Protecting Your Finances

Borrower Success Series
Banking Security & Cybersecurity Basics
for New Business Owners

You closed your loan. Congratulations! Now you're making real transactions: paying vendors, receiving deposits, and repaying your lender. That activity makes your business accounts a target. This guide covers the financial security basics every new borrower should know, and the steps you can take right now to protect yourself.
The good news: most of the tools you need already exist at your bank. You just have to ask for them.

Your First Conversation with Your Banker: Security Setup

When most people open a business account, they focus on deposits and checks. But your bank offers fraud prevention tools, but not all are turned on by default.
Schedule time with your banker and ask this directly:

"What fraud prevention tools do you offer on business accounts, and which ones are active on mine right now?"

Ask about each of the following:

- Transaction alerts: real-time notifications for every debit, wire, and ACH. Most banks offer this free.
- Daily transaction limits: ask what your default limits are. They're often set higher than a small business needs.
- Positive Pay (check and ACH): you provide a list of authorized payments; your bank flags anything that doesn't match.
- Dual authorization: requires two people to approve large transfers. Strong protection even for small teams.
- Wire transfer callback procedures: your bank's process for verifying wire requests by phone before they go out.
- Dispute and reversal windows: ask specifically how long you have to dispute each type of transaction (ACH, wire, and check all have different rules).

Business Email Compromise: The #1 Financial Threat to New Businesses

Business Email Compromise (BEC) (or Phishing) is the most common way small business owners lose money. A scammer impersonates someone you trust such as a vendor, your banker, even your own email, and asks you to wire funds or change payment instructions. These transfers are often sent to cryptocurrency wallets within minutes, making recovery nearly impossible.
BEC losses totaled $2.7 billion in 2022 alone, affecting businesses of every size.

The Golden Rule: Before sending any wire or changing any payment instructions, call the requestor directly using a phone number you already have on file, not one provided in the email or text.

Red flags to watch for:

- An email requesting urgent wire transfer or payment instruction changes
- A message that says the sender is traveling and can't be reached by phone
- An email address that looks right but is slightly off (one letter changed, a number added)
- Any request to bypass your normal payment approval process

Your Loan Payment Is a Security Target

When you're actively repaying a loan, you're making recurring, predictable, large transactions. That pattern is known to fraudsters. Here's what to watch for:

- Loan servicer impersonation: fraudsters send fake "payment instructions update" notices that look like official bank correspondence. Never change where you send your payment based on an email alone.
- If your loan is sold or transferred to a new servicer: (This happens.) Verify the legitimacy of the new entity through your original lender or the SBA directly before sending any payment.
- Never change autopay or ACH instructions based on a phone call or email. Always verify through your bank's official portal or in person.
- Your lender will never ask you to confirm account numbers, passwords, or login codes via text or email. If you receive this, call your bank using the number on their official website.

Protecting the Financial Documents You Send Your Bank

During your first two years, you'll regularly send sensitive documents to your lender such as tax returns, financial statements, and other reports. A few rules:

- Never send financial documents over regular email. Ask your banker how they prefer to receive documents securely. Most banks have a secure portal for this.
- If you use a bookkeeper or accountant, they should access your bank data through read-only tools (like Plaid or a bank-issued accountant login) — not your personal username and password.
- Monitor who has access to your accounts. Review authorized users at least once a year and remove anyone who no longer needs it.
- Keep your business account completely separate from personal accounts. Commingling creates both security and legal exposure.

If Something Goes Wrong: Act Fast

Time is the single biggest factor in recovering from financial fraud. Here's what to do:

Situation	What to Do
Unauthorized Transaction	Call your bank's fraud line immediately. Ask about the reversal window for that specific transaction type. ACH, wire, and check all have different timeframes.
Online Banking Compromised	Call the bank first. Freeze online access, then change credentials from a clean device, not the device you think was compromised.
Fake Loan Correspondence	Report to your bank, and to the SBA Office of Inspector General (sba.gov/oig) if it involves an SBA loan. Also report to the FTC at reportfraud.ftc.gov.
Wire Fraud	Report to the FBI Internet Crime Complaint Center (IC3.gov) within hours. The FBI's Financial Fraud Kill Chain is a rapid-response process that works with banks to freeze and potentially recover wired funds, but only if you report fast.

Free Resources Worth Bookmarking

Resource	What It Offers
SBA.gov/cybersecurity	Free cybersecurity tips, loan fraud prevention, and identity theft reporting.
CISA.gov	Free vulnerability scans, checklists, and fraud prevention tools specifically for small businesses.
IC3.gov	FBI Internet Crime Complaint Center where you can report wire fraud and cybercrime.
FTC.gov/smallbusiness	Guidance on avoiding scams and the Red Flags Rule for identity theft.
NACHA.org	Best practices for ACH payment security.
reportfraud.ftc.gov	Report fraud, scams, and fake loan correspondence.

Questions? Let's Talk.

This is one piece of a larger Borrower Success program designed to help you stay financially healthy throughout your loan. Your SBDC advisor is available to walk through any of this with you one-on-one, at no cost. Contact your SBDC consultant to schedule a meeting.

West Central MN SBDC and the Minnesota SBDC Network is a proud part of the Department of Employment and Economic Development in the State of Minnesota. It is funded in part through a Cooperative Agreement with the U.S. Small Business Administration. All opinions, conclusions, and/or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the SBA.
To request an accommodation or discuss accessibility needs, please contact (218) 299-6605 in advance to allow adequate time for coordination.