Lumoset

FREE ONLINE-SAFETY EDUCATION

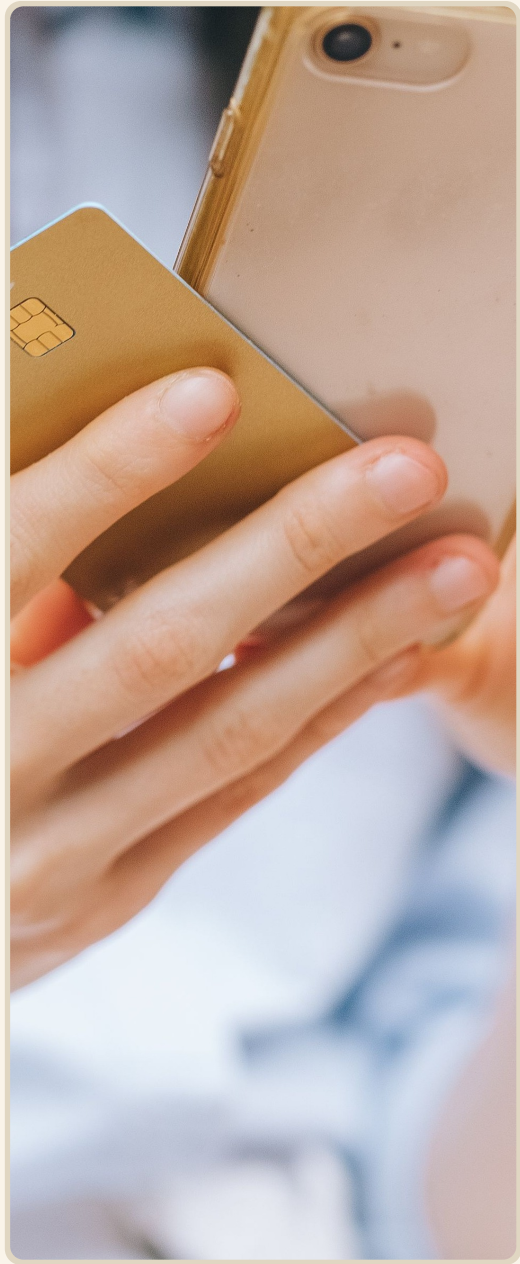
Online Banking Safety Basics

A plain-language guide to logging in safely, watching your money, and knowing what to do if something looks wrong.

A Lumoset Foundation guide · Part of the free Digital Skills series

Who it's for: anyone who is nervous about online banking, or helping someone else learn it. **Plain language, no jargon.** General education, not financial advice.

WHAT'S INSIDE THIS GUIDE



Who we are

Lumoset Foundation is a nonprofit that helps everyday people stay safe and confident online. We make clear, patient, plain-language lessons on using technology and avoiding scams, and we keep everything free, with no account and no catch. We are a registered 501(c)(3) charity based in Fort Wayne, Indiana.

Why we made this guide

Online banking can feel risky at first, but the biggest danger is usually not the bank's real app or website. The bigger risk is being tricked into a fake login page, a fake fraud-department call, or a rushed money move. This guide turns the course basics into one calm sequence: reach the bank safely, protect the login, watch the account, and respond quickly if something looks wrong.

> **Remember: Reach your bank only through the official app, a bookmark you saved on the real site, or the address you type yourself. Never through a link someone sends you.**

Jump to what you need:

Get to the Real Bank

What it is. The safest online-banking habit is choosing your own path to the bank. Use the official app you downloaded from the App Store or Google Play, or type the bank's real web address yourself.

Why it matters. Scam texts and emails often lead to fake pages that look like your bank. A padlock icon only means the connection is private. It does not prove the page belongs to your bank.

Example. A text says your account is locked and gives a login link. You do not tap it. You open your bank app directly. There is no problem. The text was bait.

Do this now

1. Download the app once from the official app store, checking the bank name as the app maker.

2. Bookmark the real website while you are already on it.

3. Before typing a password, glance at the address and make sure it is exactly your bank.

Learn it free: Money & Banking Online – Level 1: The Basics walks through the safe login habit step by step: https://lumoset.org/allcourses/money-banking-basics-online/

Lock the Account

What it is. Your bank login needs a unique passphrase and two-factor authentication. Unique means you use that passphrase nowhere else.

Why it matters. If another website is breached and you reused that password, criminals may try it on your bank. A unique passphrase plus a second login step blocks that chain.

Do this now

1. Use a long passphrase you do not use anywhere else.

2. Let your phone or browser's password manager remember it.

3. Turn on two-factor authentication. If your bank offers a passkey or authenticator app, use it. Text codes are still better than no second step.

4. Save backup codes somewhere safe.

Learn it free: Money & Banking Online – Level 1 covers passphrases, 2FA, and backup codes in plain language.

Read Balances, Transactions, and Statements

What it is. Balance is what the account shows now. Transactions or Activity is the list of money in and out. Statements are monthly summaries.

Why it matters. Checking only the balance can miss small test charges, duplicate charges, forgotten subscriptions, or cash movement you did not authorize.

Example. You see a small charge you do not recognize. It might be harmless, or it might be a test before a larger attempt. You check it instead of ignoring it.

Do this now

1. Check recent activity once a week.

2. Open statements regularly and compare them with what you remember buying or authorizing.

3. If a merchant name is unclear, check before assuming it is fine.

Learn it free: Level 1 teaches where to find balances, transactions, and statements. Level 2 goes deeper into reading statements without feeling lost.

Set Useful Alerts

What it is. Alerts are messages from your bank when something happens, like a large purchase, low balance, new login, profile change, or card-not-present charge.

Why it matters. Alerts help you notice trouble early. Early is important because banks and card issuers have formal processes for unauthorized charges, and reporting quickly protects you better.

Do this now

1. Start with a few alerts you will actually read: large purchase, new login, low balance, and profile change.

2. Treat an unexpected alert as a reason to check the account yourself through the official app.

3. Do not reply to a suspicious text alert. Open the bank app or call the number on your card.

Learn it free: Money & Banking Online - Level 2 focuses on alerts, statements, disputes, and chargebacks.

Move Money Carefully

What it is. Bill pay, transfers between your own accounts, and person-to-person payments are useful tools, but they are not all equally reversible.

Why it matters. Person-to-person payments, wires, and some transfers can be hard to reverse. Scammers exploit that by pretending to be a bank and telling people to move money to protect it.

Red flags

- A caller says to move money to a safe account.
- Someone asks for a one-time code.
- You are told to send money by Zelle, wire, gift card, or cryptocurrency to stop fraud.

Do this now

1. Set up bill pay using details from a real bill.

2. Send person-to-person payments only to people you know and have confirmed.

3. If anyone tells you to move money to protect it, hang up and call the number on your card.

Learn it free: The course shows the safe-account scam and the safe call-back habit.

If Something Looks Wrong

Even careful people run into trouble. The important part is the order: protect the account first, then document and report.

Do this now

1. Lock or freeze the card in the app if you can.

2. Call the bank using the number on your card or statement.

3. Write down the date, amount, merchant name, alert message, and who you spoke with.

4. Change the password and turn on 2FA if needed.

5. If personal information was shared, use IdentityTheft.gov. Report scams at ReportFraud.ftc.gov.

> **Remember: Lumoset teaches general education, not personal financial advice. For your specific account, your bank or credit union is the authority.**

Keep learning, free.

This guide is a companion to **Money & Banking Online - Level 1: The Basics**. The free course walks through each habit at your own pace, with a short knowledge check at the end.

• **No account. No cost. No catch.** Ever.

• Start with the course at lumoset.org/allcourses/money-banking-basics-online/.

• Know someone nervous about online banking? Please share this with them.

Key Terms in This Guide

Password Manager: A free tool, often built into your phone or browser, that creates and remembers a different strong password for every account, so you only have to remember one.

Passkey: A newer, more secure way to log in using your device's fingerprint or face scan instead of typing a password. Cannot be phished the way a typed password can.

Two-Factor Authentication (2FA): A second login step, such as a text code, an app, or a fingerprint, beyond your password. The single most effective everyday step against hacked accounts.

Sources

CISA, Secure Our World: Use Strong Passwords and Turn On MFA (cisa.gov/secure-our-world) - FTC, Lost or Stolen Credit, ATM, and Debit Cards (consumer.ftc.gov/articles/lost-or-stolen-credit-atm-and-debit-cards) - FTC, ReportFraud.ftc.gov and IdentityTheft.gov.

Help us reach one more person. Lumoset is a donor-funded 501(c)(3) nonprofit. If this helped you, you can help us teach someone else, free, at lumoset.org. Every gift keeps every lesson free.

Lend a hand. We are volunteer-powered. If you would like to help write, teach, translate, or share our free lessons, see lumoset.org.

For librarians, senior centers, and Area Agencies on Aging: please print and share this guide freely with the people you serve. That is exactly what it is for.

Did this help? Tell us at lumoset.org. Your story helps us reach more people, and shapes what we teach next.