Utah Independent Bank

How to Protect Yourself from Common Fraud and Scams

Utah Independent Bank
www.uib.bank

Introduction

Fraudsters use increasingly sophisticated methods to steal money and personal information. In 2024 alone, U.S. consumers reported losing more than $12.5 billion to fraud — a 25% increase over the prior year — according to the Federal Trade Commission (FTC). This training will help you recognize common scams, understand the latest trends, and learn practical steps to protect yourself and your finances.

What Fraud and Scams Look Like

Defining Fraud and Scams

Fraud occurs when a scammer misrepresents themselves or a situation to trick you into giving money, financial access, or personal information. Scams exploit trust, lonliness, urgency, fear, or excitement to influence your decisions.

How Often It Happens

According to recent FTC data:

- 2.6 million consumers reported fraud in 2024.
- Reported losses reached $12.5 billion.
- Investment scams caused the greatest losses — $5.7 billion.
- Losses from government and imposter scams totaled nearly $3 billion.
- Fraud contact via email was the most common method reported, followed by phone and text messages.

Common Scam Types You May Encounter

1. **Phishing & Smishing (Email/Text)**
    - Phishing happens though email, Smishing happens through text (SMS) messages.
    - Scammer uses fake messages claiming to be from your bank or company.
    - Use of random text messages or emails such as;

- ✓ **“Are you the horse-riding instructor I was told about?”**
- ✓ **“I’m coming to your BBQ tonight, what can I bring?”**
- ✓ **“Flying into town tomorrow, can’t wait to get drinks!”**

- Goal: Make contact. Gain trust. Steal login credentials, install malware or to validate the number is “live”. Once a number is “live” it becomes more valuable. (See “Social Engineering” and “Pig Butchering” below).

2. **Vishing (Phone Scams)**
   - Using filters and Arificial Intelligence (AI), an indivdual tries to gain trust. Business, social and romantic methods have all been used.
   - A live caller pretending to be from a trusted organization warns of “urgent issues,” pretends to reveal inside investment information or begins small talk, compliments, and flirting.
   - Often pushes for payment via wire transfer or gift cards.
3. **Imposter Scams**
   - Criminals pose as government agencies (e.g., IRS), companies, or family members.
     - ✓ **AI can clone trusted individual voices and mannerisms. Deep fakes can be very convincing.**
   - FTC reports losses to impersonation scams have surged dramatically, especially among older adults.
4. **Identity Theft**
   - Rise in individuals providing key credentials to scammers after social engineering scams. These include bank account, social media, digital currency applications and others.
   - Personal data (SSN, account numbers) used to open unauthorized accounts or commit financial crimes.
   - Over 1.1 million identity theft reports were submitted in 2024.
5. **Credit & Debit Card Fraud**
   - Unauthorized charges or cloned cards used by criminals. Card numbers, and account passwords being provided to online “friends” or romantic partners.

6. **Check and Payment Scams**

    - Fake refund checks or counterfeit checks that later bounce. You are responsible for money spent if a check is later determined to be fake or counterfeit after desposit.

7. **Investment & Loan Scams**

    - Digital currency trading, transportation(trucking), real estate, startups, etc.
    - Offers of high returns or “guaranteed” profits often tied to bogus investments.
        - ✓ **Small transactions often provide returns at first. The scammer will pull the plug when it is most profitable to them.**

8. **Tech Support Scams**

    - Fake alerts or calls claim your device is infected and demand payment for “fixing.”

9. **Social Engineering – Pig Butchering**

    - Pig Butchering is the idea of “fattening up” the victim over time. Social media, dating apps and random texts are used to make contact and establish if a victim is “live”. Once a victim is determined “live”, the con begins.
        - ✓ **Friendly conversation, compliments, and romantic interest**
        - ✓ **Investment opportunity – real estate, startups, digital currency trading, etc.**
        - ✓ **Small transactions that work or deliver returns.**
        - ✓ **Time is key. However long is necessary to gain the victim’s trust.**
    - Manipulative tactics, not technology alone, to influence you — e.g., posing as a friend or bank representative to gain trust and access.

10. **Cryptocurrency / Digital Currency Scams**

    - Fake trading platforms or “urgent crypto transfers” where victims are told to send Bitcoin or other digital assets to unlock accounts or make unrealistic returns.

How You Can Protect Yourself

1. Guard Your Personal and Financial Information

- Your bank, government agencies, or reputable companies will never ask for full passwords, PINs, or Social Security numbers by unsolicited email or text.
- Never provide account access, passwords, or security codes to unverified callers.

2. Authenticate Before Acting

- Verify who is contacting you:
  - Look up the organization's official phone number independently.
  - Hang up and call back using a trusted number.

3. Be Wary of Urgency and High-Pressure Tactics

Scammers commonly:

- Create panic with threats ("your account will be closed").
- Promise large rewards or payments if you act now.

4. Secure Your Digital Accounts and Devices

- Use strong, unique passwords and multi-factor authentication (MFA).
- Keep operating systems, antivirus software, and apps updated.
  - ✓ Do not give out passwords, account information or login credentials. This includes apps on your phone, which can be used as "back doors".

5. Watch Out for Cryptocurrency Red Flags

- Unsolicited offers to invest or trade digital currencies often end in loss.
- Payments via crypto (Bitcoin, Ethereum, etc.) are irreversible.

6. Learn Social Engineering Signals

- Emotional manipulation — e.g., romantic interest, claiming to be a loved one, a crisis, or a trusted authority — is a key scam tactic.
- Always independently verify suspicious requests.

If You Suspect Fraud — What to Do

Step 1: Contact Your Bank or Financial Institution Immediately

- **Your bank can help you**
- Report any suspicious transactions or messages.
- Freeze or close compromised cards or accounts.

Step 2: Report to the FTC

- File a report at ReportFraud.ftc.gov or IdentityTheft.gov if personal data was misused.
- Your report helps the FTC track patterns, which aids prevention and enforcement.

Step 3: Place Fraud Alerts and Monitor Credit

- Contact the major credit bureaus to add fraud alerts or freezes.
- Regularly check credit reports for unauthorized activity.

Step 4: Document Everything

- Keep records of calls, emails, screenshots, and reference numbers.
- Useful for investigations with banks, law enforcement, and credit bureaus.

Step 5: Stay Educated and Share with Others

- Review updates from the FTC: FTC.gov/consumer-alerts.
- Educate friends and family, especially older adults who are frequent targets.

Please contact *Utah Independent Bank* if you have any questions, or need assistance. We are here to help! Please visit our website at www.uib.bank.