AI-Driven Polymorphic Phishing

A Rising Threat to Government Agencies

Office of Information Technology
Division of Information Security
APRIL 2026

Artificial intelligence (AI) is accelerating the evolution of phishing attacks. AI-driven polymorphic phishing uses machine learning to generate constantly changing, highly personalized phishing messages designed to bypass traditional email filters and deceive even experienced employees.

Unlike traditional phishing, polymorphic attacks never look the same twice. AI can tailor messages using public records, staff directories, and open-source intelligence to impersonate agency officials, vendors, or partner organizations. Some campaigns now incorporate deepfake voice or video technology, increasing the risk of fraud, credential theft, and unauthorized access.

Government agencies are prime targets because of their access to sensitive citizen data, financial systems, critical infrastructure, and national security information. A single compromised account can lead to data breaches, ransomware incidents, business email compromise, and the disruption of essential public services.

Key Risk Factors:

- Rapidly evolving phishing content that evades detection
- Impersonation of trusted officials or contractors
- Credential theft and account takeover
- Financial fraud and procurement manipulation
- Supply chain infiltration

IHS Users Can Combat AI-Driven Polymorphic Phishing by Following These Strategies:

- Require secondary verification for financial or sensitive requests.
- Use the Cofense “Report Phishing” button in your Outlook toolbar to report and verify the authenticity of the sender’s email address with the IHS Cybersecurity Operations Center (CSOC).
- Keep up with the latest cybersecurity news and trends to recognize potential phishing attempts.
- Learn about common phishing tactics and how AI can enhance them.
- Create complex and unique passwords for all accounts and use multi-factor authentication whenever possible.
- Avoid clicking on unknown or suspicious links, especially those from untrusted sources.
- If you suspect a phishing attempt, report it to your email provider and the appropriate authorities.

By following these steps, regular users can reduce their risk of falling victim to AI-driven polymorphic phishing attacks.

Bottom Line:

AI-driven polymorphic phishing represents a modern, adaptive cyber threat that demands stronger technology, smarter policies, and more vigilant employees. Agencies that proactively modernize their defenses today will be better positioned to protect public trust tomorrow.

For questions or further information, please contact the IHS Office of Information Technology, Division of Information Security, at cybersecurity@ihs.gov.

You must immediately report all lost, stolen, or compromised Government-Furnished Equipment (GFE) mobile devices within 24 hours to your Area ISSO or the IHS Cybersecurity Operations Center (CSOC) at incident@ihs.gov or 866-347-2762 (866-DIS-CSOC) 24 hours a day, 7 days a week.