

Cyberfraud Exposed

The Top Threats Targeting You and Your Organization

Table of contents

03	Introduction	08	Living off the Land Attacks
04	The Human Element	09	Deepfakes, Synthetic Voices & AI-Enhanced Deception
05	The Billion-Dollar Threat	10	The Enforcement Challenge
06	Social Scams	11	How Trusted Partners Strengthen Fraud Defense
07	Insider Threats & Initial Access Brokers	12	Conclusion: Lower Risk, Build Resilience

Introduction

Fraud Has Gone Digital

Cyberfraud has evolved into something far more sophisticated than just stolen credit cards or fake websites. Modern cybercriminals don't just attack systems; they manipulate the trust employees place in colleagues, executives, and vendors. They study how your teams communicate and learn your business workflows, then exploit the human relationships that keep operations running smoothly. Every email from the CEO, invoice from a trusted vendor, and urgent request from a colleague becomes a potential threat vector.

From mid-sized manufacturers to enterprise corporations, organizations worldwide face an adversary that operates with the efficiency of a Fortune 500 company. These criminal networks employ specialists, operate 24/7, and continuously refine their tactics based on what works. They target the moments when employees are most vulnerable: end-of-quarter financial pressure, rushed approvals, or late-afternoon requests when people are distracted.

The stakes extend far beyond immediate financial loss. When cyberfraud succeeds, organizations face operational disruption, regulatory scrutiny, erosion of customer trust, and brand damage that can take years to repair. In 2024, the FBI reported that Business Email Compromise scams **cost organizations \$55 billion over the previous 10 years**, and that's just one type of fraud.

Bitdefender is a trusted partner in the fight against cybercrime, working with law enforcement agencies worldwide to dismantle criminal operations and protect organizations from evolving threats. Understanding how these fraud schemes work and why they succeed is the first step toward building resilient defenses that protect both your assets and your people.



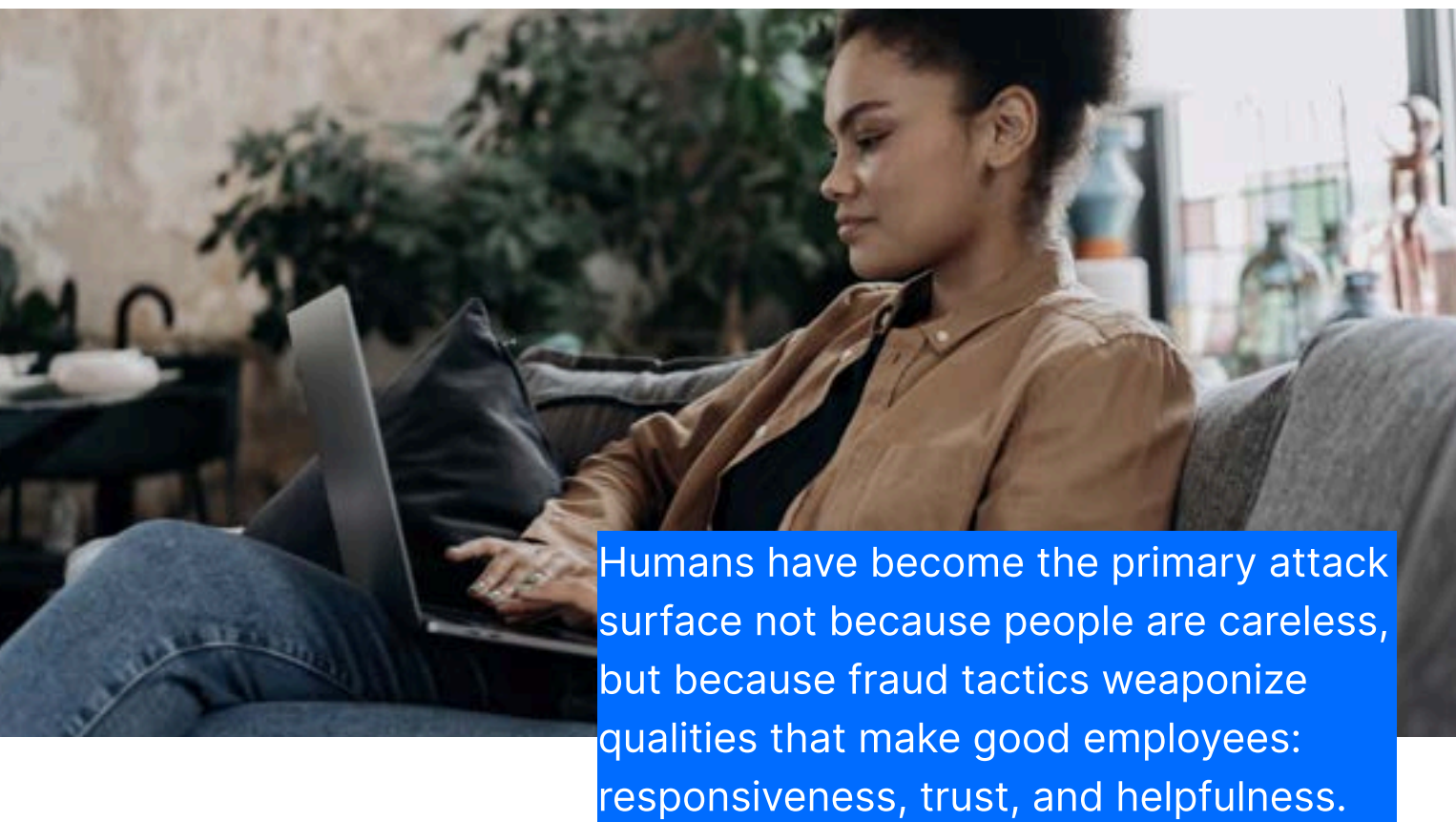
These criminal networks employ specialists, operate 24/7, and continuously refine their tactics based on what works.

The Human Element:

How People Became the #1 Attack Surface

Firewalls and antivirus software protect systems, but who protects the people using them? Cybercriminals have discovered that convincing an employee to click a link or approve a payment is often easier than breaking through technical defenses. **Humans have become the primary attack surface** not because people are careless, but because fraud tactics weaponize qualities that make good employees: responsiveness, trust, and helpfulness.

Security teams once drew a line between what was “inside” or “outside” their networks. Remote work, cloud applications, and personal devices accessing corporate resources have changed that, so now the perimeter is wherever your employees work.



Humans have become the primary attack surface not because people are careless, but because fraud tactics weaponize qualities that make good employees: responsiveness, trust, and helpfulness.

Where Attackers Strike: Everyday Business Weak Points

Email and collaboration platforms like Microsoft Teams and Slack have become battlegrounds for fraud. Vendor and billing workflows offer rich opportunities to change payment details on invoices, intercepting transactions, or impersonating suppliers. Identity gaps create vulnerability through password resets and authentication processes. When employees use personal devices to access corporate systems, they create pathways that bypass traditional controls. The genius of modern fraud is how much it looks like “business as usual.”

Common Manipulation Tactics

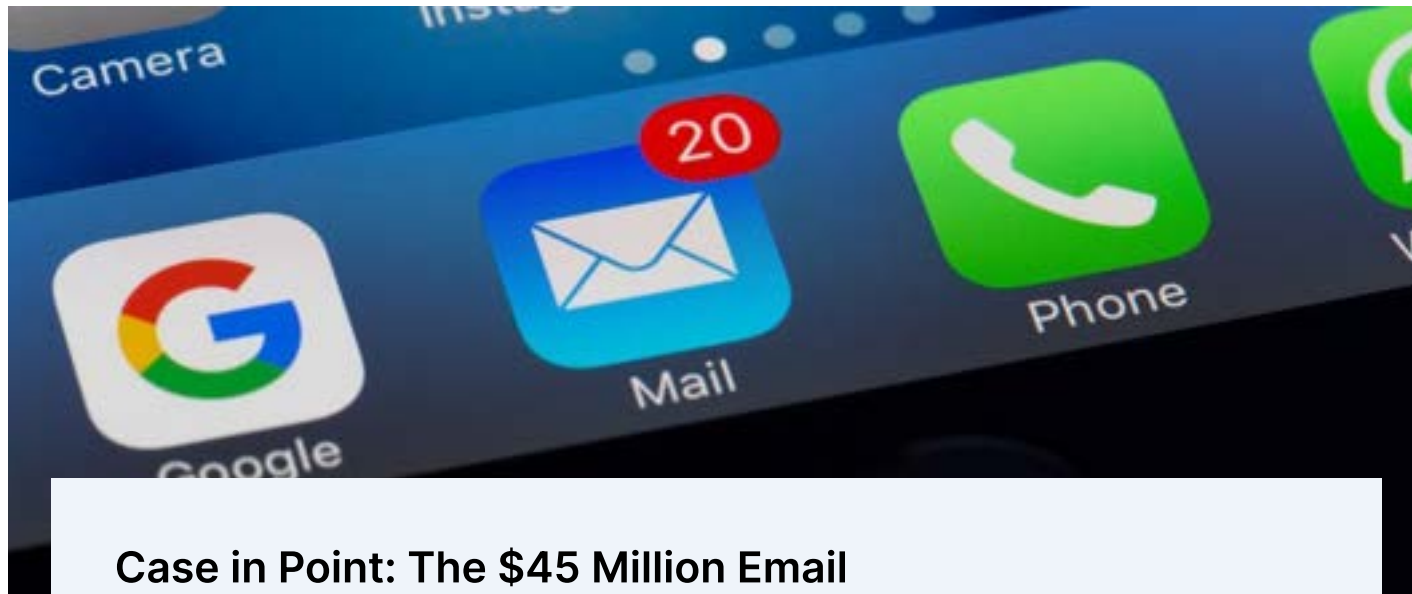
Impersonation ranks among hackers’ most effective techniques, with **89% using fake identities** to deceive targets. Cybercriminals pose as executives, vendors, or IT support, crafting emails that mirror genuine communications. They use urgency, fear, and authority to drive victims to act. Verify phrases like “We need this payment processed today” or “Your account will be suspended” can short-circuit careful thinking.

Attacks now weaponize psychology at scale. MFA fatigue exploits exhausted users who approve authentication prompts just to stop notifications. Criminals now use personalization and rapport-building, researching targets on LinkedIn and referencing real projects. According to Bitdefender research, over 70% of successful cyberattacks use legitimate tools and trusted channels to evade detection.

The Billion-Dollar Threat:

Business Email Compromise

Business Email Compromise is the most financially devastating cyberfraud tactic today. Unlike ransomware, BEC operates quietly. Attackers don't install malware or lock systems; they simply convince someone with financial authority to send money, and once funds transfer, recovery becomes nearly impossible. The FBI reported that **BEC schemes cost organizations \$2.77 billion** in 2024 alone.



Case in Point: The \$45 Million Email

Leoni AG, a billion-dollar manufacturer of automotive cables, suffered one of **Europe's most expensive BEC attacks**. The CFO at Leoni's Romanian factory received what appeared to be an urgent email from the company's CEO requesting a wire transfer. The **CFO followed standard procedures** and transferred 40 million euros (approximately \$45 million). But there was just one problem: The account belonged to scammers who had impersonated the CEO. The criminals were never found. When Leoni publicly announced the fraud, the company's stock dropped 8 percent in a single day, erasing roughly \$60 million in market value. In addition to the stolen funds, Leoni lost approximately \$100 million due to a convincing email.

Why BEC Works

BEC exploits the mundane reality of business operations. Organizations regularly process hundreds or thousands of payments. Employees expect payment requests from executives and vendors through corporate email; that's how business works. And criminals count on that expectation.

The best criminals don't rely on a single email. They orchestrate multichannel campaigns: an email followed by a phone call with a spoofed caller ID, or even an extended conversation, to build credibility. Some monitor your communications for weeks, studying payment patterns so they know precisely when to strike. The problem is that detection is slow, while payment processing is fast. By the time someone questions the transaction, often days or weeks later, funds have already moved through multiple accounts in different countries.

Prevention Strategies

Prevention starts with workflow changes that make fraud more complicated to execute:

- **Multiperson approval:** Require at least two people to authorize transactions above certain thresholds, ensuring no single employee can be deceived into approving a fraudulent payment.
- **Out-of-band verification:** When you receive unusual or high-value requests, confirm them through a separate communication channel. Pick up the phone and call a known number, not the number provided in the suspicious email.
- **DMARC email authentication:** Implement protocols that verify messages actually come from the domains they claim, making it much harder for criminals to spoof your CEO's email address.
- **AI-powered anomaly detection:** Deploy systems that flag communications deviating from standard patterns; things like emails sent at odd times, payment amounts outside typical ranges, or requests that bypass usual approval chains. These systems learn what normal looks like for your organization, then alert you when something doesn't fit.

Social Scams:

Where Fraud Meets Human Emotion

Romance and investment scams used to just target people in their personal lives, but scams perpetrated over dating apps, social media, and personal email **cost Americans \$697.3 million last year**. But now, criminals are bringing these same emotional manipulation techniques into the workplace.

Romance-Driven Access

Today's romance scammers play a long game; they're after access, not just cash. After establishing an emotional connection, attackers make technical requests that sound harmless. "My computer isn't working right. Can you help me install this program?" "I'm trying to open this file, but can't, can you check if it works for you?" Each request is a disguised attempt to compromise the victim's device.

Here's why this works: employees no longer separate their personal and work devices. They check corporate email on personal phones, access company systems from home laptops, and use the same devices for both dating apps and VPN connections. So when a romance scammer compromises someone's personal device, they automatically gain access to corporate resources. The employee thinks they're being helpful to someone they trust. In reality, they've given criminals a pathway into your organization's network.

Investment Schemes Targeting Employees

Fake investment opportunities have become recruitment tools for insider threats. A professional-looking contact reaches out to an employee on LinkedIn with a lucrative opportunity, such as cryptocurrency, a startup venture, or exclusive trading access. The criminal ensures early investments show returns to build credibility. Once the employee is hooked, the real pitch comes: earn additional money by providing company information or facilitating access.

These schemes work because criminals build convincing identities. They create detailed LinkedIn profiles, active social media accounts, professional networks, and AI-generated photos that look real. Generative AI tools craft personalized messages demonstrating industry expertise, making them nearly indistinguishable from legitimate business contacts.

Financial pressure makes people vulnerable. An employee struggling with bills, facing unexpected expenses, or worried about job security becomes more receptive to "opportunities" they'd normally dismiss. What starts as "just sharing harmless information" can escalate as criminals leverage that initial cooperation into a deeper compromise.

Insider Threats & Initial Access Brokers

Sometimes attackers don't need to break in; they already have the keys or have bought them from someone who does.

Insider-Driven Fraud

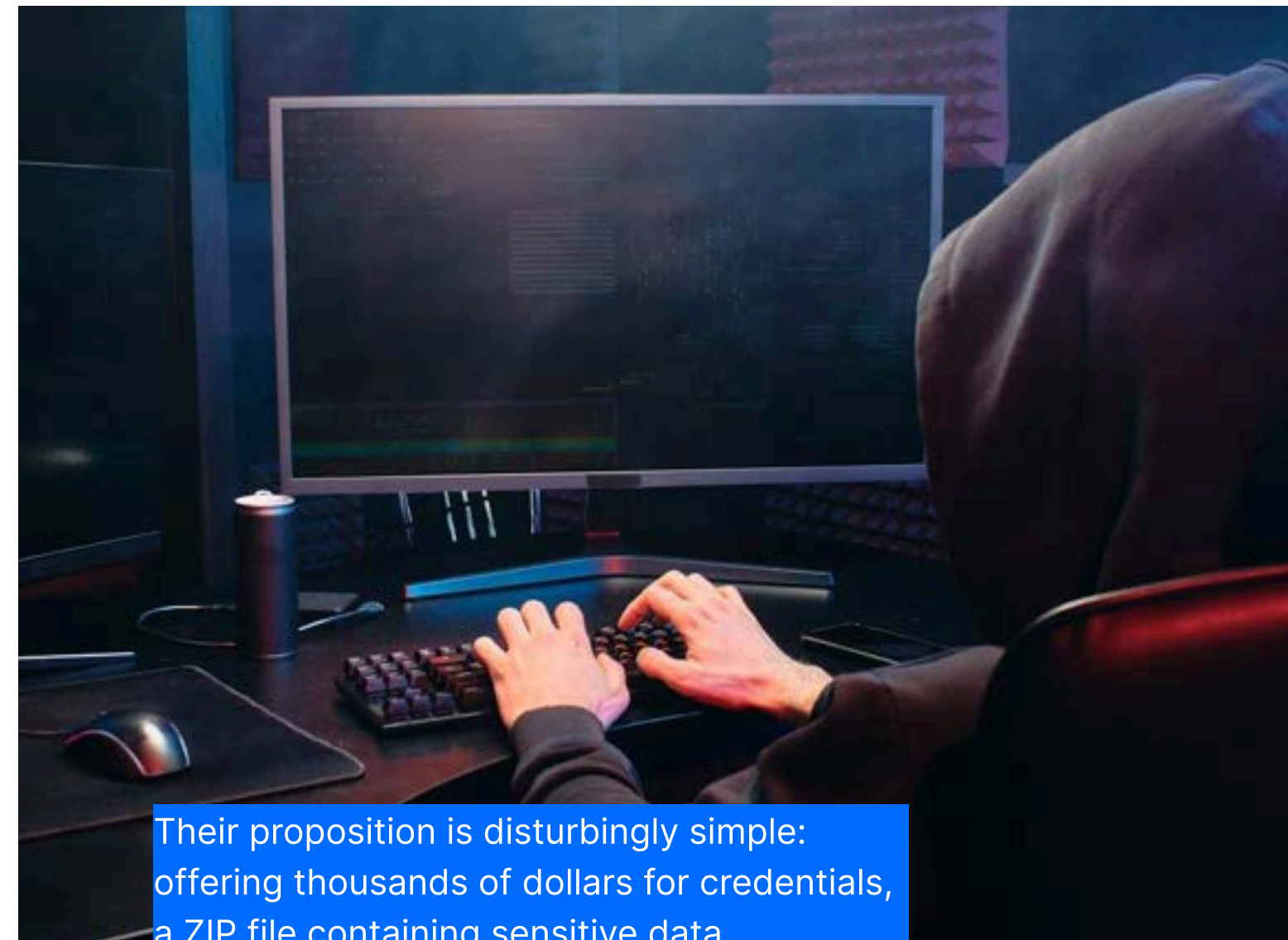
Economic stress can drive some employees to compromise intentionally. Financial difficulties, perceived unfair treatment, or direct criminal recruitment can motivate insiders to steal data or facilitate unauthorized access. Threat actors actively reach out on dark web forums, offering to pay employees for access to their organizations. Their proposition is disturbingly simple: offering thousands of dollars for credentials, a ZIP file containing sensitive data, or help establishing network access.

Initial Access Brokers

Initial Access Brokers (IABs) have professionalized the [ransomware supply chain](#). These criminals facilitate a break-in into an organization and then sell that access to other attackers. Think of it this way: if ransomware is a home burglary, IABs are specialists who pick the lock and walk away, allowing other criminals to enter and steal valuables.

The business model is straightforward: IABs sell verified access on dark web marketplaces. Listings advertise access by industry vertical, organization size, revenue, and access type. Prices range from hundreds of dollars for small-business access to tens of thousands of dollars for enterprise environments. And if their regular buyers decide to pass? It typically takes [one to three days to auction the information](#) to the highest bidder.

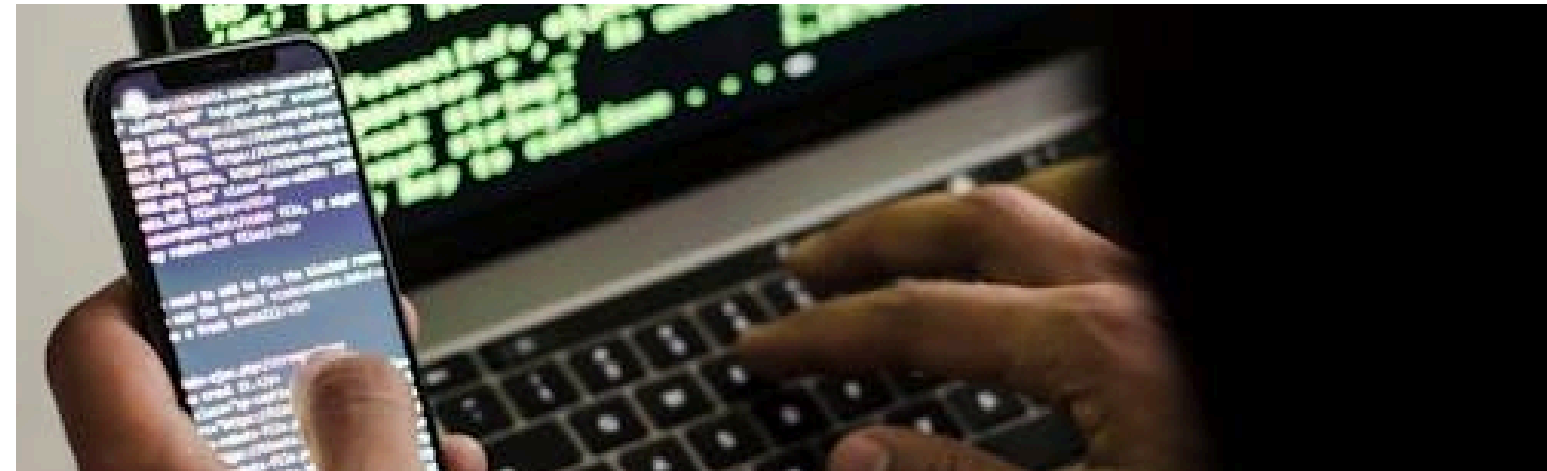
Proactive detection matters because IABs typically establish access long before attacks occur. Your organization may remain compromised for weeks or months as attackers conduct reconnaissance, escalate privileges, and plan their operations.



Their proposition is disturbingly simple: offering thousands of dollars for credentials, a ZIP file containing sensitive data, or help establishing network access.

Living off the Land Attacks

More than **70% of cyberattacks now use legitimate tools** to evade security defenses. Criminals learned that stolen administrative credentials and authorized software generate fewer alerts than custom malware. "Living off the Land" attacks leverage tools already present in PowerShell, Windows Management Instrumentation, and remote administration utilities to conduct malicious activities while appearing to perform legitimate IT operations.



Credential Theft
Phishing or IABs



Normal Login
Authorized user



Reconnaissance
Map network



PowerShell
Escalate privileges



Evade Detection
Appears normal

How LOTL Makes Fraud Invisible

Criminals kick off their LOTL attacks by harvesting credentials, either phishing for usernames and passwords or purchasing them from IABs, then using them to log in normally, where security tools see authorized user activity, not a breach. Once inside, attackers move laterally using standard protocols like Remote Desktop Protocol or Server Message Block.

Then, criminals use built-in tools such as PowerShell to escalate privileges without installing malware. These techniques often go unnoticed precisely because the tools are legitimate. Employees authorize access, thinking they're helping IT, and once criminals are in, they can do whatever they want.

Consider a common scenario: an employee receives a Teams call that shows "IT Support" as the caller. They answer, expecting routine technical assistance. The caller explains they need to perform system updates and asks the employee to install a remote access program. It sounds reasonable, after all, IT routinely installs updates remotely. The employee complies, unaware that they've just given criminals a direct pathway into the network.

Reducing the LOTL Attack Surface

Real-time behavioral analytics detect anomalies that signature-based security tools miss. Instead of looking for known malware, behavioral analytics identifies suspicious patterns, such as PowerShell scripts executing at unusual times, administrative tools running on workstations that don't require them, or data movement deviating from normal operations.

To build effective defenses against LOTL techniques, focus on visibility, access control, and monitoring:

- Unified visibility is essential. Connect your endpoint security, identity systems, and network monitoring into a single operational view. When these platforms share information, they reveal attack patterns that individual alerts miss.
- Implement identity-based defenses. Deploy multifactor authentication across your organization, not just for VPN access. Deploy privileged access management to control who can use administrative tools and when. Apply least-privilege policies, so employees have only the access they need to do their jobs, nothing more.

Consider 24/7 monitoring. LOTL attacks often happen during nights, weekends, or holidays when internal security teams are understaffed. Managed Detection and Response services provide round-the-clock monitoring specifically designed to detect LOTL techniques.

Deepfakes, Synthetic Voices & AI-Enhanced Deception

Artificial intelligence has democratized trust counterfeiting. Cybercriminals leverage the same generative AI technologies that power customer service chatbots, but they use them to impersonate executives, forge documents, and fabricate evidence that traditional verification methods can't detect.

AI-Driven Impersonation Tactics

Criminals use generative AI to mimic how your people communicate. The technology captures communication patterns, decision-making language, and relationship dynamics.

Deepfake voice scams and video call spoofing have **already cost organizations millions**. Criminals train AI models on publicly available audio to synthesize voices that perfectly match executives' speech patterns, cadence, and verbal habits. A CFO receives a call that sounds exactly like the CEO requesting an urgent wire transfer. Real-time video deepfakes take this further, allowing criminals to conduct live video conferences while impersonating executives. When someone sees and hears what appears to be their boss on a Teams call, skepticism evaporates.

AI-crafted emails clone writing styles and signatures with unprecedented accuracy. Large language models analyze previous correspondence to mimic tone, vocabulary, formatting preferences, and even subtle grammatical patterns unique to individuals.

Verification in a Post-Truth Workplace

When AI can counterfeit voices, videos, and writing styles, organizations need verification protocols that criminals can't replicate:

- Always verify out-of-band. Never trust identity at face value. When someone requests unusual actions via email or messaging, confirm through a separate communication channel.
- Establish executive communication protocols. Implement agreed-upon phrases, security questions, or verification procedures that executives use for sensitive requests.
- Deploy behavior-based anomaly detection. Use systems that identify timing irregularities, urgency patterns, and deviations from established payment request norms.
- Train employees to challenge requests. Transform organizational culture by encouraging healthy skepticism. Create safe channels for employees to verify unusual requests without fear of appearing distrustful or questioning authority. Trust must now be validated, not assumed.

The Enforcement Challenge

Law enforcement is cracking down on cyberfraud, but criminals often move faster than authorities. The prosecution rate for cybercrimes is estimated **at 0.05%**. Yet despite these daunting odds, international cooperation has achieved significant victories: **Operation DisrupTor**, **Operation Endgame**, and other coordinated efforts have dismantled major criminal infrastructure.

Jurisdiction challenges complicate enforcement. Cybercriminals operate across borders, attacking victims in one country from servers in another while laundering money through cryptocurrency exchanges in a third jurisdiction. Legal systems struggle to coordinate when crimes span multiple nations with different laws, extradition treaties, and investigative capabilities.

Cryptocurrency anonymous flows let criminals move money without traditional banking oversight. While blockchain transactions are technically traceable, sophisticated laundering techniques make it incredibly difficult to follow the money.

The importance of public-private cooperation cannot be overstated. Technology companies, cybersecurity firms, and law enforcement agencies must share intelligence, coordinate responses, and develop joint strategies. When defenders collaborate as effectively as criminals, the balance shifts toward protection rather than exploitation.

How Trusted Partners Strengthen Fraud Defense

Even with modern defenses, organizations can't fight cyberfraud alone. Today's criminal operations are unparalleled in their level of sophistication, persistence, and specialization, and they require equally sophisticated, persistent, and specialized defensive capabilities. Partnering with experienced cybersecurity providers transforms your isolated security efforts into comprehensive defense strategies.

Why Unified Security > Tool Sprawl

Many organizations accumulate a piecemeal collection of security tools over time, each generating alerts and requiring management. But this tool sprawl creates gaps that LOTL and BEC attacks exploit.

When security solutions don't communicate, attackers can move between them undetected. To reduce the gaps that LOTL and BEC attacks exploit, you must embrace integrated platforms that share intelligence and correlate events.

By adopting a unified security approach, you're connecting endpoint activity, email analysis, network traffic monitoring, and identity management into a single operational view. That way, when one component detects suspicious behavior, the others automatically adjust detection thresholds and investigation priorities.

A unified security solution offers visibility across endpoints, identities, networks, and cloud environments and reveals attack patterns that isolated tools miss. For example, an employee credential compromise may generate a single alert in your identity system, which is easy to overlook. But when that same credential accesses an unusual endpoint, moves laterally, and then attempts data exfiltration, the pattern becomes obvious. The catch? Your security platforms need to share information and context to connect those events into a coherent attack narrative.

You don't have to fight cyberfraud alone. Explore [Bitdefender's Trusted Partner in Cybercrime Defense](#) capabilities to learn how our unified security solutions and managed detection and response services can enhance your organization's defenses.

MDR/Co-Managed SOC as a Force Multiplier

Attacks often occur when security teams are understaffed. In fact, [more than half of all ransomware incidents arise on weekends or holidays](#). 24/7 monitoring and rapid response capabilities provide protection that most organizations cannot sustain internally. Managed Detection and Response services ensure that experts continuously monitor your environments, investigate alerts, and respond to threats regardless of time zone or calendar.

Traditional security tools look for known malware signatures, but MDR analysts take a different approach: they watch for suspicious behavior. They understand how criminals operate and recognize patterns that automated systems miss: the slow reconnaissance phase where attackers map your network, the careful lateral movement between systems, and the strategic timing that avoids detection. These behaviors appear normal to automated tools, but trained analysts recognize them as threats.

Large criminal operations have resources, expertise, and technology that rival corporate IT departments. And supporting your global organization with enterprise-grade protection helps level the playing field. When you partner with a cybersecurity leader like Bitdefender, you gain advantages most organizations can't build internally: threat intelligence gathered from monitoring millions of endpoints globally, research from specialized teams who reverse-engineer new malware daily, and analysts who've investigated thousands of incidents across every industry.

Criminal tactics constantly evolve, and so should your defenses. For the greatest level of protection, combine organizational knowledge with partner expertise. After all, your internal teams understand your business operations, applications, and what normal activity looks like in your environment. But external partners bring specialized knowledge, advanced technologies, and cross-industry experience; they've seen the same attacks hit hundreds of other organizations and know what works to stop them.

Conclusion:

Lower Risk, Build Resilience

Fraud succeeds when trust is unprotected. Cybercriminals have professionalized their operations, specialized their roles, and weaponized the technologies and workflows that power modern business. They've transformed cyberfraud into a thriving underground economy with profit margins rivaling those of legitimate enterprises.

Organizations facing these threats need more than technology. They need awareness, layered protections, and trusted partners. Awareness transforms employees from points of vulnerability into active defenders. When people understand manipulation tactics, recognize suspicious patterns, and feel empowered to verify unusual requests, criminals lose their primary attack vector.

Layered protections ensure that when one defense fails, others compensate. Email authentication stops impersonation. Behavioral analytics detect LOTL techniques. Payment workflows prevent unauthorized transfers. Identity controls limit credential theft impact. No single solution stops all fraud, but you can dramatically reduce your risk by deploying comprehensive strategies.

Organizations facing these threats
need more than technology

Working with a trusted partner can extend your organization's capabilities. Bitdefender has fought cybercrime for over 20 years, partnering with 32 law enforcement agencies worldwide, releasing 30+ free ransomware decryptors, and preventing \$1.6 billion in funding for criminal operations.

Strengthen your fraud defenses:

- Explore comprehensive solutions: Discover unified security platforms, managed detection and response services, and threat intelligence designed to combat modern cyberfraud. [Learn more about Bitdefender's cybersecurity solutions.](#)
- Watch expert insights: Hear directly from Bitdefender security experts about ransomware evolution, BEC attacks, initial access brokers, and AI-powered fraud tactics. Watch the ["Hit From All Sides: Cyber Fraud Targeting Organizations"](#) webinar.
- Listen to frontline perspectives: Get ongoing insights into the latest cyber threats, fraud tactics, and defense strategies from the experts fighting cybercrime every day. Listen to the [CYBERCRIME: From the Frontline](#) podcast.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
111 W. Houston Street
Suite 2105, Frost Tower Building
San Antonio, TX 78205

bitdefender.com

Trusted. Always.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.