USAPLANS BUSINESS SAFETY SERIES

2026 Business Scam Watch

Stop. Verify. Then act.

Ten major documented threats, the warning signs that expose them, and a practical response plan for small businesses.

Government-sourced and independently summarized
Printer Edition 1.1 | Last reviewed July 13, 2026

USAPlans.org

HOW TO USE THIS GUIDE

A practical watchlist, not an invented ranking.

The IRS publishes an annual ranked Dirty Dozen for tax scams. The other risks in this guide are major business threats documented by the FBI, FTC and Grants.gov.

01 TRUST

The message borrows a boss, vendor, agency or professional you recognize.

02 URGENCY

A deadline, threat, emergency or disappearing opportunity prevents careful thought.

03 CONTROL

Secrecy or unusual instructions push you outside your normal approval process.

04 PAYMENT

The request changes an account or demands wire, crypto, gift card or money back.

DEFINITIONS THAT MATTER

Phishing
Fraudulent email designed to steal information, money or access.

Smishing
The text-message version of phishing.

Spoofing
Falsifying a sender, number, domain or caller ID to appear trusted.

BEC
Business email compromise: impersonation that redirects a payment or steals data.

Account takeover
Unauthorized control of an email, bank, payroll, tax or other account.

Recovery scam
A second scam promising to recover money already lost, usually for a fee.

The pause rule

A legitimate request can survive independent verification. A scam depends on stopping it.

AT A GLANCE

Ten threats every business team should recognize.

01 IRS phishing, smishing and fake QR codes

Unexpected emails, texts and direct messages imitate the IRS and push owners toward fake websites to verify an account, enter information or claim a refund.

02 AI voice impersonation and caller-ID spoofing

A convincing voice, familiar name or official-looking caller ID is used to demand immediate payment, credentials or secrecy.

03 Business email compromise and payment diversion

A criminal impersonates an executive, vendor or closing party and redirects a legitimate payment to a fraudulent bank account.

04 Fake grants and government-fee schemes

Promoters promise guaranteed awards, hidden programs or free government money in exchange for an upfront fee or sensitive information.

05 Fake invoices and unordered merchandise

06 Bogus credits and social-media tax hacks

Promoters market refunds or credits for which an owner may not qualify, sometimes using fabricated income, withholding or forms.

07 Ghost preparers and tax-relief mills

An untrustworthy preparer refuses to sign a return, or a tax-relief mill overpromises settlement results and charges high fees.

08 Account takeover, payroll and W-2 theft

Criminals steal credentials or pose as helpers to enter tax, payroll, email or banking accounts and harvest employee information.

09 Fake charities and disaster appeals

Fraudsters exploit tragedies and disasters to collect money or information through an imitation charity or copied appeal.

10 Tech support, processing, leasing and fake checks

FBI 2025 REPORTED DATA

$3.047 billion

in reported business email compromise losses from 24,768 complaints. Complaint data does not represent every incident and is not a forecast.

SCAM WATCH 1 OF 4

Identity and authority

The message looks or sounds official.

01 TAX

IRS phishing, smishing and fake QR codes

Unexpected emails, texts and direct messages imitate the IRS and push owners toward fake websites to verify an account, enter information or claim a refund.

RED FLAGS

- Unexpected digital contact
- Odd or misspelled address
- Urgent verification
- Link, attachment or QR code

SAFEST NEXT MOVE

Do not click, scan or reply. Navigate to IRS.gov yourself and forward suspected IRS phishing to phishing@irs.gov.

IRS 2026 Dirty Dozen, items 1 and 11

02 CYBER

AI voice impersonation and caller-ID spoofing

A convincing voice, familiar name or official-looking caller ID is used to demand immediate payment, credentials or secrecy.

RED FLAGS

- Urgent prerecorded threat
- Immediate payment demand
- Bypass of normal approval
- Resistance to verification

SAFEST NEXT MOVE

Hang up. Call the person or agency through a number already in your records or found independently on an official website.

IRS 2026 Dirty Dozen, item 2

Money in motion

Fraud succeeds when normal payment checks disappear.

03 Business email compromise and payment diversion

A criminal impersonates an executive, vendor or closing party and redirects a legitimate payment to a fraudulent bank account.

SAFEST NEXT MOVE

Verify every payment change by calling a known number. If money moved, call the bank immediately and report promptly to IC3.gov.

FBI IC3 2025 Annual Report

04 Fake grants and government-fee schemes

Promoters promise guaranteed awards, hidden programs or free government money in exchange for an upfront fee or sensitive information.

SAFEST NEXT MOVE

Search for the opportunity directly on an official .gov website. Grants.gov states that applying for a federal grant is free.

Grants.gov Grant Fraud guidance

05 Fake invoices and unordered merchandise

A phony invoice looks routine, or merchandise arrives after a misleading confirmation call followed by pressure to pay.

SAFEST NEXT MOVE

Match invoices to approvals, receiving records and known vendor contacts. Do not pay merely because the document looks official.

FTC Scams and Your Small Business

SCAM WATCH 3 OF 4

Tax promises

The return belongs to the taxpayer, even when someone else prepares it.

06 TAX

Bogus credits and social-media tax hacks

Promoters market refunds or credits for which an owner may not qualify, sometimes using fabricated income, withholding or forms.

RED FLAGS

- Guaranteed refund
- Secret or universal credit
- Advice to invent figures
- No written eligibility analysis

SAFEST NEXT MOVE

Verify the provision on IRS.gov and with a qualified tax professional. The taxpayer remains responsible for an inaccurate return.

IRS 2026 Dirty Dozen, items 4, 6, 7 and 10

07 TAX

Ghost preparers and tax-relief mills

An untrustworthy preparer refuses to sign a return, or a tax-relief mill overpromises settlement results and charges high fees.

RED FLAGS

- No PTIN or signature
- Blank or incomplete return
- Fee based on refund
- Guaranteed settlement

SAFEST NEXT MOVE

Never sign a blank return. Confirm credentials and use the IRS Offer in Compromise pre-qualifier before paying a relief company.

IRS 2026 Dirty Dozen, items 8 and 12

Access, emotion and service traps

Protect accounts, verify charities and read every agreement.

08 Account takeover, payroll and W-2 theft

Criminals steal credentials or pose as helpers to enter tax, payroll, email or banking accounts and harvest employee information.

SAFEST NEXT MOVE

Create accounts directly through official sites, protect sign-in and verify sensitive document requests through another channel.

IRS 2026 Dirty Dozen, items 5 and 11

09 Fake charities and disaster appeals

Fraudsters exploit tragedies and disasters to collect money or information through an imitation charity or copied appeal.

SAFEST NEXT MOVE

Confirm the organization through IRS Tax Exempt Organization Search and use the charity's independently verified website.

IRS 2026 Dirty Dozen, item 3

10 Tech support, processing, leasing and fake checks

A seller promises lower fees, urgent repair, easy equipment or an overpayment that requires money to be sent back.

SAFEST NEXT MOVE

Pause, obtain complete documents and verify independently. A displayed or temporarily available balance does not prove a check is valid.

FTC Scams and Your Small Business

THE TEN-MINUTE PROTECTION PLAN

Build friction in the right places.

A legitimate request can survive verification. Decide who gets called before money moves.

1 **Second approval**

Use two people for new payees, account changes and unusual payments.

2 **Known-number callback**

Never verify through the phone number supplied in the request.

3 **Protected sign-in**

Use unique passwords and phishing-resistant MFA or passkeys where available.

4 **Paperwork match**

Connect invoices to approval, purchase order, delivery and known vendor.

5 **Limited access**

Restrict payroll, tax and banking access and review it regularly.

6 **Practice the pause**

Train staff to spot urgency, secrecy, authority and unusual payment.

7 **Tested backups**

Keep protected backups and a contact list outside the affected system.

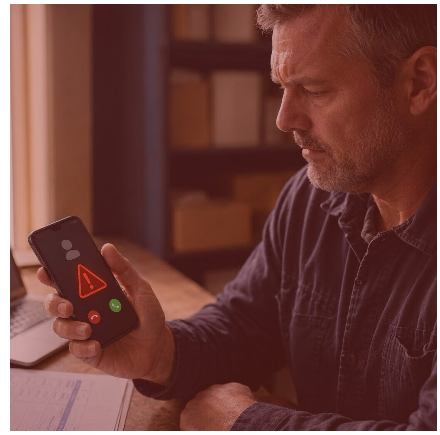
8 **Written response**

Name who calls the bank, preserves evidence, resets access and reports.

IF MONEY OR INFORMATION WAS SENT

Speed matters. Shame does not help.

Scammers are practiced manipulators. Focus on containment, evidence and fast reporting.



1 **Stop contact and further payment**

Do not pay a recovery service or additional fee.

2 **Call the bank or payment provider**

Ask immediately about a hold, recall, reversal or fraud process.

3 **Preserve the evidence**

Keep messages, headers, invoices, account details, receipts, URLs and times.

4 **Secure affected systems**

From a clean device, change credentials, revoke sessions and obtain qualified help.

5 **Report through the correct channel**

Use IC3 for internet crime, the FTC for scams and IRS channels for tax fraud.

6 **Get professional guidance**

Contact counsel, accountant, insurer, law enforcement and affected people as appropriate.

GO TO THE SOURCE

Official verification and reporting.

Public government resources are never hidden behind an email form. Use these links to confirm current instructions.

IRS 2026 DIRTY DOZEN

Tax threats, warning signs and reporting

SCAN OR CLICK TO OPEN

FBI IC3 ANNUAL REPORT

Current cyber-fraud evidence and definitions

SCAN OR CLICK TO OPEN

FTC SMALL-BUSINESS GUIDE

Common tactics, prevention and reporting

SCAN OR CLICK TO OPEN

GRANTS.GOV FRAUD

Recognizing fake federal grant offers

SCAN OR CLICK TO OPEN

REPORTFRAUD.FTC.GOV

Report scams and deceptive practices

SCAN OR CLICK TO OPEN

IC3.GOV

Report internet-enabled crime to the FBI

SCAN OR CLICK TO OPEN

USAPlans.org Practical education for the people building America's small businesses.