Liberty Bank for Savings℠

Trust & Integrity Since1898

PROTECT YOUR IDENTITY AND YOUR MONEY

Fraud and Scam Prevention Guide

02/26

CONTENTS

Scan for Security Resources
Scan the QR code or visit https://www.libertybank.com/security-center/ for fast access to the trusted third-party cybersecurity links and tools mentioned in this brochure.

SCAM AWARENESS

Email / Phone

- Be cautious of suspicious calls or emails asking for money or personal info. Common scams include:
  - Fake charities or urgent pleas about a loved one in trouble
  - Messages from "your bank," credit card company, or the IRS
  - Prize emails that ask for payment to claim winnings - If it sounds too good to be true, it probably is
  - AI-generated voice or video messages that sound real but are unexpected or create sudden urgency
- Never click links in unsolicited emails or texts—they may lead to fake websites or install malware. Avoid opening attachments in unexpected emails.
- Delete suspicious texts. Common text scams include:
  - I-PASS: Fake toll fee notices
  - Bank alerts: Phony fraud warnings
  - Delivery scams: Fake messages from UPS, USPS, or FedEx

TIP: The IRS never contacts taxpayers via email about bills or refunds, nor does it call to threaten people with arrest or deportation. Never give out private information in response to calls that you didn't initiate.

Checks

- Don't accept an overpayment check for something you're selling. Scammers ask you to return the "extra" by wire, gift cards, or Bitcoin, then their check bounces.
- Don't accept a check from a stranger who wants you to send money elsewhere. If someone mails you a check and asks for a wire, gift cards, or Bitcoin, it's a scam.
- Don't accept a check tied to a job offer if you're asked to buy supplies or equipment upfront.
- Don't accept a check for lottery or sweepstakes winnings. Real lotteries never send checks and then ask you to pay fees or taxes.

TIP: Gift cards and Bitcoin are red-flag payment methods. If someone demands them, it's almost always a scam.

Property Fraud

Property fraud is a growing crime. Scammers place fraudulent liens against your house or file forged ownership documents to take ownership of a property—often a mortgage-free home.

Counties have responded by creating free property fraud alerts that let you know whenever a document is recorded against your property.

For more information, contact the county office where your property is located.

Cook County, 312.603.4000
DuPage County, 800.728.3858
Kane County, 630.232.5935
Lake County, 847.377.2575
McHenry County, 800.728.3858
Will County, 800.728.3858

TOUGH PASSWORDS

Create tough passwords. Your pet's name followed by 123 isn't secure. Nor is "banklogin123."

- Never use a password that includes names, numbers, or information someone could link to you.
- The most secure passwords are non-personal phrases of 16 characters or more. (Example: Theoceanispurple!)
- Change passwords regularly, and update your email password (e.g., Gmail, Yahoo) immediately if you suspect any attempted fraud.
- Don't recycle passwords and don't use the same password for multiple sites.
- If you need to write down a username and password, keep it in a secure location accessible only to you.
- Don't share your bank account's User ID and Password with third-party websites or software applications designed for budgeting, managing accounts, or tax preparation. Doing so can put your privacy and money at risk.

If you've accidentally shared your Liberty Bank User ID and Password, or believe this information has been stolen, contact Liberty Bank at 773.384.2030.

MULTI-FACTOR AUTHENTICATION

Also known as MFA, multi-factor authentication requires a second step—adding a PIN, fingerprint or facial recognition—beyond your username and password to access websites. The aim is to make it more difficult for thieves to break in.

- It's smart to use MFA for email, banking, shopping, social networks, password managers, cloud storage, and productivity apps.
- All Liberty Bank accounts are protected with MFA. To learn more, search for "one-time passcodes" on https://www.libertybank.com/.
- To learn more about setting up MFA on all your online accounts, visit https://www.cisa.gov.

BIOMETRICS

Biometric authentication—like fingerprint scans and facial recognition—is commonly used to verify identity, especially in smartphones, banking apps, and secure facilities.

While convenient, unlike a password or account number, biometric data can't be changed or reissued if compromised. That makes secure storage and responsible use especially important.

Before enabling biometric features, especially with third-party apps or services, be sure you understand how your data will be stored and protected.

CHECKS

- Don't write or imprint your phone, social security or driver's license number on your checks.
- Store unused and canceled checks in a secure location.
- When ordering new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

  You can request that your check order is delivered to your branch and we will call you when they are available for pickup.

- Shred cancelled checks before disposing of them.

  If you think your checks have been stolen or you've lost them, call Liberty Bank at 773.384.2030.

ATM / DEBIT CARDS

- Use secure PINs and passwords. Never use birth dates, social security or driver's license numbers, or your house address.

If you're heading out of town—especially internationally—and plan to use your debit card, give us a quick heads-up. Call 773.384.2030 or set a travel alert using Card Control in our mobile app so your card works without interruption.

- Never share your personal identification number (PIN) with anyone.

If you've inadvertently shared your PIN or it's been compromised, contact Liberty Bank at 773.384.2030.

- Keep your debit card and your PINs in a secure location.

If you believe your debit card has been lost or stolen, please call Liberty Bank during regular business hours. After business hours, call our 24-hour debit card services line at 800.472.3272.

- Never write your PIN on your debit card or store it in the same place where you store your card.
- Be wary about entering payment information in online merchant websites, since many may not be secure.
- Shred ATM and debit card purchase receipts.
- Before inserting your card into an ATM, examine the card reader. Don't use it if it looks like the reader has been glued or taped to the machine, or feels loose. Thieves may have installed a "skimmer" in hopes of stealing account and personal information.
- Don't accept offers of assistance from anyone you don't know when using an ATM, including people who say they are there to help because the ATM is broken
- When using an ATM, for your personal safety, choose an ATM in a well-lit, public location.

Stay in control with Card Control: Instantly lock or unlock your debit card and manage how, when, and where it's used—adding an extra layer of protection against fraud. Learn more at https://www.libertybank.com.

MOBILE BANKING

Your phone contains loads of personal information that needs protection.

- Use a password to access your phone.
- Use remote wipe if your phone is lost or stolen.
- Be wary about storing usernames and passwords on your phone for retail sites and mobile banking apps.

- Always use official app stores to download any app.
- Don't tamper with your phone's operating system because this can disable your phone's security features.
- Don't let other people, especially someone you don't know and trust, use your phone or mobile device.
- Be sure no one is looking over your shoulder in public areas and reading information from your device's screen.
- Sign out of applications and lock your phone whenever you've completed a task.
- Don't send personal information over a public wireless network (Wi-Fi) in coffee shops, libraries, airports, hotels, etc.
- Don't store your passwords on your mobile device, such as in a note-taking app.
- When you dispose of your old mobile phones, remove the SIM card and do a master reset to wipe out all the stored data.

ONLINE BANKING

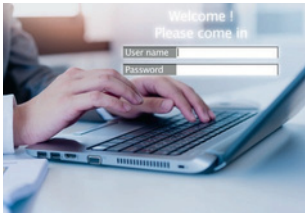
- Use up-to-date computer operating systems and browsers. Also install the latest security patches on your computer and keep anti-virus and firewall software up to date.

Find information about up-to-date operating systems and browsers at https://www.cisa.gov.

- Don't let others, especially someone you don't know and trust, use your personal computer.
- Sign out of or lock your computer whenever you leave it.
- Sign onto online banking accounts regularly to review your activity.

If you notice suspicious activity, contact Liberty Bank immediately at 773.384.2030.

- When disposing of your old computer equipment, first destroy the data on the computer's hard drive. The best way to do this is to physically destroy the hard drive.



EMAIL

- Don't send confidential information, such as your social security number or account numbers through unsecure email, text, or other messaging systems.

You can communicate securely with Liberty Bank by calling 773.384.2030, or by using a secure form on our website at https://www.libertybank.com/contact.

- Don't open email attachments or click on links in emails—even if they seem to be from someone you know—unless you're expecting them or you're confident that they are legitimate.
- Be especially suspicious of emails with:
  - Subject lines containing a general message like thought you'd be interested" or "per your request."
  - Misspellings or grammatical errors.
  - A demand for immediate response (because of an account problem, a need to update records, or any other source of urgency).
  - A request that you provide confidential information such as account numbers, passwords, or social security numbers.
  - A claim that you have won something, are owed something, or have money coming to you.
  - An emergency request from a friend who's in jail, stranded at the airport or needs cash immediately.

If you receive a suspicious email that claims to have come from Liberty Bank or simply wish to confirm that an email actually came from Liberty Bank, please call 773.384.2030.

WEBSITES

- Don't enter information into a website unless the URL in the address bar of your internet browser starts with https://. The letter "S" signifies that the website is using Hypertext Transfer Protocol Secure (HTTPS), a communications protocol for secure communication.
- Read the website's privacy policy to be sure you're comfortable with how your data is collected and used and what security measures will be implemented to keep your private data safe.

See Liberty Bank's Privacy policy at https://www.libertybank.com/privacy.

SOCIAL NETWORKING SITES

- Limit access to your networking pages to a small group of trusted people.
- Don't post too much personal information that an identity thief can use to answer "challenge" questions on your accounts.
- Do not announce your vacation plans and consider postponing posting vacation photos until you have returned home.

PHONE CALLS

- Be wary about answering calls from unrecognized numbers, especially "robo calls," because they're frequently scams.
- Don't disclose personal or financial information over the phone, unless you placed the call and are certain of the identity of the person or company you're talking to.

Liberty Bank will never call you and ask you for personal or financial information. If you receive what you believe is a suspicious phone call that purports to have come from Liberty Bank, or simply wish to confirm it came from Liberty Bank, please call 773.384.2030.

SNAIL MAIL

- Shred statements or invoices that you don't want to keep and credit card or other financial offers that don't interest you.

Keep an eye out for Liberty Bank shred event announcements or visit https://www.libertybank.com/events.

- Opt out of prescreened credit card and insurance offers.

Call 1.888.567.8688 to opt out or visit https://www.optoutprescreen.com.

- Sign up for the USPS Informed Delivery® tool to track incoming mail and help prevent mail theft: https://www.usps.com.
- Drop outgoing mail into a U.S. Postal Service collection box instead of leaving it in your mailbox, where items can be stolen.
- If you don't receive one of your regular bills, notify the company. A common identity theft scam entails changing a victim's mailing address.
- If bills include suspicious charges—even ones for $1—or you see purchases you didn't make, notify the company immediately.

If you get what you believe is a suspicious mailing that claims to be from Liberty Bank or you want to confirm that something is from us, please call 773.384.2030.

SAFE DISPOSAL

- Shred credit card applications, bank and credit card statements, and anything containing account or social security numbers.
- Before disposing of a mobile phone, remove the SIM card and do a master reset to wipe out all stored data.
- Before throwing out computers and other electronics, wipe away your personal data.

Tip: Liberty Bank regularly holds shred events. Keep an eye out for event announcements or visit https://www.libertybank.com/events.

LIBERTY BANK'S SECURITY MEASURES

Liberty Bank relies on a wide range of security tools to constantly keep an eye on your accounts and keep your information safe. Learn more at https://www.libertybank.com/security-center.

You also can takes steps to increase safety, including:

- Using Liberty's account and VISA® purchase alerts to keep track of account activity and purchases on your debit card.
- Advising Liberty Bank if you'll be traveling and using your debit card – you can set a quick travel advisory directly in our Mobile App's Card Control feature.
- Understanding that Liberty Bank will never call and demand personal information like social security or account numbers.

CREDIT

Request a free annual credit report from each of the 3 national credit reporting agencies and look for credit inquiries from unfamiliar companies, accounts you never opened and unexplained debts.

You can obtain free copies at https://www.annualcreditreport.com or by calling 1.877.322.8228. You can also request the reports by contacting each of the agencies directly.

- Equifax: 1.888.378.4329
- Experian: 1.888.397.3742
- TransUnion: 1.800.680.7289

Create security freezes—sealing your credit report so others can't establish credit in your name—through the three credit reporting agencies to reduce your risk of identity theft.

Contact each agency to establish a freeze. You can always thaw your account—temporarily allowing an agency to release information—when you're applying for credit.

- Equifax—1.888.298.0045 or https://www.equifax.com/personal/credit-report-services/credit-freeze/
- Experian—1.888.397.3742 or https://www.experian.com/help/credit-freeze/
- TransUnion—1.833.806.1627 or https://www.transunion.com/credit-freeze

Find out about credit freezes at consumer.ftc.gov/articles/credit-freeze-or-fraud-alert-whats-right-your-credit-report.

In addition, consider using an identity theft credit monitoring service that keeps tabs on your credit and notifies you when it spots signs that an identity thief may be trying to use your personal data (https://consumer.ftc.gov/articles/what-know-about-identity-theft#services).

ADDITIONAL RESOURCES

Visit the Federal Trade Commission website to learn about identity theft, report identity theft, and keep up on the latest scams (https://consumer.ftc.gov).

The site also includes a list of signs that you may be an identity theft victim:

- You see withdrawals from your bank account that you can't explain.
- You stop getting your bills or other mail.
- Debt collectors call about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.

11/2025