SBS CyberSecurity

FRAUDACITY FILES

SPOTTING SCAMS

A Field Guide to Recognizing and Avoiding Today's Most Common Financial Schemes

WHAT'S INSIDE THE

FRAUDACITY FILES

Scams continue to change in appearance, but the techniques behind them remain remarkably consistent. Criminals rely on pressure, urgency, and emotional triggers to push people into fast decisions before there's time to think.

This field guide outlines the most common scams affecting both everyday people and the financial institutions that protect their information. Each file explains what the scam is, how it typically unfolds, the warning signs that are easy to miss, and steps to respond confidently.

Across the Fraudacity Files, 12 fictionalized characters from different backgrounds and life stages encounter today's most common financial schemes, revealing how criminals tailor their tactics — and how easily anyone can be caught off guard.

TABLE OF

CONTENTS

Use this table of contents to quickly find the scams most relevant to you.

WHAT'S AT

STAKE

Financial scams can lead to stolen funds, compromised accounts, and leaked personal information. Community banks and credit unions regularly handle cases like these, and anyone with a phone, email inbox, or social media account can be targeted.

Many incidents start with something that feels routine: a call, a notification, an unexpected request, or a transaction that seems legitimate at first glance. In the moment, it's easy to miss the small warning signs that something isn't right.

The Fraudacity Files that follow are grounded in real-world scenarios. Each story illustrates how a scam could unfold step by step — and how recognizing red flags and responding appropriately can prevent loss.

73%

of U.S. adults say they've been targeted by an online scam or cyberattack.

Pew Research Center, 2025

The Golden Rule of Email

Treat every email as if it's a phishing attempt. If a message feels urgent, unexpected, or out of character, pause and verify before responding, clicking, or sharing information. Many of the schemes in this guide succeed when this step is skipped.

Dig Deeper

For more free fraud-awareness education, join the monthly Hacker Hour webinar series.

link.sbscyber.com/hackerhour

CASE 001
FRAUDACITY FILES

PHISHING

Fake emails that appear legitimate trick recipients into clicking links, opening attachments, or sharing sensitive information.

VICTIM

EMMA

PROJECT MANAGER

LOGIN STOLEN

HOW IT HAPPENED

Emma, a busy project manager balancing client meetings and personal accounts, was catching up on emails when one message stood out. It appeared to be from her bank, warning of unusual activity. The subject line felt urgent, the branding looked correct, and the tone seemed serious and professional.

The message claimed her account would be temporarily restricted unless she verified recent activity. A “Verify Now” button caught her eye. After a brief hesitation, she clicked and entered her credentials. By evening, unauthorized transactions appeared. Emma’s account had been compromised through a carefully crafted phishing email designed to mimic a legitimate bank notification.

WHAT EMMA MISSED

- x Unexpected, unverified email message
- x Link leading to fake website
- x Asked to log in via suspicious link instead of official website
- x Pressure to act immediately without verification

WHAT EMMA COULD HAVE DONE

- ✓ Hovered over link to confirm destination
- ✓ Accessed bank account through official website
- ✓ Called bank using verified phone number
- ✓ Enabled multifactor authentication (MFA)

WHO TO CONTACT

- > Bank or credit union
- > Employer’s IT team
- > Local law enforcement
- > FBI IC3 (for significant financial loss)
- > FTC

SBS CyberSecurity

CASE 002
FRAUDACITY FILES

PHONE SCAMS

Texts (smishing), phone calls (vishing), or QR codes (QRishing) deceive victims into sharing sensitive information or taking actions benefitting criminals.

VICTIM

JASON

TECH CONSULTANT

ACCOUNT DRAINED

HOW IT HAPPENED

Jason, a tech consultant often working between client sites, received a text claiming his debit card was locked, asking him to click a link to reactivate it. Moments later, a call from someone claiming to be his bank's fraud department requested his login code. The caller sounded authoritative, and the timing felt urgent.

That same week, a QR code on a flyer in his mailbox claimed to link to account verification. Believing it was connected to the earlier alert, Jason scanned it and followed the instructions. Within hours, unexpected withdrawals appeared. By combining a fraudulent text, a follow-up phone call, and a QR code, the scammer gained access to his accounts.

WHAT JASON MISSED

- x Text from unknown number with urgent request
- x Call requesting login code
- x QR code leading to fraudulent site
- x Pressure to act without verification

WHAT JASON COULD HAVE DONE

- ✓ Ignored links from unknown numbers
- ✓ Called bank using verified phone number
- ✓ Avoided scanning QR codes from unverified sources
- ✓ Enabled multifactor authentication (MFA)

WHO TO CONTACT

> Bank or credit union
> Mobile carrier
> Local law enforcement
> FTC

SBS CyberSecurity

CASE 003
FRAUDACITY FILES

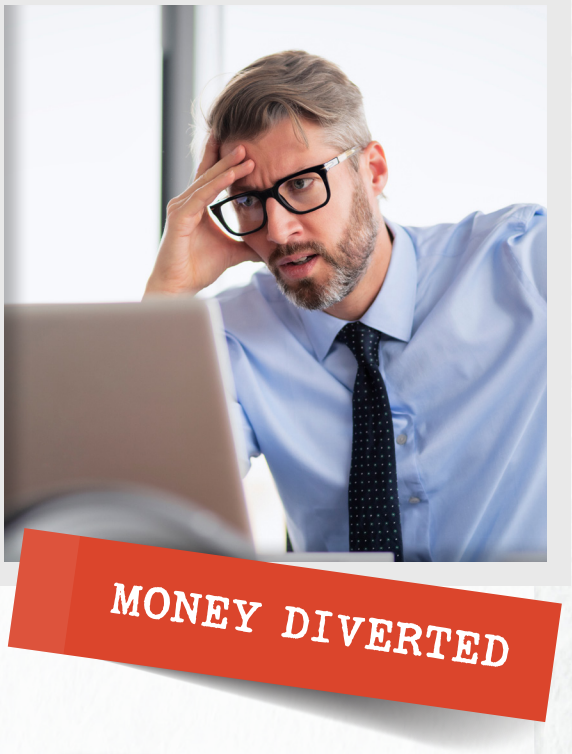
BUSINESS EMAIL COMPROMISE

Criminals gain access to company email accounts to request fraudulent transfers or sensitive information.

VICTIM

MARCUS

FINANCE OPERATIONS MANAGER



MONEY DIVERTED

HOW IT HAPPENED

Marcus, responsible for approving finance requests at his company, received an email appearing to come from the finance department requesting an urgent wire transfer. The email looked legitimate, with familiar formatting and signatures, but he also noticed an unexpected recipient had been copied on the message. Focused on approvals and deadlines, Marcus assumed it was routine and processed the transfer.

By the end of the day, funds had been diverted to a fraudulent account. The transfer was part of a business email compromise, in which attackers exploited trusted workflows and familiar formatting to redirect company funds.

WHAT MARCUS MISSED

- x Email requesting urgent transfer
- x Slightly off tone in message
- x Unexpected recipient copied
- x Request for sensitive information via email

WHAT MARCUS COULD HAVE DONE

- ✓ Verified payment request through separate channel
- ✓ Followed dual-approval process
- ✓ Noted anomalies in email tone or sender
- ✓ Ensured email systems were updated and secure

WHO TO CONTACT

- > Bank or credit union
- > Employer's IT team
- > FBI IC3 (for significant financial loss)
- > FTC

SBS CyberSecurity

CASE 004
FRAUDACITY FILES

ROMANCE SCAMS

Criminals build emotional relationships online to exploit trust and request money or sensitive information.

VICTIM

LINDA

ONLINE DATER

TRUST BETRAYED

HOW IT HAPPENED

Linda, active on dating apps while balancing work and personal projects, met someone online who seemed genuinely interested in a relationship. They exchanged messages regularly, sharing details about their lives and building familiarity over time. Eventually, the person claimed to be facing a financial emergency and asked for help. Believing the situation was legitimate, Linda sent the money without verifying the request.

When follow-up questions were met with excuses and the account suddenly disappeared, Linda realized she'd been scammed. The relationship had been carefully constructed to create confidence and lower her guard.

WHAT LINDA MISSED

- x Rapid expressions of affection from new acquaintance
- x Requests for money, gifts, or financial help
- x Stories always involving urgent crises

WHAT LINDA COULD HAVE DONE

- ✓ Avoided sending money to a stranger
- ✓ Verified identities independently
- ✓ Refrained from wire transfers or gift card payments
- ✓ Reported suspicious profiles to platform

WHO TO CONTACT

- > Bank or credit union
- > Social media platform support
- > Local law enforcement
- > FTC

SBS CyberSecurity

CASE 005
FRAUDACITY FILES

PIG BUTCHERING SCAMS

Scammers lure victims with promises of high investment returns, gradually extracting money over time.

VICTIM

RICHARD

FIRST-TIME INVESTOR

INVESTMENT LOST

HOW IT HAPPENED

Richard, interested in trying online investing, was approached by someone offering guidance on a cryptocurrency platform. Initial small gains felt legitimate, and over time, he was encouraged to invest increasingly large amounts. The early "successes" built trust, masking the risk.

Eventually, Richard attempted to withdraw his funds and found the account inaccessible. The platform disappeared, along with the money he'd invested, revealing that the platform and advisor had been fraudulent from the start.

WHAT RICHARD MISSED

- x Promises of unusually high returns
- x Pressure to invest quickly
- x Requests to move money to untraceable accounts
- x Complex or secretive investment schemes

WHAT RICHARD COULD HAVE DONE

- ✓ Researched investments independently
- ✓ Avoided platforms with pressure tactics
- ✓ Verified regulatory registration of advisors or brokers
- ✓ Consulted trusted financial professional

WHO TO CONTACT

> Bank or credit union
> FTC
> SEC

SBS CyberSecurity

CASE 006
FRAUDACITY FILES

DEEPFAKE SCAMS

Realistic but fake audio or video is used to manipulate, extort, or impersonate individuals.

VICTIM

SARAH

REMOTE MANAGER

IDENTITY FAKED

HOW IT HAPPENED

Sarah, managing a small remote team, received a video message that appeared to be from her manager requesting an urgent fund transfer. The voice and mannerisms were convincing, and the timing coincided with a real pending payment. Believing it authentic, Sarah began the transfer process and nearly authorized the payment.

Inconsistencies in the video and unusual instructions prompted her to double-check the request. She reached out to her manager via a separate channel and discovered the video was fabricated. The deepfake had been designed to exploit her trust and urgency.

WHAT SARAH MISSED

- x Unexpected video request for money
- x Message creating strong sense of urgency
- x Communication method unusual for this type of request

WHAT SARAH COULD HAVE DONE

- ✓ Verified request through separate channel immediately
- ✓ Questioned high-pressure video communications
- ✓ Enabled multifactor authentication (MFA) and multistep verification for transactions

WHO TO CONTACT

> Bank or credit union
> Employer's IT team
> Local law enforcement
> FTC

SBS CyberSecurity

CASE 007
FRAUDACITY FILES

VIRTUAL KIDNAPPING SCAMS

Scammers exploit fear by claiming a loved one is in danger to extract money quickly.

VICTIM

MIGUEL

PARENT

THREAT FABRICATED

HOW IT HAPPENED

Miguel, unwinding at home after work, received a frantic call from someone claiming his child had been kidnapped. Referencing personal details obtained from social media, the caller demanded immediate payment via gift cards to secure the release of his child and warned that involving anyone else would make the situation worse. Panicked and fearful, Miguel rushed to a nearby store and purchased several gift cards.

Before sending the codes, discrepancies in the caller's story caused him to pause and contact authorities. He soon learned his child was safe and the call was a scam that relied on fear and personal details to pressure victims into immediate action.

WHAT MIGUEL MISSED

- x Sudden claim of loved one in danger
- x Pressure to act immediately
- x Threats if instructions weren't followed
- x Requests for gift cards or wire transfer

WHAT MIGUEL COULD HAVE DONE

- ✓ Called supposed victim or authorities immediately
- ✓ Avoided following instructions until verified
- ✓ Stayed calm and sought law enforcement support

WHO TO CONTACT

> Bank or credit union

> Local law enforcement

> FBI IC3 (for significant financial loss)

> FTC

SBS CyberSecurity

CASE 008
FRAUDACITY FILES

PREPAID CARD SCAMS

Scammers demand payment in prepaid cards because they are hard to trace and nonrefundable.

VICTIM

TANYA

TAXPAYER

CARDS TAKEN

HOW IT HAPPENED

Tanya, who had recently submitted her personal taxes, received a call claiming to be from the IRS and warning that she owed money that needed to be paid immediately with prepaid cards. The caller instructed her to keep the payment secret. Feeling pressured, Tanya purchased the cards and shared the codes.

When she later contacted the IRS directly to verify the claim, she learned it was a scam. The urgency and insistence on secrecy had created a false sense of obligation.

WHAT TANYA MISSED

- x Requests for prepaid cards
- x High-pressure threats
- x Instructions to keep payments secret

WHAT TANYA COULD HAVE DONE

- ✓ Avoided paying with gift or prepaid cards
- ✓ Verified requests with official agencies
- ✓ Reported suspicious demands

WHO TO CONTACT

> Local law enforcement

> FTC

SBS CyberSecurity

CASE 009
FRAUDACITY FILES

PAYMENT FRAUD

Criminals manipulate victims into sending money through altered, forged, or fraudulent financial transactions, including wire, check, or ACH fraud.

VICTIM

RAVI

SMALL-BUSINESS OWNER

FUNDS REDIRECTED

HOW IT HAPPENED

Ravi, reviewing vendor payments for his small business, received an email requesting urgent changes to payment instructions for an upcoming transfer. The message appeared legitimate and referenced an existing vendor relationship. During a busy workday, Ravi followed the new instructions and authorized the payment.

Days later, a reconciliation review revealed that the funds had been sent to a fraudulent account. The request was part of a payment diversion scam exploiting routine workflows and trusted processes.

WHAT RAVI MISSED

- x Unexpected payment requests
- x Changes to account or routing information
- x Request sent via email or phone without verification

WHAT RAVI COULD HAVE DONE

- ✓ Verified changes with payer or bank
- ✓ Enabled multifactor authentication (MFA) and multistep verification for transactions
- ✓ Monitored accounts regularly

WHO TO CONTACT

> Bank or credit union
> Local law enforcement
> FTC

SBS CyberSecurity

CASE 010
FRAUDACITY FILES

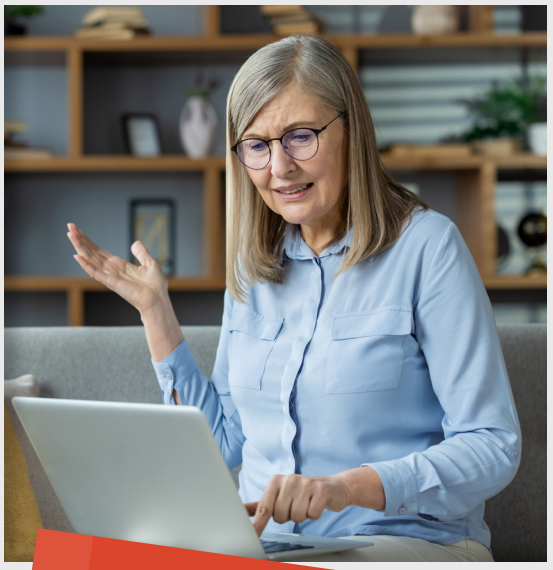
SWEEPSTAKES AND LOTTERY SCAMS

Scammers notify individuals of a supposed prize or winnings and require fees or taxes to be paid up front before the prize is released.

VICTIM

ELEANOR

SWEEPSTAKES ENTRANT



HOW IT HAPPENED

Eleanor frequently entered online sweepstakes for travel deals. When she received an email claiming she had won a free trip, it didn't immediately raise concern. The message referenced common sweepstakes language but directed her to complete the claim process outside the platform she had used to enter.

To receive the prize, she was asked to wire a processing fee. After sending the money, Eleanor tried to confirm her booking on the official sweepstakes platform and realized the trip didn't exist. The message had mimicked legitimate sweepstakes communication while redirecting the interaction to an unverified channel.

WHAT ELEANOR MISSED

- x Request to claim prize off-platform
- x Request for up-front payment
- x Pressure to act immediately

WHAT ELEANOR COULD HAVE DONE

- ✓ Avoided sending money to claim prize
- ✓ Verified sweepstakes legitimacy independently
- ✓ Reported suspicious notices

WHO TO CONTACT

> Bank or credit union
> Local law enforcement
> FTC

SBS CyberSecurity

CASE 011
FRAUDACITY FILES

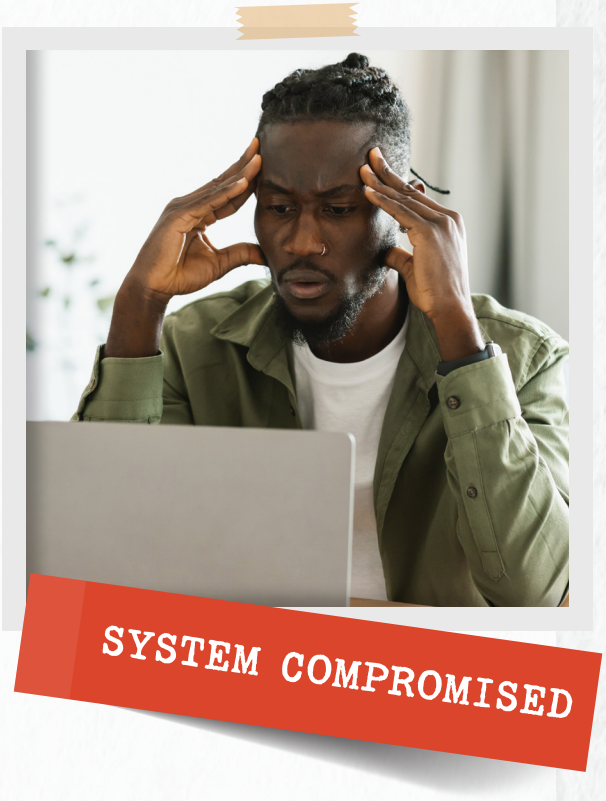
TECH SUPPORT SCAMS

Attackers pose as tech support to gain access to devices or extort money.

VICTIM

ANTHONY

HOME COMPUTER USER



HOW IT HAPPENED

Anthony, completing routine updates on his home computer, encountered a pop-up warning claiming a virus had been detected. Shortly after, he received a call from someone posing as tech support who requested remote access to fix the issue. Believing the alert was legitimate, Anthony granted access and paid for the supposed service.

Soon after, his system slowed dramatically, and files became inaccessible. He realized the pop-up and call had been fraudulent and that attackers had used remote access to install malware and extract payment, leaving his system compromised.

WHAT ANTHONY MISSED

- x Unexpected alerts about device problems
- x Requests to install software or grant remote access
- x Urgent demand for payment

WHAT ANTHONY COULD HAVE DONE

- ✓ Avoided granting remote access to unknown parties
- ✓ Contacted official support channels directly
- ✓ Closed suspicious pop-ups and deleted unexpected emails

WHO TO CONTACT

> Bank or credit union
> Employer's IT team
> FTC

SBS CyberSecurity

CASE 012
FRAUDACITY FILES

SOCIAL MEDIA ACCOUNT TAKEOVER

Scammers gain control of online accounts to impersonate victims or steal information.

VICTIM

CHLOE

SOCIAL MEDIA USER

PROFILE HIJACKED

HOW IT HAPPENED

Chloe, active across several social media platforms, received a notification about an attempted login she didn't recognize. Assuming it was a mistake, she dismissed the alert. Shortly afterward, she was locked out of her account.

Friends and contacts began reaching out, sending her screenshots of suspicious messages and posts appearing under her name that promoted links and requested money. Through these alerts, Chloe deduced that her credentials had been captured via a phishing message that mimicked a routine account alert. The attackers had tried to use her account to send scam messages to her contacts before her access was restored.

WHAT CHLOE MISSED

- x Unusual login notifications
- x Messages posted she didn't write
- x Changes to account settings
- x Weak or reused passwords

WHAT CHLOE COULD HAVE DONE

- ✓ Used strong, unique passwords
- ✓ Enabled multifactor authentication (MFA)
- ✓ Monitored accounts regularly
- ✓ Reported suspicious activity immediately

WHO TO CONTACT

> Bank or credit union

> Social media platform support

> FTC

SBS CyberSecurity

TOP 5 WAYS TO

PROTECT YOURSELF

1. PAUSE AND VERIFY

Always check unexpected messages before acting.

2. GO DIRECT

Access websites directly instead of clicking links.

3. ENABLE MFA

Add an extra layer of protection with multifactor authentication.

4. BE SKEPTICAL

If messages feel urgent, unusual, or too good to be true, take a step back.

5. REPORT IT

Contact your bank or credit union, affected platforms, or authorities promptly.

STAY ONE STEP

AHEAD OF FRAUD

Fraud awareness is ongoing. Join the Hacker Hour webinar series to stay informed, practice spotting scams, and learn practical prevention strategies.

link.sbscyber.com/hackerhour