COMMON SCENARIOS

PHONE & TEXT SCAMS / PROTECT YOUR MOBILE DEVICE

ONLINE & EMAIL SCAMS / PAYMENT APP SCAMS / ELDER ABUSE

IDENTITY THEFT RECOVERY PLAN / EDUCATION

REPORTING A LOST CARD / FRAUD / RESOURCES

OVERVIEW / TOOLS & FEATURES

FRAUD PREVENTION

THERE'S ONLY ONE **YOU.**

DACOTAH BANK®

DACOTAH BANK

Safe & secure banking is our focus

Identify theft and fraud is rapidly growing. Together, we can protect your confidential information so you can bank with ease. Our dedicated Risk and Fraud Team is working to protect your identity and financial information.

Bank fraud detection and prevention refers to the collective policies, protocols, procedures, and technologies financial institutions leverage to protect their assets, systems, and customers against fraud. Detection includes any activities related to threat monitoring, account monitoring, behavioral profiling, and proactive risk identification. On the prevention side, it includes any proactive measures related to threat mitigation, such as developing internal controls, conducting employee training, and implementing multi-layered security.

Dacotah Bank is committed to bank fraud detection and prevention. From extensive training with our employees and customer education, to multi-layered security systems and monitored databases of known threats, our Risk and Fraud Team is on the lookout for active and emerging threats 24/7.

By collecting fraud data from internal and external sources, banks can gain a comprehensive view of the fraud landscape and make more informed risk decisions. Dacotah Bank uses internal and external resources to support fraud awareness training so employees recognize a broader range of potential threats.

Together, we are working to protect your identity and personal information with financial fraud detection and prevention strategies so you can bank securely, conveniently and confidently.

For more information, please call (800) 881-5611 Extension 6315 Option 1.



Tools and features to fight fraud

Dacotah Bank has a multitude of measures in place to protect your confidential, personal, and financial information to include:

Debit and Credit Card Fraud Text Alerts

To enhance account security and provide peace of mind, Dacotah Bank offers personalized instant notifications. Stay informed about account changes, such as online transactions, password modifications, and low funds through text, email, or phone calls. Simply add alerts in the Settings section of the Dacotah Bank App to get started.

Card Control Center

You have uncompromising fraud protection with Card Control Center. Available right within your online banking experience and mobile app tools, you can report lost or stolen cards in a couple of clicks, as well as immediately turn off a lost or stolen card.

EMV Chip Card

Get BIG protection in a tiny chip! Dacotah Bank's Visa Debit and Credit Cards now feature EMV chip technology! Our free Visa Debit Card offers zero liability against fraud and identity theft.

Duplicate Detection

Risk and Fraud Analytics for Online Banking

Positive Pay for Business Customers

Positive Pay is a powerful check and ACH fraud prevention tool and comprehensive check management system for your business. It is simple, safe, secure and web-based.



Lost or stolen card?

If your Dacotah Bank credit card or debit card is lost or stolen, please call the appropriate number below.

Dacotah Bank Credit Card **(800) 558-3424**

Dacotah Bank Visa Debit Card

(800) 881-5611 ext. 3120
7:30am-7:00pm (CT) Monday - Friday
9:00am-1:00pm (CT) Saturday
(800) 554-8969 – After Hours

When your debit card expires, Dacotah Bank will mail you a new one. If a replacement card is not received before the expiration date listed on your current card, call (800) 881-5611, extension 3120.

Suspicious Activity? **(800) 881-5611** extension 6315, option 1

Elder Abuse? **(800) 881-5611** extension 6315, option 1



Resources

If you are the victim to fraud, please contact the applicable organization below. If you are the victim of identity theft, please review the Identity Theft Recovery Plan on page 6 for more information.

Agencies & Businesses

Identity Theft Resource Center 1-888-400-5530
www.idtheft.org (Victim Assistance Center - speak with a Victim Advisor for free)
IRS Identity Theft Hotline 1-800-908-4490, To report Tax Fraud or Identity Theft
Social Security 1-800-772-1213
Medicare 1-800-633-4227
CFPB Consumer Financial Protection Bureau 1-855-411-2372

Credit Bureaus for Fraud Alerts

Equifax Fraud Assistance Service Center 1-888-766-0008
Experian 1-888-397-3742
TransUnion 1-800-680-7289

To obtain a copy of your free credit reports from Equifax, Experian and TransUnion:
Annual Credit Report 1-877-322-8228, annualcreditreport.com

Reporting scams

Internet Crime Complaint Center www.IC3.gov
Federal Trade Commission 1-877-438-4338, www.ftc.gov
AARP Fraud Watch Helpline 1-877-908-3360
National Fraud Information Center www.fraud.org
Anti-Phishing Work Group www.antiphishing.org
US Postal Inspection Service 1-877-876-2455

Opting out / do not call

Do Not Call Registry 1-888-382-1222, www.donotcall.gov
Email List Removal Service dmachoice.thedma.org
Prescreened Credit/Insurance Opt Out 1-888-567-8688, www.optoutprescreen.com



Identity Theft Recovery Plan

What to do right away

Is someone using your personal information to open new accounts, make purchases, or receive a tax refund? Report it at IdentityTheft.gov and get a personal recovery plan.

STEP ONE: Call the companies where you know the fraud occurred.

- Ask for their fraud department. Explain that someone stole your identity.
- Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- Change logins, passwords, and PINs for your accounts.

*You might have to contact these companies again after you have an Identity Theft Report.

STEP TWO: Review your credit report, and add fraud alerts.

- To place a fraud alert, contact one of the three credit bureaus listed below. The fraud alert is free of charge, and you will receive a letter from each bureau confirming a fraud alert was created.
    - Equifax: 1-888-766-0008 // Equifax.com/CreditReportAssistance
    - Experian: 1-888-397-7289 // Experian.com/fraudalert
    - TransUnion: 1-800-680-7289 // TransUnion.com/fraud
- To obtain a copy of your free credit report, go to annualcreditreport.com or call 1-877-322-8228.
- If you already ordered your free annual report this year, you may pay to obtain your report immediately or follow the instructions in the fraud alert cofirmation letter from each credit bureau to request a free report, which may take longer to receive.
- Review your reports and make note of any account or transactions you do not recognize. This will assist in reporting identity theft to the Federal Trade Commission (FTC) and local law enforcement.

STEP THREE: Report identity theft to the FTC.

- Based on the information entered, IdentityTheft.gov will create your Identity Theft Report and recovery plan. Include as many details as possible.
- If you create an account, the FTC will explain each recovery step, update your plan as needed, track progress, and pre-fill forms and letters. If you do not create an account, you must print and save the Identity Theft Report and Recovery Plan. Once you leave the page, you cannot access or update the Report.
- Visit IdentityTheft.gov and click Get Started or call 1-877-438-4338.

STEP FOUR: File a report with your local law enforcement.

- Provide law enforcement with:
    - A copy of your FTC Identity Theft Report
    - A government-issued ID with a photo
    - Proof of your address (mortgage statement, rental agreement, or utilities bill)
    - Any other proof you have of the theft (bills or IRS notices)
    - The FTC's Memo to Law Enforcement (available at IdentityTheft.gov)
- Obtain a copy of the police report. You will need this to complete other steps.
- Create your Identity Theft Report by combining your FTC Identity Theft Report with your police report. The Identity Theft Report proves to businesses that someone stole your identity. It also guarantees you certain rights.

Educate and protect yourself

Be aware of phishing attempts in emails, calls and texts with the following requests:

- They ask you to open a link.
- They use urgent or fear-inducing language.
- They send an attachment.
- They request personal info including PINS, passwords or social security numbers.
- They pressure you to log into or send money with payment apps.
- They pressure to to move money to a different institution, to "protect your funds".

Top reported cyber-scams as reported by Federal Trade Commission

#1 Imposter scams
Imposter scams remained the top fraud category with reported losses of $2.7 billion. These scams include people pretending to be your bank's fraud department, the government, a relative in distress, a well-known business, or a technical support expert.

#2 Investment scams
While investment-related scams were the fourth most-reported fraud category, losses in this category grew. People reported median losses of $7.7K – up from $5K in 2022.

#3 Social media scams
Scams starting on social media accounted for the highest total losses at $1.4 billion – an increase of 250 million from 2022. But scams that started with a phone call caused the highest per-person loss ($1,480 average loss).

#4 Payment methods
Scammer preferred victims pay with bank transfers and person-to-person payments, which accounted for the highest losses ($1.86 billion). Cryptocurrency losses were a close second at $1.41 billion reported in losses.

#5 Losses by age.
Of people who reported their age, younger adults (20-29) reported losing money more often than older adults (70+). However, when older adults lost money, they lost the most.



Computer and internet fraud

Online scams

Many people store a wealth of information on their personal computers, including financial information. This makes your computer a great target and the common access point is the internet. Protect your data and confidential information by following the steps below.

- Keep your computers up-to-date, your anti-virus protection is updated, and secure the internet connection.
- Make your passwords long, strong and unique. Know who has access to your devices, and never reuse your passwords. If your password is compromised they now have access to any application with the same password.
- Set your browser security to highest and most secure settings. Enable pop-up blockers, and use caution when installing software.
- Back up your data regularly, and use virus protection on all devices.
- Wipe your computer or mobile device before you donate, sell or trade it.

Email scams

Phishing emails attempt to trick recipients into clicking on malicious links or downloading malware, which could grant scammers access to your confidential information. Below are tips to help you avoid falling victim to email scams:

- Do not click links, download software, or open attachments unless you are certain of the sender and purpose of the attachment.
- Do not unsubscribe from spam emails; deleting the spam email instead avoids clicking potentially malicious links.
- Verify the sender's email address is accurate.
- Carefully review the email's content. Phishing emails often contain poor grammar, incorrect punctuation, and misspelled words.
- To opt out of receiving unsolicited commercial emails from national companies, visit www.dmachoice.org.

DB TIP: ***Never let anyone you don't know remotely take control of your computer.***



Protect your money

Banks would never ask you to move money out of your Dacotah Bank account. Dacotah Bank has measures in place to protect your funds.

Payment app scams

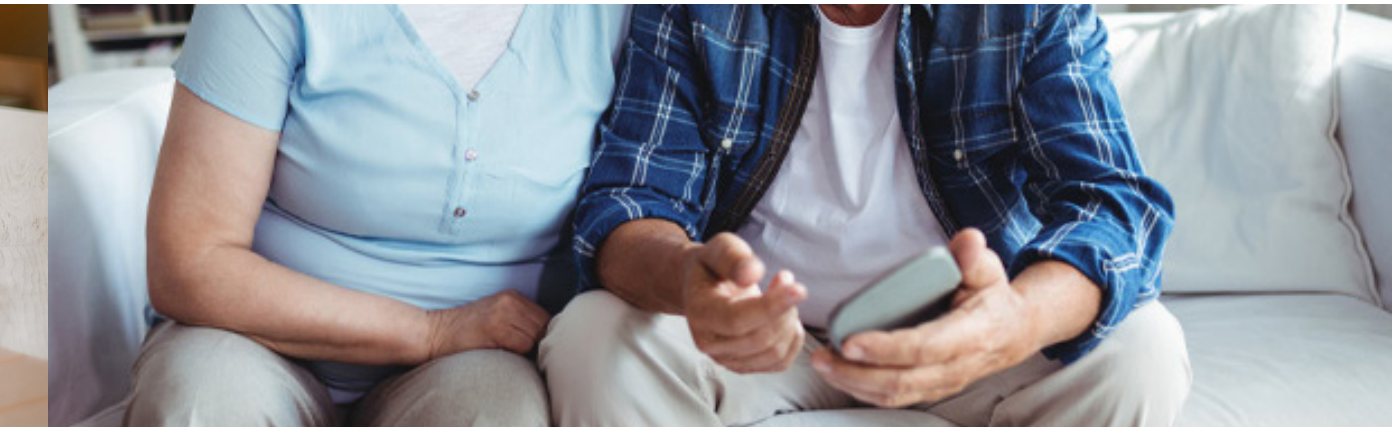
- **Unexpected Requests** - Be cautious if you receive unexpected requests from strangers or organizations asking you to send money through a payment app. This is a scammer move.
- **Sending Money to Yourself** - Scammers impersonating your bank may call to alert you about "suspicious activity" on your account and direct you to send money to yourself to reverse a transaction or to verify the account is not frozen. However, your bank will never tell you to send money to anyone, not even yourself.
- **Overpayment Claims** - Be skeptical if a sender claims to have accidentally overpaid you through Zelle® or another payment system, and requests a refund of the excess amount. Scammers use this tactic to trick you into sending them money. This could include Venmo, PayPal, etc.
- **Suspicious Links** - If you receive a payment app-related message that contains a link, never click it. Scammers often send links to fake login pages to steal your username and password.
- **Pressure and Urgency** - Scammers attempt to trick you by creating a sense of urgency. If they mention unforeseen emergencies, unverified transactions, account suspension, or unsolicited prize winnings, it's a scam.

Elder Abuse

Elder abuse can start with a stranger or someone you know and trust, such as a family member or friend. Delegate a trustworthy person to act as your agent if you are unable to facilitate financial transactions. Understand the terms of assigning a Power of Attorney (POA). Granting an individual POA gives them the authority to act on your behalf, including managing and having access to your financial accounts. Ensure any POA documents address how financial matters should be addressed.

Check references and credentials before you allow a hired individual into your home. Consult with a financial advisor or attorney before you sign any documents. Safeguard your personal information. Shred old bills, bank statements, junk mail, and any other personal information to avoid misuse.

Report Elder Abuse by calling: **(800) 881-5611** Extension 6315 Option 1



Suspicious calls and texts

Phone & Text Scams

Dacotah Bank will never contact you requesting your personal and confidential financial information. This information is already available to Dacotah Bank. Never send cash, checks, or gift cards to companies or individuals you haven't personally met. A legitimate business will never request payment by gift card. Scammers can make incoming phone numbers appear local. This tactic is referred to as spoofing. If you think the caller is being honest, hang up and call the phone number you know is genuine.

Remember these tips:

- Everyone is a potential target. Fraud is not limited to race, ethnic background, gender, age, education or income. However, certain groups such as the elderly, may be targeted because the caller assumes they live alone, have a nest egg, or may be more polite to strangers.
- Urgency is their specialty. Scammers are cunning and do not give you time to think about their pitch. They quickly provide extra information such as directing you to their website.
- Scammers use exaggerated fake prizes, products or services as bait.

Ask yourself these questions:

- Who is calling, and why?
- What is the hurry?
- If it is free, why are they asking me to pay?
- Why am I confirming my account information or giving it out?

Scammers may also send text messages to trick you into revealing confidential information. This tactic is referred to as smishing. Do not provide personal confidential information until you have verified the sender. Never respond to these text messages. Do not call the numbers they provide or click on links they send.

DB TIP: ***What time is it? The law allows telemarketers to call only between 8 a.m. and 9 p.m. A seller calling earlier or later is violating the law.***



Steps you can take

Safeguard your mobile device

Your mobile device provides convenient access to your email, bank and social media accounts. However, it can provide the same convenient access for criminals.

Remember these tips:

- Keep mobile devices and apps up to date, and use caution when downloading apps.
- Use the passcode lock setting on your mobile device.
- Know who has access to your devices and what activities they are engaged in.
- Install a mobile security application for IOS or Android.
- Avoid storing sensitive information, and be aware of shoulder surfers.
- Contact your bank immediately if you change your phone number or lose your mobile device.
- Wipe your device before you donate, sell or trade it.

Fraud Defender

For just pennies a day, Dacotah Bank's Fraud Defender identity theft restoration program can provide peace of mind.

Fraud Defender Benefits:

- Low monthly cost
- Credit monitoring
- Expense reimbursement
- Dedicated recovery advocate
- Fully-managed identity recovery
- Lost document replacement

All you need is a valid form of payment and an email address to enroll.

DB TIP: ***Log out completely when you finish an online banking session, every time.***



Common scams, fake scripts

"You've Won" Scams

You receive a card, call, or email claiming you won! Maybe it is a trip, prize, lottery, or sweepstakes. The person calling is so excited and cannot wait to send your winnings. Then they tell you there is a fee, some taxes, or customs duties to pay. They ask for your credit card or debit card number, bank account information, or ask you to wire money. **It is a scam. Never wire money to anyone who asks you to.**

IRS Imposter Scams

You receive a call from someone claiming to be from the IRS stating you owe back taxes. They threaten to sue you, arrest or deport you, or revoke your license if you do not pay immediately. They ask you to send money through digital wallet or a person to person method, such as Zelle, Venmo, CashApp, etc. They tell you to put money on a prepaid debit card or gift card and provide the card numbers. They may know personal information about you such as part of your Social Security Number, date of birth, middle name, and address. **It is a scam. Do not wire money or pay with a prepaid debit card or gift card. For tax questions, go to irs.gov or call the IRS at 1-800-829-1040.**

Grandkid Scams

You receive a call - "Grandma, I need money for bail." The caller may also request money for a medical bill or other kind of trouble. The caller says it is urgent and you need to keep it a secret. **It is a scam. Call your grandchild or other family member to verify.**

Job Scams

You receive a call, email, text, or see an ad promising you a job, a certificate to improve changes of obtaining a job, or work-from-home offers. Each scenario presents the promise of making large sums of money. The catch? They require you to pay upfront before they hire you. **It is a scam. Never pay in advance for information about a job.**

Investment / Pig Butchering Scams

A pig-butchering scam is a type of investment fraud where scammers promise high investment returns within a short period. Pig-butchering scammers often use fake images and impressive-yet-fraudulent investment portfolios. Once victims are hooked and have invested a significant amount of money, the scammers suddenly disappear, leaving victims with no way to recover their funds. The term "pig butchering" is derived from the idea the scammers fatten up their victims with the promise of lucrative returns before "slaughtering" them for their money. **It is a scam. Be cautious of unsolicted messages and group chats. Verify the legitamacy of brokerages. Be skeptical of high investment returns with low risks. Exercise skeptism toward obscure private investment opportunities.**

Healthcare Scams

You see an ad on TV explaining a new law requiring you to obtain a new health care card, or you receive a call offering discounts on health insurance. The caller may claim to work for the government and needs your Medicare number to issue a new card. Scammers follow the headlines. When it is medicare open season, they present a new script. **It is a scam. Before sharing information, call 1-800-MEDICARE, research, and check with someone you trust.**

Online Dating Scams

You meet someone special on a dating website. Soon they want to move off the dating site to email or phone calls. They say they love you but live far away due to work. Then they ask for money. They might say it is for a plane ticket to visit you, an emergency surgery, or other urgent incident. Scammers, both male and female, make fake dating profiles, using stolen photos of other people. **It is a scam. Do not send money. Report your experience to the dating site, the Federal Trade Commission, and the Federal Bureau of Investigation. If you have already sent money, contact your bank immediately.**

Tech Support Scams

You receive a phone call or a pop-up on your computer from someone saying your computer is infected. It might seem like the individual is from a well-known company, such as Microsoft, Apple, or your internet service provider. The individual indicates viruses or malware exist on your computer and requests remote access to your computer to resolve the issue. **It is a scam. Do not call the phone number or click the link. Do not send money, provide your credit or debit card number, or give control of you computer to anyone who contacts you. If you feel your computer is infected, take your computer to a local technician.**

Money Wiring Scams

Someone you do not know asks you to wire money and may use different ways to convince you to wire the money. You won a prize or inherited money, but you have to pay fees first. A friend or family member is in trouble. You receive a check for too much money and need to send back the extra. You won the lottery, but need to pay fees first. **It is a scam. Wiring money is like sending cash. Do not wire money to people you don't know. The scammer wants you to feel like you know them, you are friends, or even related. Do not be fooled. You should not have to pay money to receive winnings, an inheritance or a commission.**

Phishing / Spoofing Email Scams

You receive a phishing email or text message allegedly from a business or organization you know or trust. The message often includes a link or attachment when opened installs malware on your computer or mobile device or directs you to a look-alike website where personal information is requested. **It is a scam. Do not click on the link. If the correspondence is out-of-the-blue, it is probably a scam. When in doubt, delete the message.**


DB