



Online Banking Hygiene

Simple habits that keep your money — and your identity — safe online.

You don't need to be technical to bank safely online. Almost every drained account has one of a few weak spots — a reused password, a link clicked in a hurry, a code read aloud to a stranger. **Fix those, and you've closed the doors that thieves actually use.** Here are the fundamentals, in order of what matters most.

THE EIGHT HABITS THAT MATTER MOST

- 1 Use a long, unique password**
One password per account, never reused. A password manager remembers them so you don't have to — you only memorize one.
- 2 Turn on a second lock (MFA)**
Even a stolen password can't get in without your second step. Prefer an authenticator app or passkey over text-message codes.
- 3 Go straight to the source**
Type your bank's address yourself or open its official app. Don't reach your account through links in emails or texts.
- 4 Guard your one-time codes**
A code sent to log in or approve a payment is a key. No real bank employee will ever ask you to read one to them.
- 5 Mind the network**
Skip banking on public Wi-Fi at cafes and airports. Your phone's cellular data is far safer for anything involving money.
- 6 Keep your devices healthy**
Install updates promptly, lock your screen with a PIN or fingerprint, and only download banking apps from the official app store.
- 7 Watch your own account**
Turn on transaction and login alerts, and glance at your statements. You'll spot a stray charge long before anyone else would.
- 8 Log out and clean up**
On any shared or public computer, log out fully and never save your password. Better yet, don't bank on devices that aren't yours.

HOW TO SPOT A SCAM

- **Urgency or fear.** "Your account will be closed in 24 hours." Pressure is the point — slow down.
- **A request for codes or passwords.** Legitimate banks never ask for these by phone, text, or email.
- **A link that looks almost right.** Hover or read carefully — *bankofamerica* is not *bankofamerica*.
- **An unexpected contact.** A call "from your bank" you didn't expect? Hang up and call the number on your card.
- **Off details.** Odd grammar, a generic "Dear Customer," or a payment request that doesn't add up.

YOUR BANK WILL NEVER ASK YOU TO...

- Read out a one-time passcode or PIN
- Share your full password or card CVV
- Move money to a "safe account" to protect it
- Install screen-sharing software so they can "help"

IF SOMETHING GOES WRONG

1. **Contact your bank now.** Use the number on the back of your card — not one from the suspicious message.
2. **Change your password** from a device you trust, and turn on MFA if it isn't already on.
3. **Freeze or lock the card** in your banking app to stop further charges while you sort it out.
4. **Report it.** Ask the bank to flag fraud, and file a report at reportfraud.ftc.gov to protect your record.
5. **Check your other accounts.** If you reused that password anywhere, change it there too — today.

YOUR FIVE-MINUTE CHECKUP

- | | |
|---|--|
| ☐ MFA is on for your bank login | ☐ Your phone and computer auto-install updates |
| ☐ Alerts are on for transactions and sign-ins | ☐ You have the official app , not a bookmarked link |
| ☐ Your banking password is unique (used nowhere else) | ☐ You know your bank's real fraud number (it's on your card) |