VTAY CAPITAL
ENTERPRISES LLC
fraud prevention starts with you

A Guide to Vigilance, Trust, and Action

VTay Capital Enterprises LLC exists to expose deception, educate communities, and champion accountability — because fraud prevention starts with you.

VTay Capital Enterprises LLC www.vtaycapitalenterprisesllc.com Ph:307 429-2786

Understanding Fraud

What Is Fraud?

Fraud is intentional deception for personal or financial gain. It can occur in many forms — identity theft, phishing, financial scams, and corporate manipulation.

Why It Matters:

- In 2024, consumers reported losing over $12.5 billion to fraud
- Online scams resulted in a record $16.6 billion in losses reported to the FBI
- $8.8 billion lost to fraud in the U.S. in 2022
- 1 in 4 Americans targeted by scam attempts weekly
- Businesses lose 5% of annual revenue to fraud on average

Common Misconceptions:

- “It won’t happen to me.”
- “Only big companies are targeted.”
- “If it looks legit, it must be safe.”

Types of Fraud	Description	Common Examples	Impact
Cyber Fraud	Fraud committed using digital means.	Phishing emails, ransomware, online scams	Data theft, financial loss
Financial Fraud	Deception for financial gain.	Credit card fraud, investment scams	Monetary loss, damaged credit
Identity Fraud	Stealing or misusing personal information.	Identify theft, account takeover	Loss of reputation, financial loss
Corporate Fraud	Fraudulent activities within or against companies.	Embezzlement, accounting fraud	Financial loss, loss of trust

Red Flags & Risk Factors

Behavioral Red Flags:

- Urgent requests for money or information
- Emotional manipulation (fear, guilt, excitement)
- Requests to keep things secret

Technical Red Flags:

- Misspelled URLs or email addresses
- Suspicious attachments or links
- Unusual login activity

High-Risk Environments:

- Remote work setups
- Social media platforms
- Online marketplaces

Fraud Red Flags Checklist

Red Flag	Cyber Fraud	Financial Fraud	Identity Fraud	Corporate Fraud
Unusual transaction patterns	✓	✓	✓	✓
Inconsistent account or customer information	✓	✓	✓	✓
Suspicious documents or altered IDs	✓	✓	✓	✓
Multiple accounts with similar details	✓	✓	✓	✓
Transactions from unusual locations/devices	✓	✓	✓	
Large/unusual payments or withdrawals	✓	✓	✓	✓
Employees living beyond their means				✓
Reluctance to share duties or take vacations				✓
Defensive or evasive behavior about procedures				✓
Close relationships with vendors/customers				✓
Last-minute financial adjustments		✓		✓
Unusual working hours or access patterns		✓		✓
Alerts from consumer reporting agencies		✓	✓	
Notice from law enforcement or victims	✓	✓	✓	✓

Prevention Strategies

Personal Vigilance:

- Use strong, unique passwords and multi-factor authentication
- Verify sources before clicking links
- Monitor financial accounts regularly
- Regularly review accounts and transactions for unusual activities

Business Protocols:

- Conduct regular audits
- Train employees on fraud awareness
- Implement secure systems and access control
- Set up transaction limits and approval processes
- Confirm identities before processing sensitive transactions
- Check documentation for authenticity
- Use fraud detection software and alerts
- Update policies based on new threats and lessons learned

Community Awareness:

- Share knowledge with peers
- Encourage reporting and transparency
- Support fraud prevention initiatives

Resources & Contacts

Emergency Contacts:

- FTC Fraud Hotline 1-877-382-4357
- Local law enforcement
- Financial institution fraud departments

Helpful Links:

- consumer.ftc.gov
- identitytheft.gov

Fraud Awareness Quiz

Test Your Fraud Prevention Knowledge!

1. What is a common sign of a phishing scam?

a. An email from a known contact

b. A request for personal information urgently

c. A newsletter subscription

2. Which of the following is a strong password practice?

a. Using "password123"

b. Using a unique combination of letters, numbers, and symbols

c. Using your birthdate

3. What should you do if you suspect fraud?

a. Ignore it

b. Report it to the proper authorities

c. Share it on social media

4. Which environment is considered high-risk for fraud?

a. Remote work setups

b. Public libraries

c. Outdoor parks

5. What is the best way to protect your financial accounts?

a. Monitor them regularly

b. Share passwords with friends

c. Use the same password everywhere

Answer Key: 1. b, 2. b, 3. b , 4. a , 5. a