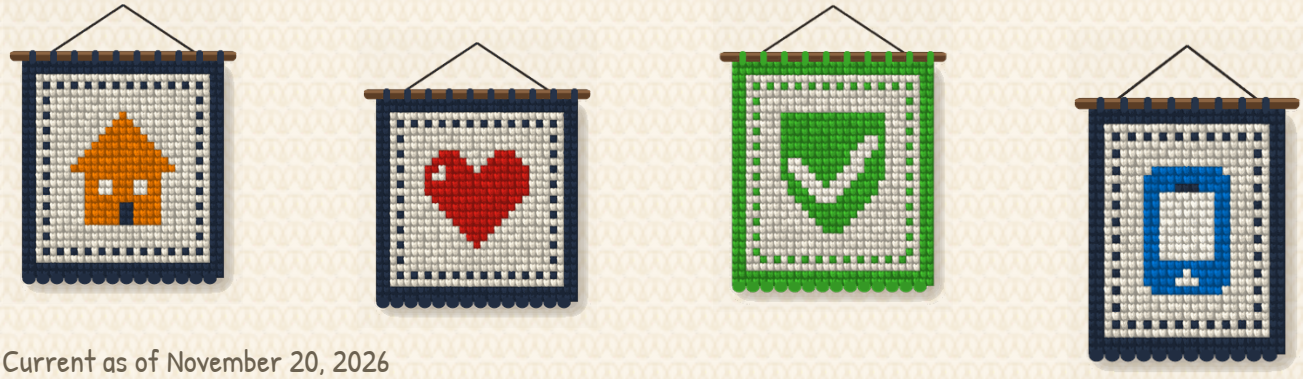
centrexIT™

A free guide for the holiday season



What changed this week, what scammers are doing right now, and the specific steps that protect your office and your home. Every claim in this guide is sourced, so you can check it and share it.



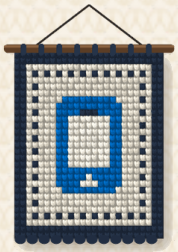
Current as of November 20, 2026

centrexIT, San Diego managed IT and cybersecurity, since 2002

People-First. AI-Amplified. Cyber IT.

Mid-November 2026

WHAT HAPPENED THIS WEEK



Five stories from the past two weeks that change what we'd tell any business owner or family right now.

Banking and AI

Major banks say you carry the risk if you give an AI tool your bank login

Citi updated its online user agreement this week. It says that if a third-party AI tool leaks your banking credentials or gets hacked, you're responsible for what the hackers do with your account.[1] PNC changed its terms on November 18, Citizens emailed customers a similar warning, and JPMorgan and Bank of America announced similar policies in October.[1] More on what this means on the next page.

Travel

Expedia confirms a breach through a third-party vendor

Expedia confirmed it was hit by a supply chain attack in which hackers compromised a third-party data platform provider and used its access to reach several companies' systems. An extortion group claims it took more than 830 million loyalty program records, including email addresses and points balances.[7] Expect "your account" and "your points" emails that look real.

Remote support tools

Attackers abused a remote-support tool many IT providers use

On November 11, ConnectWise reported attackers getting into cloud-hosted ScreenConnect instances belonging to IT providers and installing unauthorized remote-access software on client computers.[8] Huntress counted rogue clients on at least 288 computers at 48 organizations within about 90 minutes, entering through a third-party add-on that bypassed the tool's user accounts and MFA. ConnectWise said it found no compromise of its own infrastructure and no flaw in ScreenConnect itself.[9]

Text messages

125 million texts, including bank login codes, left exposed

A telecom provider in the Baltic states left a database of more than 125 million text messages publicly accessible, including messages from banks, airlines and medical providers. Attackers could have seen one-time login codes and password reset links before the recipients did.[8]

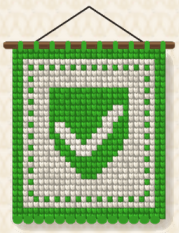
Holiday season

Federal and consumer warnings are out

AARP's 2026 holiday report found 84% of U.S. adults have experienced at least one common type of fraud.[10] The U.S. Treasury's 2026 seasonal advisory names online sales fraud, gift card fraud and charity scams as the most common holiday scams.[11] With a record 122 million Americans expected to travel, the Better Business Bureau is warning about fake airline booking sites.[12]

The new risk to know about

YOUR BANK, AI AND YOUR MONEY



AI assistants that can read statements, pay bills or move money are new. Banks are now telling customers, in writing, who pays when something goes wrong.

What the banks are saying

- **Citi:** if an AI tool leaks your credentials or is hacked, you're responsible for what hackers do with your account. Citi says the AI agents it provides itself can be used without that added liability.[1]
- **Chase,** in a November email: "authorized transactions may not be reversible if your information is misused."[2]
- **Ally,** in an email to customers: "When you use an AI service, you're responsible for any actions that the AI takes."[2]
- **Wells Fargo's** updated agreement, taking effect November 24, says: "Your use of any AI Agent is AT YOUR OWN RISK."[3]
- Every bank email Business Insider reviewed told customers not to share usernames, passwords or security codes.[2]

Why you might not get your money back

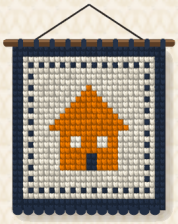
Federal Regulation E protects consumers from unauthorized electronic transfers. But a transfer made by someone you gave access to generally doesn't count as unauthorized, unless you've told your bank that person's access is no longer authorized.[4] How that rule applies to AI agents is still unsettled, which is why banks are spelling it out in their terms.[13] One more point for business owners: Regulation E defines a consumer as a natural person,[5] so its consumer protections may not reach a business account. Ask your bank what your business agreement says.

What to do

- **Don't give any third-party AI tool your bank username, password or security codes.**[2]
- **If you want AI help with money, use your bank's own assistant,** or a read-only tool that can analyze your finances but can't move money.[1,6]
- **If you already connected one,** disconnect it, change your banking password, and tell your bank in writing that the tool is no longer authorized.[4]
- **At work, set a simple rule:** no company banking, payroll or admin logins go into an AI tool unless leadership has approved that tool.

Why this matters

THE NUMBERS BEHIND THE SEASON



Scammers don't care whether they reach you at your desk or on your couch. They use the same scripts and, more and more, the same AI tools. A scam that starts at home can end up at work.

$20.9B
reported lost to internet crime in 2025, up 26% from 2024[14]

$3.05B
in business email compromise losses reported to the FBI in 2025, the second-largest category[14]

$2.1B+
lost to tech support scams in 2025[14]

$893M
lost across more than 22,000 complaints with an AI connection, the first year the FBI tracked it[15]

$3.5B
reported lost to imposter scams in 2025; nearly one in three fraud reports[16]

$2B+
reported lost to scams that started on social media in fiscal 2025, the top contact method by losses[17]

47%
of adults got a fake shipping alert in the past year, and 44% got a fake toll payment text[10]

Text
was the most commonly reported way scammers made contact in 2025[17]

The pattern under almost all of it

Something urgent, a reason to keep it quiet, and a payment you can't take back. Treasury's advisory names the same warning sign, a sense of urgency or authority, and warns against sending money or crypto to people you don't know.[11] You don't need to be a tech expert to beat that. You need permission to slow down, and a way to check.

What to watch for

SCAMS SHOWING UP RIGHT NOW



Each one has a work version and a home version. Same trick, different target.

Fake delivery and toll texts

Work: a text to a staff phone linking to a fake sign-in page.

Home: "Your package is on hold" or "you owe an unpaid toll."

Fake package delivery was the most reported text scam in FTC data for 2024.[18] Don't tap links you didn't ask for.

"Move your money to keep it safe"

Work: a "bank fraud team" calls finance about suspicious wires.

Home: a "fraud alert" says to move savings to a "safe" account.

Some of the costliest scams start with a fake security alert, often from a bank.[16]

AI voice and video impersonation

Work: a call that sounds like an executive approving an urgent wire.

Home: a call that sounds like your child or grandchild in trouble.

A scammer needs only a short clip of a voice to clone it.[19] Criminals use AI audio to impersonate public figures and loved ones.[20]

Payment-redirect email

Work: a real vendor's "new bank details," from a hijacked or lookalike address.

Home: a contractor or landlord "changing" where your deposit goes.

Wire transfers made up the bulk of business email compromise losses.[14]

Gift card requests

Work: "Grab some gift cards for the team and send me the codes."

Home: a "utility" or "government" caller who wants gift cards.

The FTC says anyone who demands payment by gift card is always a scammer.[21]

Fake tech support

Work: a "help desk" call asking staff to install remote-access software.

Home: a pop-up or renewal email with a number to call.

The FTC says a tech support call you don't expect is a scam, even if the number looks local.[22]

Fake stores, ads and charities

Work: lookalike "year-end giving" requests sent to staff.

Home: too-good deals in social ads, and charities that don't exist.

About one-third of adults got a request to donate to a fraudulent charity.[10]

Travel and breach follow-ups

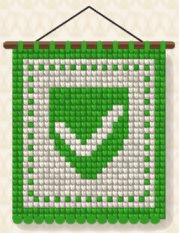
Work: "trip change" or "loyalty account" emails to traveling staff.

Home: fake booking sites and "your points are expiring" messages.

Fake airline booking sites are spreading through social ads.[12] After the Expedia breach,[7] sign in through the official app instead of email links.

For owners and managers

A CHECKLIST FOR YOUR BUSINESS



Pick two this week. Each item says why it matters right now.

- **Turn on MFA for email, banking, payroll and remote access.**
  Choose an authenticator app or security key over text codes. CISA notes text and voice codes can be phished or stolen through SIM swaps.[23] This week's exposed text messages are a reminder why.[8]

- **Write a call-back rule for payment changes.**
  Any new bank details get confirmed by calling a number you already have, never one in the message.[11]

- **Set an AI tool policy.**
  No company banking, payroll or admin logins in third-party AI tools. Banks now say the account holder carries the risk.[1,2]

- **Read your business banking agreement.**
  Regulation E defines a consumer as a natural person, so its protections may not reach a business account.[5]

- **Ask your IT provider about its remote-access tools.**
  This week's ScreenConnect attack came through a third-party add-on that bypassed MFA.[9] See page 9 for the questions.

- **Turn on automatic updates.**
  CISA says updates fix security risks and recommends turning on automatic updates.[24]

- **Keep offline, encrypted backups and test a restore.**
  CISA and the FBI recommend it because ransomware actors try to find and delete reachable backups.[25]

- **Train your team on texts, calls and video, not just email.**
  Text is now the top reported way scammers make contact,[17] and AI makes fake voices and video more believable.[20]

- **Make sure staff know who your real IT people are.**
  Never give remote access to someone who contacts you unexpectedly.[22]

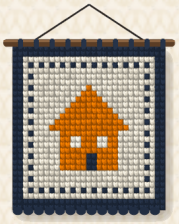
- **Ban gift card payments outright.**
  No real vendor, agency or executive needs them, and the FTC says anyone who demands them is a scammer.[21]

- **Warn traveling staff about "loyalty" and "booking" emails.**
  The Expedia breach and fake booking sites make these timely.[7,12]

- **Write down your first-hour call list.**
  Bank, IT provider and the FBI's IC3. The FBI's first step is calling your bank as soon as fraud is recognized.[26] See page 10.

For you and the people you love

A CHECKLIST FOR YOUR HOUSEHOLD



Do these with a parent, a teenager or a grandparent. Ten minutes at a time.

- **Pick a family safe word.**
  The FBI recommends a secret word or phrase your family can use to verify identity.[20] More on the next page.
- **Turn on MFA, starting with email.**
  Your email account resets everything else. Use an authenticator app over text codes where you can.[23,24]
- **Use a password manager.**
  CISA recommends passwords of at least 16 characters, random and unique for each account.[24]
- **Keep AI assistants out of your bank account.**
  Use your bank's own tools, or read-only apps that can't move money.[1,6]
- **Already connected one? Revoke it in writing.**
  Disconnect it, change your password and tell your bank it's no longer authorized.[4]
- **Limit what you post of your voice and face.**
  The FBI advises limiting online images and voice recordings that can be used to clone you.[20]
- **Never pay with gift cards because someone called you.**
  Anyone who demands payment by gift card is always a scammer.[21]
- **Know that your bank will never ask you to move money to "protect" it.**
  The FTC flags this as one of the costliest scams.[16]
- **Forward scam texts to 7726 (SPAM).**
  It helps your carrier spot and block similar messages.[18]
- **Freeze your credit at Equifax, Experian and TransUnion.**
  A freeze is free to place or lift, doesn't affect your score, and lasts until you lift it.[27]
- **Check charities and gift card balances before you give.**
  35% of adults say they've given or received a gift card with no balance.[10]
- **Book travel through the airline or hotel directly.**
  Fake booking sites are spreading through social ads this season.[12]

If you only do two things

TWO HABITS THAT STOP MOST OF IT



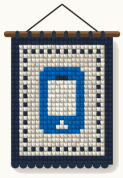
Real emergencies can wait two minutes for a phone call. Scams can't.



Pick a family safe word

The FBI recommends creating a secret word or phrase with your family to verify identity.[20] If a call sounds like someone you love asking for money, ask for the word. A voice can be copied. A word nobody posted online can't.

- Choose something that isn't online anywhere: not a pet's name, a street or a team.
- Share it in person, not by text or email.
- Ask for it before any money moves. If it's ever used for real, pick a new one.
- **At work, the same idea:** a second step for payment requests, such as a code or a call on a known number.



Hang up and call back

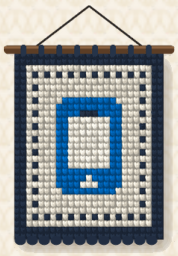
Caller ID can be faked: the FTC notes tech support scammers use fake caller ID to look like local businesses.[22] When something feels urgent, end the call or close the message, then reach the person or company at a number you already have. Treasury's 2026 advisory says the same: contact the person being impersonated another way, and pause to ask someone you trust.[11]

- A grandchild "in jail" or "in the hospital"
- A bank "fraud alert" telling you to move money to keep it safe
- A vendor with new bank details, or a boss who needs gift cards today

When you gather for the holidays

When family and friends get together this season, take five minutes after dinner. Pick your safe word, agree on the call-back rule, and ask whether anyone has connected an AI app to their bank account. It may be the most useful thing anyone brings to the table.

For businesses that use an IT provider



QUESTIONS FOR YOUR IT PROVIDER

This week's ScreenConnect attack hit IT providers and their clients.[8] A good provider will welcome these questions.

1. Which remote-access tools and add-ons are installed on our computers?

The attack came through a third-party add-on, with a shared access key that defaulted to blank, that bypassed the tool's user accounts, roles and MFA.[9]

2. Did this week's ScreenConnect activity touch our environment, and how did you check?

ConnectWise disabled five third-party add-ons across about 400 partner environments. Huntress advises not investigating infected computers through ScreenConnect itself.[9]

3. Is MFA required on every admin and remote-access account, and what kind?

CISA calls phishing-resistant MFA the most secure form and urges organizations to adopt it.[23]

4. When did you last test restoring our data from backup?

CISA and the FBI recommend offline, encrypted backups that are tested regularly.[25]

5. How fast are critical updates applied?

CISA added four actively exploited flaws to its catalog on November 18 alone.[9]

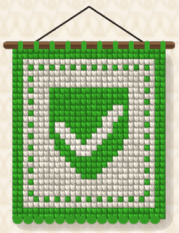
6. Who do we call first if something happens, and how fast will you respond?

For wire fraud, the FBI's first step is contacting the originating bank as soon as fraud is recognized.[26] Your provider should be the next call.

centrexIT is an IT provider, too. If you'd like a second opinion on any of these answers, that's exactly what our free assessment is for.

If it happens

WHAT TO DO IN THE FIRST HOUR



It happens to careful, smart people every day. Moving fast matters more than feeling embarrassed.

At your business

1. **Call your bank right away.** Ask for a recall or reversal of the payment, plus a Hold Harmless Letter or Letter of Indemnity.[26]
2. **Report it to the FBI at ic3.gov,** no matter how much was lost. IC3 can help banks and law enforcement with recovery.[28]
3. **Call your IT provider** before anyone tries to fix the affected computers.
4. **Check affected email accounts** for new rules that auto-forward or auto-delete messages.[29]
5. **Change passwords** on any account whose login you shared, and anywhere you reused it.[31]

At home

1. **Paid by card?** Call your bank or card company right away and ask whether they can reverse the charge.[30]
2. **Paid by gift card?** Contact the company that issued it, and keep the card and your receipt.[21]
3. **Gave an AI tool or a person access?** Tell your bank in writing that their access is no longer authorized.[4]
4. **Identity stolen?** Go to IdentityTheft.gov for a personalized recovery plan, and freeze your credit.[27]
5. **Report it** at ReportFraud.ftc.gov[16] and ic3.gov.[20] Then tell your family, so they can watch for follow-up calls.

Want to know where your business stands?

Take the free 2-minute cybersecurity assessment.

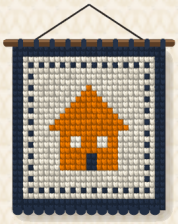
centrexit.com/assessment/cybersecurity/

centrexIT™

centrexIT is a San Diego managed IT and cybersecurity company, since 2002. People-First. AI-Amplified. Cyber IT. Share this guide with anyone you'd like to keep safe this season.

Check our work





1. TechCrunch, "More banks say customers using AI agents are on their own, even if they get hacked," Nov. 18, 2026. techcrunch.com/2026/11/18/more-banks-says-customers-using-ai-agents-are-on-their-own-even-if-they-get-hacked/
2. Business Insider via Yahoo Finance, "Banks are warning customers they could be liable for an AI agent's mistakes," Nov. 19, 2026. finance.yahoo.com/technology/ai/articles/banks-warning-customers-could-liable-100101120.html
3. Cryptopolitan, "Citi and PNC tighten rules as AI agents gain access to bank accounts," Nov. 2026. cryptopolitan.com/citi-and-pnc-tighten-rules-as-ai-agents-gain-access-to-bank-accounts/
4. Regulation E, 12 CFR Part 1005 (definition of unauthorized electronic fund transfer). ecfr.gov/current/title-12/chapter-X/part-1005
5. Regulation E, 12 CFR 1005.2(e), definition of "consumer." ecfr.gov/current/title-12/chapter-X/part-1005/subpart-A/section-1005.2
6. TechRadar, "Major US banks crack down on AI agent use by customers," Nov. 20, 2026. techradar.com/ai-platforms-assistants/major-us-banks-crack-down-on-ai-agent-use-by-customers-telling-them-theyre-on-their-own-if-it-gets-hacked-or-makes-a-mistake
7. Security Affairs, "Extortion Group Claims Theft of Nearly One Billion Expedia Traveler Records," Nov. 14, 2026. securityaffairs.com/203062/cyber-crime/extortion-group-claims-theft-of-nearly-one-billion-expedia-traveler-records.html
8. Kaseya, "The Week in Breach News: November 18, 2026." kaseya.com/blog/the-week-in-breach-news-11-18-26/
9. Sherlock Forensics, "Weekly Security Roundup: November 15 to 20, 2026," summarizing Huntress and ConnectWise reporting. sherlockforensics.com/blog/2026-11-20-weekly-security-roundup.html
10. AARP, "How to Avoid Fraud and Scams This Holiday Season," Nov. 11, 2026. aarp.org/press/releases/2026-11-11-how-to-avoid-fraud-and-scams-this-holiday-season-aarp-breaks-down-what-to-watch-out-for/
11. U.S. Treasury OCCIP, 2026 Seasonal Scam Advisory. home.treasury.gov/system/files/136/Treasury%20OCCIP%202026%20Seasonal%20Scam%20Advisory.pdf
12. Click2Houston, "Holiday travel scams are on the rise," Nov. 10, 2026. click2houston.com/news/local/2026/11/10/holiday-travel-scams-are-on-the-rise-how-to-avoid-fake-airline-booking-sites/
13. Yahoo Finance, "US Banks Fear Rogue AI Agents Inside Customer Accounts," Oct. 2026. finance.yahoo.com/markets/crypto/articles/us-banks-fear-rogue-ai-182636604.html
14. CyberScoop, "Cybercrime losses jumped 26% to $20.9 billion in 2025" (FBI IC3 2025 report). cyberscoop.com/fbi-internet-crime-complaint-center-annual-cybercrime-report/
15. Techlicious, "FBI Report: Online Scams Stole $20.9 Billion from Americans in 2025," Apr. 7, 2026. techlicious.com/blog/fbi-online-scam-losses-2025/
16. FTC, "FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025," June 15, 2026. ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025
17. FTC testimony, Joint Economic Committee hearing on the rising scam economy, 2026. ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf
18. FTC, "New FTC Data Show Top Text Message Scams of 2024," Apr. 2025. ftc.gov/news-events/news/press-releases/2025/04/new-ftc-data-show-top-text-message-scams-2024-overall-losses-text-scams-hit-470-million
19. FTC consumer alert, "Scammers use AI to enhance their family emergency schemes," Mar. 2023. consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
20. FBI IC3, PSA I-120324-PSA, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," Dec. 3, 2024. ic3.gov/PSA/2024/PSA241203
21. FTC, "Gift cards top scammers' wish lists," Data Spotlight, Dec. 2020, and "Holiday 'grift' exchange," Dec. 2020. ftc.gov/news-events/blogs/data-spotlight/2020/12/gift-cards-top-scammers-wish-lists
22. FTC, Cybersecurity for Small Business: Tech Support Scams. ftc.gov/business-guidance/small-businesses/cybersecurity/tech-support-scams
23. CISA, "Implementing Phishing-Resistant MFA" fact sheet, Oct. 2022. cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
24. CISA, "National Internet Safety Month: This June, Take 4 Easy Steps to Stay Safe Online" (Secure Our World). cisa.gov/news-events/news/national-internet-safety-month-june-take-4-easy-steps-stay-safe-online
25. CISA and FBI, #StopRansomware Guide. cisa.gov/stopransomware/ransomware-guide
26. FBI IC3, Business Email Compromise: What to do in case of a BEC incident. ic3.gov/CrimeInfo/BEC
27. FTC consumer alert, "Get a credit freeze to stop identity thieves," Sept. 2025, and "What to Know About Credit Freezes and Fraud Alerts." consumer.ftc.gov/consumer-alerts/2025/09/get-credit-freeze-stop-identity-thieves
28. FBI IC3, PSA I-060923-PSA, "Business Email Compromise: The $50 Billion Scam," June 2023. ic3.gov/PSA/2023/psa230609
29. North Carolina State Bar, "CEO and Wire Transfer Fraud Checklist." ncbar.gov/media/730467/news-image.pdf
30. FTC, Tech Support Scams. ftc.gov/techsupportscams
31. FTC, "How to Spot a Tech Support Scam" infographic. consumer.ftc.gov/articles/0557-infographic-how-spot-tech-support-scam

This guide is general information, not legal or financial advice. Bank terms vary; read your own account agreement.