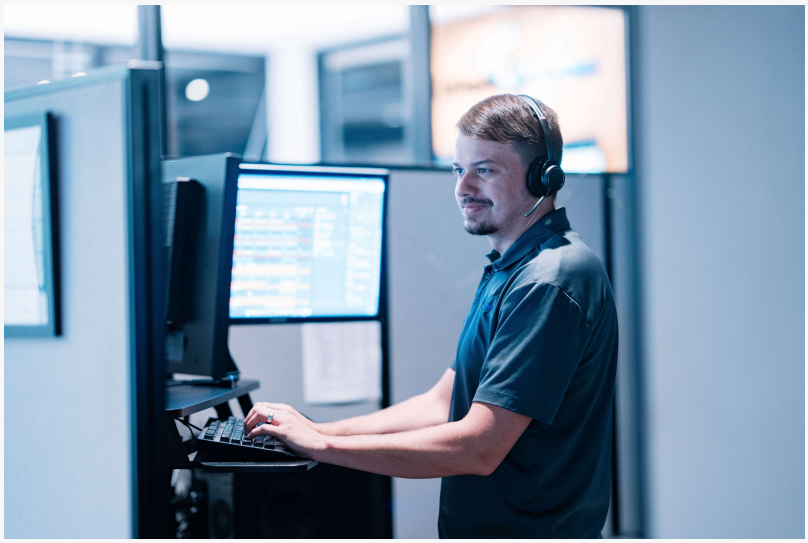
FBI Warns New Microsoft 365 Attack Could Give Hackers Access to Business Emails, Files, and Communications

Local ethical hacker with 15+ years of experience says incident demonstrates why technology alone cannot stop today's cybercriminals

AUGUSTA, GA, GA, UNITED STATES, June 2, 2026 /EINPresswire.com/ -- Business owners across Georgia and South Carolina are being urged to pay close attention to a recent FBI warning about a sophisticated cyberattack targeting Microsoft 365 users.

The FBI recently issued a Public Service Announcement regarding "Kali365," a phishing-as-a-service platform that allows cybercriminals to gain access to Microsoft 365 accounts using legitimate Microsoft authentication processes. Once access is obtained, attackers may be able to view emails, Microsoft Teams conversations, OneDrive files, SharePoint data, business documents, and other sensitive information stored within a company's Microsoft environment.

Importantly, Microsoft itself has not been breached.



An IntelliSystems cybersecurity professional monitors and helps protect business systems against evolving cyber threats. Experts say the FBI's recent Microsoft 365 warning highlights the importance of skilled cybersecurity practitioners, not just security

IntelliSystems is a leading provider of managed IT services and cybersecurity solutions throughout Georgia and South Carolina.

Instead, attackers are exploiting human behavior and legitimate authentication workflows to trick users into unknowingly granting access to their accounts.

According to local cybersecurity experts, that distinction is critical.

"This wasn't a failure of Microsoft," said Robert Smith, Director of Cybersecurity and Risk Management at IntelliSystems, ethical hacker, and cybersecurity practitioner with more than 15 years of experience. "It's a reminder that modern cybercriminals increasingly target people rather than technology. Attackers are finding ways to exploit trust, human behavior, and gaps in security programs rather than simply hacking software." For many business owners, the risk extends far beyond email.

Robert Smith, Director of Cybersecurity and Risk Management at IntelliSystems, is an ethical hacker and cybersecurity practitioner with more than 15 years of experience helping organizations reduce risk and strengthen their cybersecurity defenses.

Because Microsoft 365 serves as the central hub for communication, collaboration, and file storage for many organizations, a compromised account can potentially expose financial records, customer information, contracts, internal communications, intellectual property, stored passwords, and confidential business data.

"Many people hear a story like this and think it's an email problem," Smith said. "In reality, email is often the key that unlocks everything else. If an attacker gains access to the wrong Microsoft account, they may also gain access to Teams conversations, shared files, cloud storage, sensitive business documents, and information that can be used to launch additional attacks."

The FBI warning also highlights how dramatically the cybercrime landscape has evolved. Platforms like Kali365 provide cybercriminals with sophisticated attack tools, automation, phishing templates, and technical support that previously required advanced expertise to develop independently.

"Hackers now have their own IT departments," Smith explained. "There are organized groups providing tools, support, training, and infrastructure to cybercriminals around the world. Someone who may not have had the skills to conduct a sophisticated attack a few years ago can now gain access to capabilities that rival those of large criminal organizations."

Smith, who regularly performs cybersecurity risk assessments, penetration testing, and security evaluations for organizations throughout Georgia and South Carolina, says the sophistication of today's attacks continues to increase while the technical barrier to entry for cybercriminals continues to decrease.

> Cybersecurity is not a product. It is a program. A good IT and cybersecurity provider knows how to design, implement, and maintain a real security program."
>
> *Robert Smith, Director of Cybersecurity and Risk Management, IntelliSystems*

"Attackers no longer need advanced technical skills to launch sophisticated campaigns," Smith said. "Many of the tools, infrastructure, and support systems are now readily available. That's why businesses must focus on building real security programs rather than relying solely on technology."

According to IntelliSystems, the incident exposes a dangerous misconception many businesses still have about cybersecurity.

Many organizations believe purchasing security software or checking a compliance box automatically makes them secure. In reality, cybersecurity tools are only one component of an effective security strategy.

"Anyone can buy a toolbox," Smith said. "That doesn't mean they can repair your house or rebuild your engine. The same principle applies to cybersecurity. Tools are important, but if they aren't properly selected, configured, monitored, maintained, and regularly tested by experienced professionals, they cannot provide the protection businesses expect."
Smith holds multiple advanced cybersecurity certifications, including CISSP, CISM, CISA, CASP+, and AAISM, and has spent more than fifteen years helping organizations identify vulnerabilities, reduce risk, and strengthen their cybersecurity defenses.

The company warns that many low-cost IT providers unintentionally create risk because they lack the advanced expertise, resources, or security capabilities necessary to address today's threat landscape.

"The less a provider charges, the less they're typically able to do," Smith said. "In many cases, they aren't cutting corners intentionally. They simply don't have the training, personnel, or security resources required to build and maintain a mature cybersecurity program."

According to IntelliSystems, the businesses most successful at defending against modern threats understand that cybersecurity is not a product. It is a program.

"A good IT and cybersecurity provider knows how to design, implement, and maintain a real security program," Smith said. "That includes technology, monitoring, employee education, policies, procedures, incident response planning, and continuous improvement. No software package alone can accomplish that."

The FBI warning serves as another reminder that even the most widely used and trusted business platforms can become targets when cybercriminals exploit human behavior and security gaps.

For business owners, the question is no longer whether attackers will attempt to gain access. The question is whether their organization has the people, processes, and expertise necessary to stop them.

About IntelliSystems
Founded in 1993, IntelliSystems provides managed IT services, cybersecurity, compliance consulting, cloud solutions, business communications, and technology strategy for organizations throughout Georgia and South Carolina.
The company supports more than 200 organizations and approximately 3,000 end users annually across Augusta, Columbia, Greenville, Savannah, and Macon. IntelliSystems is the only company in Georgia and South Carolina currently holding the GTIA Cybersecurity Trustmark Assured designation, an independent third-party validation recognizing organizations that meet the highest standards for cybersecurity practices, controls, and operational excellence. Fewer than 60 companies worldwide currently hold the designation.

With more than 200 technical certifications across its engineering and cybersecurity teams, IntelliSystems helps organizations reduce risk, improve productivity, and align technology with business goals through proactive technology management and advanced cybersecurity expertise.

Kristin Cato
IntelliSystems
+1 706-842-3215
KristinC@intellisystems.com
