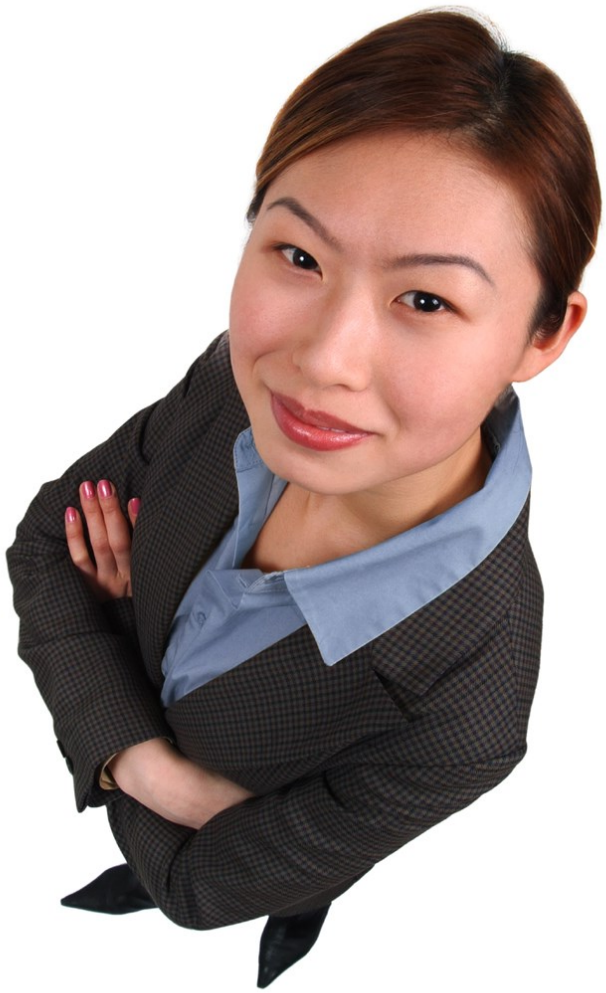
HELP FIGHT FRAUD

Important Information You Need to Know

The following pages describe four of the most common scams utilized by fraudsters. Fraudsters are trying to take your money!! They are very convincing and use “every trick in the book” to get you to disclose personal information or to send them money.

Any time you feel uncomfortable, STOP communicating with them and call us. If you have given out sensitive information, please don’t be embarrassed! Take action right away by contacting DNB National Bank at 605-874-2191. We are here to help and want to assist you.

We specialize in helping you determine if the request is legitimate and keeping your account safe.



Our customers are our top priority!

DNB National Bank

Common Scams

SOCIAL ENGINEERING & PHISHING SCAMS

WHAT IS IT?

The fraudulent attempt to obtain sensitive information, such as usernames, passwords, and account details, typically through an email or text message. These messages may impersonate a reputable company and include an urgent request to convince you to sign on to a spoof site, open an attachment containing malware, or respond with personal or account information. Once obtained, this information can be used to access your account and steal money. Scammers may hope to convince you to reveal personal information by using compelling language, such as a need to communicate with you for your own safety or account security.

HOW TO STOP IT

- Don't respond to messages from a sender you don't recognize. Keep security patches and anti-virus programs up to date on your computer and mobile devices. Don't share your password information.
- Turn *off* your mobile device's settings to auto-download attachments.
- Watch out for spelling or grammar mistakes in the message. Unusual text treatments, ID numbers, all caps, or punctuation like exclamation points may be signs of a scam.
- If you receive an *unexpected* request to unblock your DNB account, update your information, or verify your identity, be leery! Don't click on any links or respond. We may contact you, usually by telephone, for an action you have taken, such as signing in to your account or sending money. We occasionally send emails for information purposes only.
- Contact DNB at 605.874.2191 if you need assistance. Don't call any phone numbers that are listed in an email or other communication.

Common Scams

FAMILY EMERGENCY SCAMS

WHAT IS IT?

In this scam, you will receive a telephone call or email from a scammer claiming to be a friend or family member in need of money for an emergency. The person may seem legitimate because they have specific personal information, such as details about friends and family. This scam preys on people's emotions to convince you to immediately initiate a wire transfer.

HOW TO STOP IT

- Be cautious about sending money to friends and family until you have verified their identity and confirmed that the request is legitimate.
- Hang up if you feel uncomfortable, particularly about a call you didn't initiate.
- Contact your friend or family member directly to confirm the caller's story.
- Contact DNB if you need assistance determining the legitimacy of the call.

Common Scams

INTERNAL REVENUE SERVICE (IRS) FRAUD SCAMS

WHAT IS IT?

Imposter scams that may lead to tax fraud and identity theft increase during tax season. These scams can take many forms, such as fake IRS tax notices and fraudulent phone calls. In one scenario, scammers impersonating IRS agents call to claim you owe taxes or are due a refund.

HOW TO STOP IT

- The IRS initiates communication via mail, not email, text messages, or social media channels.
- The IRS does not demand that you pay taxes without letting you appeal the amount in question.
- The IRS does not require you to pay via wire transfer or any specific payment method.
- The IRS does not threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.
- Contact DNB if you need assistance determining the legitimacy of the communication.

Common Scams

WIRE TRANSFER SCAMS

WHAT IS IT?

A wire transfer is an immediate form of payment. Once a scammer has obtained the funds you wired in exchange for a check, the wire transfer cannot be reversed, even if the check is fraudulent. You have likely lost any wired funds.

For that reason, it's essential to take steps to reduce your risk of fraud by knowing best practices for wire transfers

HOW TO STOP IT

- Be wary of schemes claiming your payment will allegedly cover a loved one's expenses, lottery winning fees, and other scenarios.
- Situations where you're requested to deposit a check and send a portion back under the pretense that the extra money is commission or overpayment are often fraudulent. If the check bounces, you may be responsible for the amount.
- Check the information you include on a wire transfer. One typo could send the money to the wrong person or business.

DNB National Bank

Fraudsters are constantly coming up with new scams, but their goal remains the same: Take your money and/or personal information. The most important things you can do to stop fraud are:

- Stop Communicating with them.
- Do not open or download attachments you were not expecting
- Do not give out your personal information or passwords
- Contact DNB National Bank right away so that we can assist you.

605-874-2191 or bank@dnbanks.com