On June 20, 2025, major insurance company Aflac disclosed that it had experienced a cyber incident within its network. Although the company confirmed that it identified and resolved the incident in a matter of hours and remained operational throughout, various types of sensitive stakeholder files (e.g., claims data, health history, Social Security numbers and personal contact information) were potentially compromised during this time frame. This incident marks the third large-scale cyberattack targeting a U.S. insurance company in the last few weeks. Each attack involved some degree of advanced social engineering tactics and ransomware; according to reports from Google Threat Intelligence, this indicates a connection to the well-known cybercrime group Scattered Spider. In the days since Aflac reported the incident, cybersecurity experts have voiced concern over the possibility of a continued attack spree across the insurance industry, urging financial and underwriting businesses to be on "high alert."

Scattered Spider, which consists of experienced hackers across the United States and Europe, is believed to have first formed in 2022. These hackers are known for leveraging sophisticated phishing scams and multifactor authentication exploits to launch disruptive ransomware attacks. Since its inception, the cybercrime group has been tied to several attacks on high-profile organizations worldwide. Scattered Spider generally focuses on a single industry at a time, attacking a series of businesses in the same sector for an extended period. In 2023, the group was assumed responsible for cyber incidents impacting multiple Las Vegas hotels and casinos operated by Caesars Entertainment and MGM Resorts. During the first half of 2025, the group was connected to two different system outages among global retailers: Marks & Spencer and Co-op in April and Victoria's Secret in May. In recent weeks, Scattered Spider appears to have shifted its focus to the U.S. insurance industry, being linked to cyberattacks on Philadelphia Insurance Companies and Erie Insurance prior to the Aflac incident.

In light of these developments, businesses in the insurance sector should prepare for a possible influx of social engineering attempts and ransomware attacks. Businesses should closely monitor their threat detection systems to swiftly identify unusual network activity and instruct employees, especially those working at help desks and call centers, to diligently watch for and report suspected phishing scams. In addition, businesses should review their cyber incident response plans to promote prompt remediation efforts following an attack. Contact us today for more industry updates.

Phishing attacks, in which cybercriminals manipulate users into disclosing sensitive information or installing malware through fraudulent communications, have been a persistent cybersecurity threat, often resulting in significant financial and reputational damage for impacted businesses. Recently, cybercriminals have begun leveraging artificial intelligence (AI) to power these attacks, making them more convincing and difficult to detect. Traditional phishing attacks are more generic, prone to errors and contain red flags (e.g., misspellings, incorrect names and grammatical errors) that are relatively easy to spot. AI-powered phishing attacks, on the other hand, are highly personalized, linguistically polished and difficult to differentiate from legitimate communications. These types of cyberattacks are also more easily scalable and increasingly targeted. For example, AI-led attacks may use "spear-phishing" schemes, in which fraudulent communications are sent to specific recipients, or business email compromise tactics, where cybercriminals impersonate corporate leaders (e.g., a CEO or partner) by hacking into their account or creating a realistic counterfeit message with an illegitimate request for sensitive information or payment. AI is changing traditional phishing techniques in several key areas, including enhanced personalization and social engineering capabilities, greater automation and scale, and simplified bypassing of standard safeguards. While AI-powered phishing attacks present new risks, businesses can take several steps to protect their operations:

- **Deploy advanced security solutions.** Utilizing anti-phishing software with AI-driven detection capabilities and context-based defenses can help companies' security systems evolve as the attacks advance.
- **Strengthen email and identity security.** Businesses should implement multiple measures to ensure email accounts are secure. Requiring multifactor authentication and routinely changing strong, unique passwords can make it more difficult for cybercriminals to infiltrate them. Email filters, firewalls, email authentication protocols and other security measures should also be utilized.
- **Educate and empower employees.** Staff should receive ongoing security awareness training that teaches them about the latest cybersecurity threats and hackers' newest tactics. Businesses should conduct phishing simulations to help employees recognize and respond effectively to fraudulent communications.
- **Develop comprehensive policies.** Clear data protection policies should be created, communicated and enforced. They should be regularly reviewed and updated to respond to emerging cyberthreats.

Contact us today for further risk management guidance.

While most cyberattacks involve users being manipulated into doing certain tasks—whether it's sharing login credentials, downloading dangerous attachments or clicking on harmful links—that help hackers compromise their systems or data, some incidents can be launched without these exchanges. In particular, zero-click attacks entail hackers leveraging software flaws in devices and applications to deploy malicious code, all without any user interaction.

Zero-click attacks can affect businesses in many ways, leading to stolen assets, damaged systems and technology, and regulatory and legal penalties. That's why it's vital for businesses to implement the following mitigation measures:

- **Maintain updated software.** Businesses should make it a priority to regularly update all workplace devices, operating systems, applications and firmware to help patch known vulnerabilities and other security weaknesses, thereby blocking cybercriminals from exploiting this technology.
- **Utilize multilayered security solutions.** By equipping their devices with advanced threat identification systems, antivirus programs, firewalls and intrusion detection tools, businesses can ensure greater visibility of their entire IT infrastructures and watch for any abnormal activity.
- **Establish segmented networks.** To prevent cybercriminals from traveling laterally through their systems and expanding attack surfaces, businesses should segment their networks. This way, hackers will only be able to compromise a small portion of corporate resources at a time, minimizing the risk of large-scale damage.
- **Vet all vendors and applications.** Businesses should carefully evaluate all third-party software vendors and applications, especially niche or lesser-known providers, for possible security flaws before finalizing contracts.

Contact us today for additional cybersecurity resources.