

FRAUD & SCAM GUIDE



Smart ways to protect your money, identity, and peace of mind.

Brought to you by Minster Bank—Bank Close. Go Far.



Phishing & Fake Emails

SCENARIO: You receive an email saying your bank account has “unusual activity” and you must click a link to verify. The webpage looks real, but it’s a scam—and entering your info gives the scammer full access.

WATCH FOR: Urgent language, unknown senders, requests for login details or verification codes.

PROTECT YOURSELF: Never click unexpected links. Go directly to the official website or mobile app.



Online Marketplace Scams

SCENARIO: You sell a textbook online. The buyer “accidentally” overpays and asks for a refund through Zelle. Their original payment later disappears, and you’re out the money.

WATCH FOR: Overpayments, pushy buyers, fake screenshots of payments.

PROTECT YOURSELF: Meet in public places, avoid instant payments to strangers.



Text Message Scams (Smishing)

SCENARIO: You receive a text that says, “Your debit card has been locked. Tap here to reactivate it.” The link leads to a fake login page designed to steal your information. Other examples may include:

- ◆ “Package delivery failed—update your address.”
- ◆ “You’ve won a prize! Claim it here.”
- ◆ A verification code you didn’t request.

WATCH FOR: Unknown numbers, urgent wording, links asking you to “fix” something, fake alerts pretending to be Amazon, Apple, UPS, or your bank.

PROTECT YOURSELF: Don’t click links or reply. Verify everything by logging into your banking app or trusted website.



Rideshare Scams

SCENARIO: A car pulls up claiming to be your driver and asks you to cancel the ride and pay them directly.

WATCH FOR: Cars not matching the app, drivers requesting off-app payments or QR code scans.

PROTECT YOURSELF: Confirm the driver’s name, photo, and license plate in-app before getting in.



Venmo & Zelle Safety

SCENARIO: Someone pretending to be a friend asks you to send money to a “new account.” Later you learn their real account was hacked—and the message wasn’t from them.

WATCH FOR: Unexpected payment requests, urgency, usernames that don’t match.

PROTECT YOURSELF: Only send money to people you’ve confirmed directly.



Social Media & Influencer Scams

SCENARIO: You get a DM from someone claiming to be a brand ambassador who wants to send you money — “just send \$50 first.” You never hear from them again.

WATCH FOR: Cash-flip posts, impersonated accounts, fake giveaways, friends asking for verification codes.

PROTECT YOURSELF: Contact the person through another method to confirm it’s really them.



FRAUD & SCAM GUIDE



Re-Shipping Scams

SCENARIO: A “job” offers to pay you for receiving and re-mailing packages. The items are stolen, and your address is used for fraudulent activity.

WATCH FOR: Jobs involving mailing packages from your home.

PROTECT YOURSELF: Real employers don't operate this way.



PayPal Scams

SCENARIO: You get a fake email saying there's a large payment on your account and you must “verify” it through a link.

WATCH FOR: Fake invoices, refund requests, links to login pages.

PROTECT YOURSELF: Always check your PayPal app directly.



Roommate & Rental Scams

SCENARIO: A landlord asks for a deposit via Venmo before you've seen the apartment. After you pay, they disappear.

WATCH FOR: Prices too good to be true, refusal to meet or show the property, requests for gift card or payment app deposits.

PROTECT YOURSELF: Verify ownership, request a live video tour, never pay before seeing the place.



Behavior Blackmail (Sextortion)

SCENARIO: Someone online convinces you to send intimate images, then threatens to share them unless you pay.

WATCH FOR: Requests for personal content early in conversations, threats, refusal to video chat.

PROTECT YOURSELF: Stop communication immediately. Save messages, tell a trusted adult, and contact law enforcement if threatened.



Amazon Scams

SCENARIO: You get an email stating your order is shipping — but you never placed one. Clicking the link opens a fake Amazon sign-in page.

WATCH FOR: Fake confirmations, unusual account activity messages, requests for payment by gift cards.

PROTECT YOURSELF: Log in through the official Amazon app or website.



Fake Apple Pay Scams

SCENARIO: You're selling something online, and the buyer sends a fake Apple Pay “receipt.” They ask you to refund part of the money, but the payment was never real.

WATCH FOR: Payment screenshots, requests for partial refunds, pressure to act quickly.

PROTECT YOURSELF: Check your Wallet app—if the payment isn't there, it doesn't exist.



Identity Theft

SCENARIO: Your mail is stolen or your info is taken from a public Wi-Fi network. Weeks later, a credit card you never opened appears on your credit report.

WATCH FOR: New accounts, credit declines, unfamiliar mail.

PROTECT YOURSELF: Monitor your credit regularly using Credit Sense, avoid public Wi-Fi for financial activity, and shred sensitive documents.



Scholarship, Internship & Job Scams

SCENARIO: You get offered a job with great pay for little work—but they want your bank information upfront for “direct deposit.”

WATCH FOR: Jobs that sound too good, employers who won't meet, requests for personal info before hiring.

PROTECT YOURSELF: Research employers and never pay for job placement.



Student Loan & Financial Aid Scams

SCENARIO: A message promises guaranteed student loan forgiveness for a fee. You pay—but nothing happens.

WATCH FOR: Upfront fees, “guaranteed approval,” unofficial websites.

PROTECT YOURSELF: FAFSA and loan assistance don't cost money.



BANKING & CREDIT PROTECTION

Protecting your finances doesn't have to be complicated. Follow these simple steps to help keep your money and identity safe—because a little awareness goes a long way in stopping fraud and scams before they start.



Set Up Account Alerts

Inside your mobile banking app, turn on:

- ◆ Large purchase alerts
- ◆ Low balance alerts
- ◆ Card-not-present transactions
- ◆ Login alerts
- ◆ ATM withdrawal alerts

These help you catch fraud early and respond quickly.



Quick Safety Checklist

- ◆ Trust your instincts—pause before acting
- ◆ Never share verification codes
- ◆ Avoid public Wi-Fi for banking
- ◆ Use strong, unique passwords
- ◆ Turn on all available alerts
- ◆ Limit what you share online
- ◆ Confirm payment requests through another channel



Use Free Credit Monitoring (Credit Sense)

With Credit Sense, you can:

- ◆ Track your credit score
- ◆ Catch new accounts in your name
- ◆ Monitor changes in real time
- ◆ See personalized tips for improving your credit



If You Think You've Been Scammed

- ◆ Contact your bank immediately
- ◆ Freeze your card
- ◆ Change your passwords
- ◆ Take screenshots of messages
- ◆ Report it to campus security or local police
- ◆ Review your Credit Sense alerts for new activity

Have questions? Want help setting up alerts?

Our team is here for you. Contact us at minsterbank.com or 866.646.7837. Scan the code to watch a quick, alert set-up video. Power up your financial knowledge even further by downloading Zogo—our free gamified financial learning app. Use code **MNSTR** to get started.

