COMMONWEALTH PAYROLL & HR

How to Outsmart The Next Wave of Payroll Cyber Fraud

March 10, 2026

isolved Fraud Prevention

isolved NETWORK PARTNER

Introductions

Jeff Plakans
Founder & President
Commonwealth Payroll & HR

Steve Lenderman, CFE, CFCI
Head of Fraud Prevention
isolved

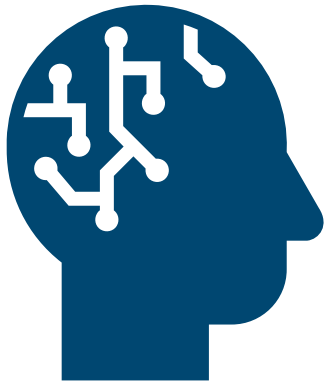
Agenda

- **Cybercrime Landscape**: What's Changing in 2026
- **Payroll Under Attack**: New Vectors & Vulnerabilities
- **Outsmarting the Scammers**: Tools & Tactics
- **Top 3 Trends for 2026**

Cybercrime Landscape: What's Changing in 2026

Rise of AI-driven Scams and Deepfake Impersonations

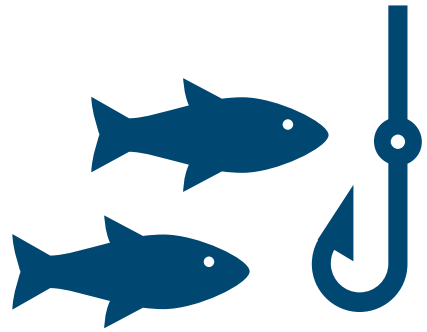
- **AI-scaled fraud**: Criminals now use automation to run thousands of scams simultaneously, making each interaction feel personalized and human.
- **Deepfake impersonations**: Voice cloning and synthetic video are being used to impersonate executives, IT staff, or even family members.
- **Synthetic relationships**: Fraudsters build long-term trust with victims using AI chatbots and deepfake "companions," before exploiting them financially.



Cybercrime Landscape: What's Changing in 2026

Social Engineering 2.0: Hyper-Personalized Phishing

- **Beyond generic emails:** Attackers now craft hyper-personalized phishing messages using stolen data, social media insights, and AI-generated text.
- **Multi-channel fraud journeys:** Victims are lured across SMS, social media, encrypted chats, and fake payment portals.
- **Voice phishing (vishing):** AI-driven voice cloning makes phone scams sound authentic, increasing success rates.

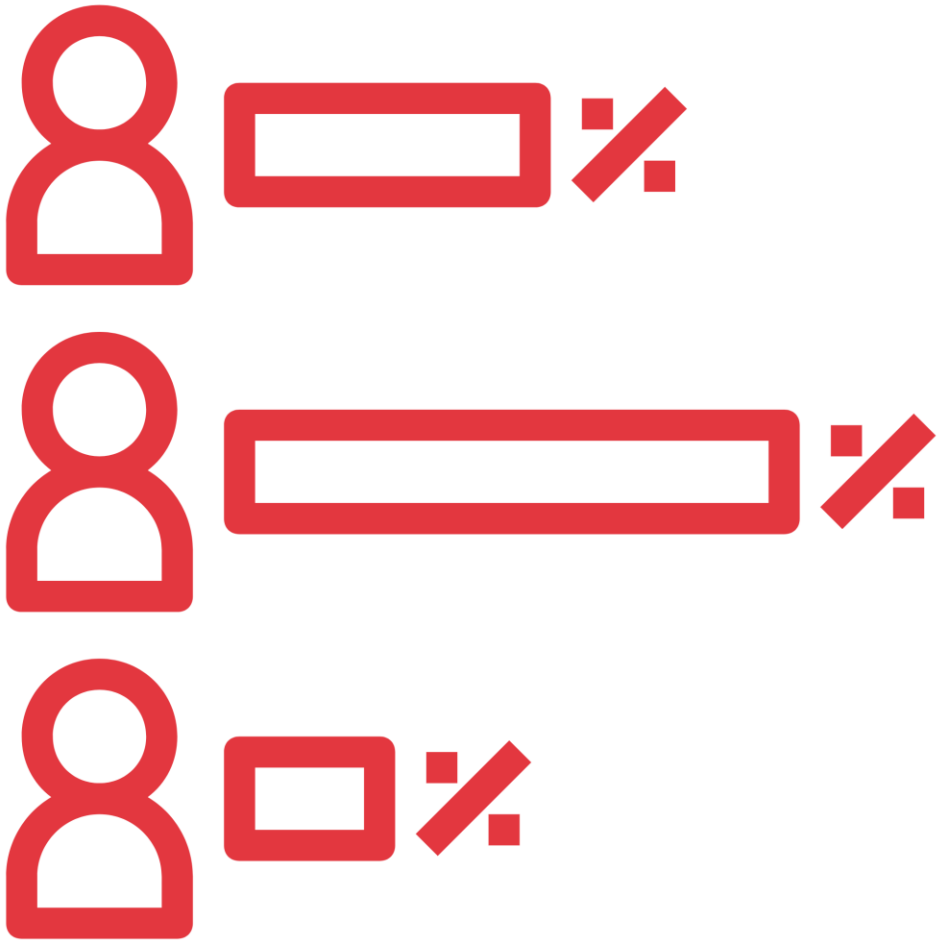


Cybercrime Landscape: What's Changing in 2026

Regulatory Shifts and Enforcement Priorities

- **Global divergence**: Europe continues to lead with AI regulation, while the U.S. is slower to impose strict controls.
  - Focus areas:
    - AI misuse (deepfakes, impersonation fraud)
    - Instant payment fraud and crypto-related scams
    - Data privacy and consumer protection
- **Enforcement trend**: Regulators are prioritizing cross-border collaboration and industry accountability, pushing organizations to adopt proactive fraud prevention measures even before mandates arrive.
- **Implication for SMBs**: Compliance will increasingly require not just technical safeguards but cultural and training initiatives.

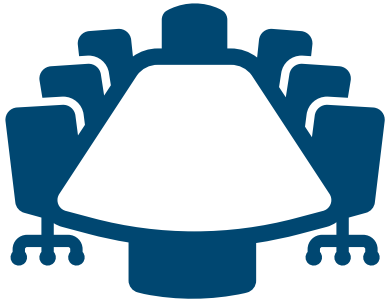
Let’s Take a Poll



Payroll Under Attack: New Vectors & Vulnerabilities

Business Email Compromise (BEC) Targeting Payroll Teams

- **AI-crafted emails**: Attackers will use generative AI to create flawless, context-aware messages that mimic internal tone and style.
- **Voice deepfakes**: Payroll staff may receive urgent “executive” calls using cloned voices to authorize changes.
- **Adaptive attacks**: AI will analyze prior communications to tailor timing and language for maximum success.



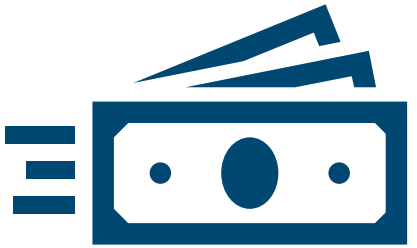
Business Email Compromise (BEC) – True Story

That time CommPayHR stopped a client's potential $80k loss due to Business Email Compromise…

Payroll Under Attack: New Vectors & Vulnerabilities

Fake Direct Deposit Change Requests

- **Automated personalization**: Fraudsters will scrape employee data from LinkedIn or breached HR records to make requests look authentic.
- **Synthetic identities**: AI will generate realistic fake employees with complete digital footprints to slip into payroll systems.
- **Real-time response**: AI bots will reply instantly to verification questions, making fraud harder to detect.



Payroll Under Attack: New Vectors & Vulnerabilities

Insider Threats and Credential Misuse

- **AI-assisted insiders**: Employees misusing access may rely on AI tools to cover tracks, automate credential abuse, or bypass monitoring.
- **Behavior masking**: AI can mimic “normal” activity patterns, making insider fraud harder to distinguish from legitimate actions.
- **Credential stuffing at scale**: AI will accelerate brute-force and credential-reuse attacks against payroll portals.

Payroll Under Attack: New Vectors & Vulnerabilities

Third-Party Payroll Platform Exploitation

- **Automated vulnerability scanning**: AI will continuously probe payroll vendors for weak APIs or misconfigurations.
- **Supply-chain fraud**: Compromising one payroll provider could expose dozens of SMBs simultaneously.
- **AI-driven malware**: Smarter malware will adapt to defenses in real time, persisting longer inside vendor systems.

Outsmarting the Scammers: Tools & Tactics

Multi-Factor Authentication and Access Controls

- Require MFA for all payroll and HR system logins.
- Limit access based on role — only authorized staff can make changes.
- Regularly review and update access rights to prevent privilege creep.

Outsmarting the Scammers: Tools & Tactics

Behavioral Analytics and Anomaly Detection

- Establish baselines for normal payroll activity (login times, device use, transaction frequency).
- Flag deviations such as sudden changes from new devices or unusual locations.
- Use AI-driven anomaly detection to catch emerging fraud tactics beyond static rules.

Outsmarting the Scammers: Tools & Tactics

Secure Payroll Change Protocols

- Enforce dual verification for direct deposit or payroll changes (e.g., call-back confirmation).
- Segregate duties so no single employee can authorize and execute changes.
- Maintain audit trails and conduct regular reviews of payroll updates.

Outsmarting the Scammers: Tools & Tactics

Employee Education

- Provide ongoing awareness training tailored to payroll staff.
- Use gamified simulations with scores and ratings to keep engagement high.
- Celebrate employees who report suspicious activity, reinforcing vigilance as a cultural norm.

Employer Responsibilities

- **Data Security**: Use strong encryption to protect sensitive company information accessed by remote workers, especially over unsecured networks.
- **Multi-factor Authentication (MFA)**: Secures the many access points created by a dispersed remote workforce, adding extra verification layers beyond passwords to reduce vulnerabilities.
- **Education**: Provide ongoing employee training on data security—covering phishing awareness, strong password habits, and risks of unsecured networks—to ensure remote workers understand and uphold their role in protecting company data.

Top 3 Trends for 2026

Agentic AI Attacks

- **Autonomous fraud bots**: AI agents capable of planning and executing complex payroll fraud schemes without human oversight.
- **Adaptive strategies**: These agents learn from failed attempts and adjust tactics in real time.
- **Multi-vector campaigns**: Simultaneous attacks across email, payroll portals, and vendor systems to overwhelm defenses.

Top 3 Trends for 2026

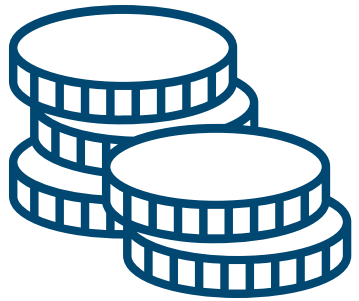
Deepfake & Synthetic Media Fraud

- **Executive impersonation**: Fraudsters use deepfake video or voice to authorize payroll changes.
- **Synthetic employee identities**: AI generates realistic digital personas with fake credentials to infiltrate payroll systems.
- **Emotional manipulation**: Deepfake “urgent calls” exploit trust and pressure payroll staff into bypassing protocols.

Top 3 Trends for 2026

Crypto in Payroll

- **Stablecoin adoption**: More companies experimenting with crypto payroll for speed and global reach open fraud vectors
- **Fraud risks**: Fake wallets, phishing for private keys, and unstable exchange rates exploited by attackers.
- **Regulatory uncertainty**: Compliance challenges as jurisdictions tighten rules on crypto payments and reserves.



How We Protect Your Data

- Since 2010, **CommPayHR** has partnered with **isolved** to deliver secure, certified HCM technology.
- Customers benefit from layered security, advanced protection, specialized hardware, and a global team of **3,500+ cybersecurity experts**.
- As cyberthreats grow, having a trusted partner with a secure system and reliable support is essential to **protecting payroll and employee data**.
- We pair **powerful technology** with **personalized service** to keep your business secure and well-supported.

Wrapping Up

- **AI is reshaping fraud**: Attacks are faster, smarter, and harder to detect.
- **Payroll is a prime target**: BEC, fake deposit requests, insider misuse, and vendor exploitation are evolving.
- **Crypto adds complexity**: New fraud risks emerge with wallets, stablecoins, and regulatory uncertainty.
- **Defense must be layered**: MFA, anomaly detection, secure change protocols, and employee awareness are essential.
- **Culture drives resilience**: Leadership messaging, daily reminders, and peer recognition reinforce vigilance.
- **Prepare for 2026 and beyond**: Invest in adaptive, AI-powered defenses and proactive compliance today.

Remember…

When, *not if*, it hits the fan…
Are CommPayHR & isolved going to be there for you?
YES!

Our **Network Partnership** with isolved provides you with **bank-level security**…**protecting you and your employees!**

Thank You!

Whether you have a question or want to learn more, we're happy to speak with you.

(978) 599-1050

jeff.plakans@commpayhr.com

COMMONWEALTH PAYROLL & HR

slenderman@isolvedhcm.com

https://www.linkedin.com/in/steve-lenderman/

isolved Fraud Prevention