credit Union

A Member-Owned Financial Cooperative

Important information for Lincoln Maine Federal Credit Union Members Winter 2017

# 10 Ways to Stay Safe Using Online Banking

When using your credit unions' online or mobile banking services, your main goal is most likely to balance your account or ensure that a check has been deposited. While these essential tasks are made easy with online banking, Maine's Credit Unions want members to be aware it's important to take precautions online. These services are safe and secure, but there are steps you can take on your devices to ensure that your personal or account information is not in anyone else's hands but your own.

Here are the top ten tips that credit unions offer their members about securing their online banking accounts:

1. **Update your web browsers and computer software**, such as your Windows or Mac operating systems. Threats from viruses and attackers often take advantage of vulnerabilities in outdated software packages. Contact the software vendor directly to access any available updates.
2. **Install antivirus/anti-spyware software** to protect your computer, and to detect and remove viruses. Make sure your software is up-to-date, new viruses appear daily.
3. **Install software for spam filtering and spam blocking**. Don't respond to "spammed" emails.
4. **Do not open email offers from a source you don't recognize**. If you believe an email is fraudulent, don't reply to the email, click any links within the email, or open any attachments.
5. **Beware of any email or pop-up messages declaring your account is in jeopardy or asking for personal information.** Your credit union will never ask for personal information via email. When in doubt, call or visit your local branch with any questions.
6. **Do not click the links in suspicious emails**. If an email seems suspicious, don't click the link asking to be taken off the sender's list. A response only confirms the accuracy of your email address and may result in even more messages filling up your inbox.
7. **Never submit your credit card details or other personal information on non-secure websites**. Before submitting your user name and password to log on, make sure your browser window displays the closed padlock symbol and that the URL begins with "https://". Secure web pages show a locked padlock icon that appears in yellow, or in a yellow box, at the bottom of the web browser screen.
8. **Never share your user names and passwords or store them on your computer**.
9. **Be cautious when using public computers or shared computers**. Public computers, including those at libraries, internet cafés, and schools are traditionally on open networks and can be susceptible to monitoring without your knowledge.
10. **Always log out when you are finished**. After you've accessed sensitive account information online, log off the website and close your web browser.

## 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

Martin Luther King, Jr. Day
Monday, Janaury 16

Presidents' Day
Monday, February 20

Memorial Day
Monday, May 29

Independence Day
Tuesday, July 4

CO-OP SHARED BRANCH℠

EQUAL HOUSING OPPORTUNITY

NCUA

Federally Insured by NCUA

# Six Scams to Watch Out For This Winter

Nowadays, "You better watch out" isn't just about Santa Claus coming to town. It's also a heads-up about scammers whose Grinch-like efforts to grab money and identities tend to multiply at this time of year. Here are six kinds of scams to beware of— online, on the phone, or in person:

1. **Charity scams: "Help those less fortunate than you!"** These scams usually take the form of a phone call asking for a holiday contribution to benefit military veterans, firefighters or police, needy children, or victims of a natural disaster. The caller may solicit a credit-card donation before you have time to check out the request.

   While some of these appeals are legit, the cost of telemarketing means that, at best, only part of your donation will ever reach the charity. To protect yourself, say, "I don't make financial decisions over the phone." Hang up and visit the charity's website, give.org, or charitynavigator.org so you can decide whether or not to donate directly.

2. **Utility scams: "We'll have to shut off your service unless you pay your overdue balance right now."** The threat of being without power, gas, or water in cold weather can scare anyone. But don't rush to buy a prepaid gift or debit card, which is often how these fraudsters want to be paid. Instead, check your utility account status directly by phone or online. If you're indeed in arrears, you'll be given weeks or months of notice before a shutoff.

3. **Medicare scams: "We're updating our records and need to verify that you're enrolled."** What these crooks want is your Medicare number, which is the same as your Social Security number. With it, they may succeed in taking out new loans in your name and ruining your credit. Also beware of bogus health care providers who say you owe them money, or insurers who demand to be reimbursed for an "overpayment."

4. **Tax scams: "You owe a penalty because of the Affordable Care Act."** The complexity of the ACA, also known as ObamaCare, has inspired a new version of the imposter-IRS agent scam. In a phone call or an email, you're notified that you owe a tax penalty because you didn't have proper health care coverage last year. You're told to send a check made out to "I.R.S." or a prepaid gift card. (In reality, the IRS doesn't accept gift cards. And checks should be made out to "United States Treasury.")

5. **Contractor scams: "Get a special price if you pay in advance."** Sounds good— but once the helpful stranger pockets your payment and drives off in his plow truck, you won't see him all winter. Other drive-by scammers may offer to fix your roof ("With those old shingles, you'll have ceiling leaks by spring,") or your furnace ("How long has your chimney been putting out that funny-colored smoke?"). Don't agree to anything, no matter how sweet the deal sounds. Take down their contact information, then ask a contractor you trust for a second opinion.

6. **Investment scams: "This risk-free investment pays high returns—guaranteed."** If you're invited out of the blue to a financial seminar that includes a free lunch, go for the food— not the advice. According to the AARP Bulletin, you're likely to be pitched such "unsuitable if not bogus investments" as oil and gas, precious metals, promissory notes, life settlements, and long-maturity annuities. For better advice tailored to your situation, find a fee-only financial planner at napfa.org or garrettplanningnetwork.com.

If you've been scammed, notify your police department. It's better, of course, to avoid becoming a victim. Stop in and talk to us if you've been approached with an unusually good deal or an urgent demand. We may be able to help you discover if it's from a legitimate source. With a little research, just like Santa, you're gonna find out who's naughty or nice.

## How To Shield Yourself from Scams

**Email and Text:** If you receive an unexpected message demanding prompt action, don't click on links, open attachments, or respond using "Reply To." These actions could install malware on your device. If you need to follow up, contact the supposed sender via an email or text address or a phone number you know to be legit. Delete the suspicious message.

**Phone:** Caller ID can be hacked, so don't assume you've really been contacted by the "Internal Revenue Service" or "Red Cross." If you didn't initiate the call, don't give out your Social Security number or bank card details. Instead, ask the caller to mail you the info they want you to act on. (Real scammers won't follow up, since mail fraud is a federal crime.)

**In Person:** Put on the brakes. Don't let yourself be scared into a financial decision you'd avoid if you were calmer. If the person on your doorstep keeps trying to argue you into acting now, close the door and call the police. It's not rude to protect yourself from being taken advantage of.

Sources: Sid Kitchheimer, "Beware Fall Scams," *AARP Bulletin*, 10/15; and Laura Saunders, "The New IRS Email Scam," *The Wall Street Journal*, 10/1-2/16