

Sanford Gladding
President

ATS Leverages Advanced Business Email Compromise Technology

Leading Managed Intelligence Partner (MIP), Helps Block Email-Based Attacks, the Preferred Vector for Hackers

CONCORD, CA – October 27, 2026– ATS a leading managed intelligence partner (MIP), announced today that the company is deploying the latest in advanced email and account protection technology to help small and mid-sized businesses (SMBs) defend against Business Email Compromise, phishing and other increasingly sophisticated cyberattacks targeting employees through their inboxes.

For years, employees were told to look for obvious warning signs in a suspicious email: misspelled words, poor grammar, strange formatting or awkward language. That advice is becoming less effective. Cybercriminals now use artificial Intelligence (AI) to create polished, professional emails in seconds. Attackers can research a company, identify its executives and vendors, learn how employees communicate and then create messages that look remarkably similar to legitimate business correspondence. In advanced cases, hackers are creating deep-fake videos or audio recordings to impersonate managers. In other words, the phishing email asking an employee to update banking information may no longer be obviously fraudulent.

"Most people still picture a scam email as something obviously fake," said Sanford Gladding, President at ATS . "But those easy clues are disappearing. Today, a fraudulent message can use your employee's real name, reference an actual vendor, sound like your CEO and look almost identical to the messages your team receives every day. Historically, awkward phrasing or spelling mistakes were dead giveaways, but as AI has become more sophisticated, so too have hackers' methods. That's what makes this new generation of attacks so dangerous."

Email remains the preferred attack vector for the majority of social engineering breaches, according to Verizon's 2026 Data Breach Investigations Report. One of the most common forms of email-based fraud is Business Email Compromise, often called BEC. A BEC attack occurs when a criminal impersonates someone the employee trusts, such as an executive, coworker, customer or vendor. In some cases, the criminal simply creates a convincing fake email. In more advanced attacks, the criminal gains access to a legitimate employee's email account. Once inside, the attacker can become significantly more difficult to detect.

They may study existing conversations, learn which vendors the company works with and wait for an opportunity to insert themselves into a real transaction. A cybercriminal may send a fake request to change payment instructions, redirect an invoice, ask an employee to purchase gift cards or send additional phishing messages from a legitimate company account. Since the email is coming from someone the employee recognizes, the normal warning signs may not be there.

"If somebody breaks into an employee's real mailbox, they do not have to pretend to be that employee anymore," Gladding said. "They are that employee as far as everyone receiving the email is concerned. They can see the conversations, understand the relationships and send something at exactly the right moment. That's why protecting the inbox alone is no longer enough."

To address that problem, ATS recommends a layered approach designed to protect organizations both before and after an attempted account compromise. The first layer works like an intelligent security checkpoint for email. Instead of simply searching messages for known viruses or suspicious words, the technology analyzes the email itself and the context surrounding it. It can examine whether the sender appears legitimate, whether a domain is attempting to imitate a trusted company, whether a link or attachment appears dangerous and whether the message resembles known phishing or impersonation techniques. Suspicious emails can then be blocked or quarantined before the employee ever has an opportunity to interact with them.

But no security system can assume that every attack will be stopped at the front door. That's why another layer continuously looks for signs that someone may have successfully gained access to an employee's Microsoft 365 account. It can identify unusual login behavior, suspicious activity inside a mailbox, unauthorized forwarding rules, stolen sessions and other behaviors that may indicate that the person operating the account is not actually the employee.

When suspicious account activity is discovered, technology can help contain the incident quickly by ending unauthorized sessions, disabling methods attackers use to maintain access, removing malicious email rules and retracting phishing messages that may have already been sent to other employees. This is especially important because a compromised employee account can quickly become a company-wide problem. An attacker who successfully takes over one mailbox can use that trusted identity to target coworkers, customers and vendors.

"The goal is not to make everyone afraid of email," Gladding concluded. "It's too valuable of a tool and isn't going anywhere. The goal is to give employees the freedom to do their jobs while leveraging Business Email Compromise technology to protect them. Cybercriminals are using AI, so businesses have to respond with better technology as well. Our job is to make sure our clients are not fighting today's attacks with yesterday's defenses."

ABOUT ATS

ATS Communications is an award-winning managed intelligence provider serving small and medium-sized businesses throughout Northern California and across the United States. The company distinguishes itself by unifying managed IT services, enterprise-grade cybersecurity, and practical AI strategy into a single, integrated offering – enabling SMBs not only to remain secure and operational, but alsl to become more intelligent, efficent, and competitive. ATS designs, implements, and proactively supports enterprise IT networking and infrastructure, comprehensive cybersecurity solutions, unified communications, business continuity, cloud technologies, and video surveillance through a managed services model centered on reliability, security, and optimization.

With more then 50 years of experience, AT has earned a strong reputation as a trusted technology partner committed to delivering best-practice solutions that enhance performance, strengthen resilience, and create measurable business value. ATS has offices in Concord and Sacramento, California. For more information, call the corporate office in Concord at (925) 602-1500 or visit www.teamATS.com.