

Stay Money Smart While Traveling

When you're preparing for a trip, you likely make arrangements for someone to care for your pets and plants, tell the post office to hold your mail, and ask the neighbors to pick up any packages that arrive from other carriers. You may even set timers to turn your lights on and off at specified intervals.

These steps ensure that your home remains safe while you're gone. A few more preparations will ensure that your money remains secure.

Set a Budget

If you use cash, set a daily spending limit. Take the necessary cash with you and leave the rest in the hotel safe, either the main safe or the small safe in your room. Not only does this help you keep your vacation spending in check, it also ensures that if you lose your wallet, you'll still have funds for the rest of your trip. And always be aware of your surroundings, especially when your cash or wallet are visible.

Sticking to your budget is also important — and possibly more challenging — if you are using your debit and credit cards on the trip. Keep your receipts and ensure that you're not overspending. Consider taking only one card with you and keeping the rest in the hotel safe, just like you would with cash.

Take Advantage of Technology Tools

When you're in vacation mode, you sometimes lose track of what's happening at home — and when your bills are due. Sign up for payment reminders or automatic payments to make sure everything stays on track while you're having fun.

Also consider signing up for text alerts on your credit and debit cards. Tools such as (smsGuardian or the text alert system you use) let you know when card activity is out of the ordinary, based on the settings you choose. Additionally, be aware and able to verify charges if our fraud prevention team contacts you.

Notify Us of Your Travel Plans

One of the factors that can trigger our fraud prevention specialists is when charges are made on your card in different states or countries. You can help prevent issues with using your card while you travel by letting us know when you'll be out of town and where you will be going. Contact us at 207.794.8623 or www.lincolmainefcu.com so we can note your travel on your account.

Be aware that cards may not work in certain countries because of government sanctions, prevalence of fraud, or their own restrictions on card usage. Find out more about limits here: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/faq_10_page.aspx.

Keeping track of your funds while you travel can be easy — and these simple tips will help prevent a lot of headaches.



Products & Services

Visa® Check Cards
Direct Deposit
Payroll Deduction
On-Line Bill Pay Services
Teller-PhoneSM
Home Banking
CUE-StatementSM
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@lincolmainefcu.com
www.lincolmainefcu.com

Holidays

Independence Day
Wednesday, July 4

Labor Day
Monday, September 3

Columbus Day
Monday, October 8



Five Easy Ways to Protect Yourself from Hackers

Tired of worrying about hackers? Security experts say more people could protect their home computers by doing five simple things.

1. **Don't rely on simple passwords.** A popular password like "12345678" won't stop the typical hacker for a millisecond. Instead, use a different password for each account, combining letters, numbers, and symbols. Better yet, opt for dual-factor identification such as a password, plus a security question, or a biometric ID such as a fingerprint or retinal scan.
2. **Keep up with patches.** If you require your computer to ask before downloading a software update, be sure to permit legitimate patches that may solve a security issue. Keep your antivirus software up to date.
3. **Stop spam.** Malware that rides in on an ad or a phishing email can steal account and password data, or even take over your computer. If you need better protection, ask your tech support specialist to recommend a good web-based spam blocker.
4. **Encrypt your WiFi.** If your home network isn't password-protected, any drive-by hacker can jump onto it. To change this, enter your wireless router's IP address in your Internet browser. Log in with your user name and password, then select WiFi Protected Access (WPA or WPA2) and create a strong password for the network.
5. **Keep your online doors shut.** Marketers are touting Internet connectivity for appliances, thermostats, and other devices, but be careful what you hook up to your network. Administrative passwords may be easy to guess or hack, opening a back door into your computer files. If a device doesn't need to be online, take it off.

Last, back up your most valuable files regularly. Whether you store them on a flash drive or external hard drive or in the cloud, a hacker won't be able to rob you of important programs, photos, music, and documents. That can take away a lot of worry, too.

Experts advise creating a complex password that's unique for each online account, so hackers who gain entry to one of your accounts won't have access to others.