What the Fraud

The Official ANB Guide to Protecting Yourself and Your Business Against Fraud

If you give out any personal information, call us immediately.

(806) 378-8000 | 1-800-ANB-FREE

Amarillo National Bank

Member FDIC

CONTENTS

What is Cyber Fraud?

Cyber Fraud is a catch-all term that refers to all the ways bad guys use the internet to steal from individuals or businesses. It comes in a lot of disguises, often through e-mails or text messages pretending to be from trusted sources.

Threatening E-Mails

Bad guys use harsh and threatening language to trick you into giving them your information. (For instance: "We've hacked your email and have access to your personal data. Pay $1000 or we will release your private information.")

- **What you should do**: Ignore these emails. Mark them as spam. Don't reply.

Email Spoofing

Bad guys forge an email so it appears to come from a familiar source. Imagine a spoof from a vendor containing new payment instructions, or changes to an account that seem to come from someone in your business.

- **What you should do:** If you get a work email from the CEO or director of a business asking you to transfer funds, be suspicious. Always verify instructions verbally with the sender with the phone number you have on file. Bad guys will sometimes provide a new phone number in the email to verbally confirm instructions are correct.
- **What you should do:** If you get an e-mail that appears to be from a business you normally work with and they are asking you to update how you pay them, always verify. Call the business or e-mail a known contact at the business to verify the updated payment instructions before making changes.

Phishing

The bad guys try to lure you to fake websites that trick you into revealing passwords, credit card numbers, social security numbers, or other personal details. Never respond to an email that requires you to click a link, open an attachment, give away personal or banking information, or that requires immediate action.

- **What you should do:** Be extra cautious with links in unexpected emails. Check the "From" address to see if it's valid. Be suspicious of urgent language or threats of consequences if you don't respond. Be on guard if it wants you to verify account numbers, user IDs, passwords, or other personal info.
- **What you should do:** Never click a link or provide any personal information when prompted by an unexpected e-mail.

Impersonation and Identity

This varies. Sometimes a bad guy may impersonate your friend, family member or colleague asking for urgent financial help so they can steal from you. Sometimes they pretend to be tech support from a company and want remote access to your computer. And sometimes a bad guy will steal your identity to perform fraud.

- **What you should do:** Shred documents! Be careful with your wallet, purse, credit cards, bank information, and items in your trash. Criminals can get the information they need to impersonate you or contact you from lots of sources. And again, verify the email address or try to rule out impersonation before taking action.
- **What you should do:** If someone calls pretending to be a family member in need of assistance, hang up the phone and call the person at their trusted contact number to verify. These bad guys use a sense of urgency to keep you from verifying their information, always verify.

Protect Yourself Against Cyber Fraud

The best fraud prevention starts with you. Here are our tips.

YOU SHOULD NEVER:

- Share your 6-digit access code
- Share your user ID, password, or answers to security questions with anyone
- Open emails, links or attachments from unknown sources
- Follow links on pop-up messages on websites
- Write log-in credentials on a note near your computer
- Update payment info without confirming the change with a beneficiary or known vendor contact

YOU SHOULD ALWAYS:

- Use Dual-control whenever possible
- Log off secure websites when you're finished
- Forward suspicious emails that appear to come from ANB to WhatTheFraud@anb.com
- Call ANB immediately at (806) 378-8000 if any communication makes you suspicious
- Sign up for account alerts and review payments at anb.com
- Keep your computer operating system, web browsers and antivirus software up-to-date
- Keep tabs on user permissions in your business or organization
- Pay attention to your account activity for suspicious transactions or errors
- Be sure employees are trained on proper fraud prevention techniques

THINGS WE WILL NEVER DO

Amarillo National Bank will never...

- Email you to say your account has been compromised or passwords need to be changed.
- Ask you to reply to an email with personal or business info.
- Send an email threatening to close your account unless you give us information.
- Ask you for your password.
- Call you to offer login assistance (unless you contact us first).

When you call us, only call your ANB Support team at (806) 378-8000 or your ANB representative at our published numbers.

Protect Yourself Against Malware

Malware is any software designed to damage a computer or gain unauthorized access to a computer network. These go by a number of names: viruses, worms, Trojan horses, spyware, etc. They try to obtain your financial credentials.

We've received reports of scammers installing malware on our customers' computers. This forces customers to make multiple login attempts, enter secure access codes multiple times, or have someone else login from their machine.

What if you suspect malware fraud?

- Call ANB and alert our fraud department immediately.
- If you're on a work computer, contact your business's Security Administrator.

REMINDER

- We will NEVER request that another user attempt to log on from your computer.
- We will NEVER ask you to enter multiple secure access codes as part of the log-on process.

Additional Safety and Security Rules

We take security very seriously at ANB. Here are some of the things we tell our employees about basic computer security:

Always keep an updated version of a trusted antivirus program on your computer.

Beware of emails from senders you don't know. Unless you have verified or trust the sender, don't click links or open attachments.

Control physical access to your computer and devices. Log off when you leave a desktop or laptop. Don't leave an open laptop or phone in unsecured locations.

Never install software if you don't know the source or have authorization from your company.

Use only trusted computers or devices for online banking.

Don't hesitate to call ANB. Really, we don't mind. Contact us about any suspicious communication or activity at (806) 378-8000..

7 PASSWORD TIPS AND TRICKS!

1. Never base passwords on easily obtainable personal information like your user ID, telephone number or birthday.
2. Predictable passwords like ABCD1234 or Passw0rd or QWERTY are the first things cyberthieves will try.
3. Change passwords frequently.
4. Always use different passwords for different accounts.
5. Don't give passwords to anyone.
6. Don't save passwords on your computer or on written notes near your computer.
7. Use a reputable password manager app or program to generate and store complex passwords securely.

How ANB Protects You

It's important for you to take personal precautions. At the same time, ANB has your back.

Here's how we manage risk and safeguard your online information:

- Secure internet banking services
- Secure customer and user on-boarding
- Multi-factor user authentication security
- Required password changes
- Session inactivity timeout
- Automated account alerts
- Blocking of unsupported operating systems and browsers

We also employ a lot of behind-the-scenes technical stuff like intrusion detection, penetration testing and system monitoring. We'll spare you the complicated jargon. Just know that we have a whole team and a bunch of digital barriers in place to make sure no unauthorized users can get access to your accounts.

Additional Resources

Want to learn more? Here are some other resources to help you stay safe:

Amarillo National Bank Payments Fraud Protection

Knowledge and awareness are the strongest defense against fraud scams. Learn how to identify and prevent fraud at your business:

https://www.anb.com/education/staying-safe-online.html

Federal Trade Commission (FTC)

Government-recommended steps to prevent and protect against identity theft:

https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection

Protect Yourself and Your Money from the Bad Guys

The best fraud prevention starts with you. Here are our tips.

- Banks will **NEVER** call **YOU** to ask for personal information, account details, PINs, Passwords or Social Security Numbers. They already have this information. When in doubt hang up.
- Beware of text messages with Links. Do not enter your personal information.
- If someone calls and pressures you to send money "NOW" or buy gift cards, **it's a SCAM, hang up!**
- Don't rely on caller ID – Bad guys use technology to display bank names or numbers on caller ID.
- Bad guys pose as law enforcement, jury duty, or the IRS – if they call demanding money or personal information, hang up.

Bad guys will say things to make you panic.
If something feels off, hang up!

Call us immediately
if you give out any personal information
(806) 378-8000 | 1-800-ANB-FREE

Download this booklet
and get more information
anb.com

Amarillo National Bank
Member FDIC