SCSO QUARTERLY

STATE CYBERSECURITY OFFICE

THE QUARTERLY NEWSLETTER FROM THE STATE CYBERSECURITY OFFICE

First Quarter 2026

Resilience in Action: Understanding Today's Threats

Email: SCSO@arkansas.gov

Web: https://sas.arkansas.gov/state-technology/cybersecurity/

Welcome to the latest SCSO Quarterly Update!

As we kick off 2026, the State of Arkansas has made a significant investment in implementing and deploying CrowdStrike services across the enterprise to strengthen our cybersecurity defenses. This represents a strong commitment and a material step forward by our state leaders in protecting state technology and information assets. However, even with these advanced tools in place, our people remain the most essential component in building resilience against evolving threats. Your awareness, vigilance, and commitment to security practices are critical, and we are going to need your help.

Simple Ways You Can Help

1. **Complete KnowBe4 training promptly**
2. **Verify emails and phone calls**
3. **Use strong, unique passwords** – Do not reuse passwords intended to protect state systems and assets.
4. **Report suspicious activity immediately**
5. **Protect sensitive information** – Never share login credentials or confidential data without verification.
6. **Stay alert to unusual requests** – Pause and verify, as attackers can mimic legitimate users.

Understanding the Evolving Threat Landscape

The State Cybersecurity Office leverages multiple sources of threat intelligence, including CrowdStrike, to stay informed and align defensive strategies across the enterprise. By understanding the tactics and patterns of adversaries, staff are better equipped to recognize suspicious activity and take action to protect state systems and information. Recent insights highlight evolving threats in the threat landscape that require attention:

- **Breakout time is shrinking:** The time it takes for an adversary to move laterally across a network reached an all-time low in the past year. On average, lateral movement now occurs in just **48 minutes**, with the fastest observed breakout happening in a mere **51 seconds**. This underscores how quickly threats can escalate once an initial breach occurs.
- **Voice phishing (vishing) attacks are surging:** Adversaries are increasingly using phone calls to manipulate victims with persuasive social engineering. These attacks grew **442%** between the first and second half of 2024, highlighting the need for vigilance beyond email and digital channels.
- **Initial access attacks are on the rise:** In 2024, more than half of all observed security weaknesses involved attackers trying to gain entry into systems. A growing underground market allows criminals to buy and sell access to company networks, making it easier for them to break in.
- **Interactive intrusions are on the rise:** Modern cyber threats are increasingly dominated by "interactive intrusion" techniques, where attackers **manually perform actions** to achieve their objectives. Unlike traditional malware, these intrusions mimic legitimate user or administrator behavior, making them extremely difficult to detect. The **government is among the top 10 industries targeted** by these sophisticated attacks.

These trends make it clear: threats are faster, smarter, and more targeted than ever. Understanding the speed and sophistication of these attacks helps us take the "Simple Ways You Can Help" to heart and prevent small incidents from becoming major breaches.

CROWDSTRIKE