NEW MEXICO OFFICE OF CYBERSECURITY

Public Service Announcement:

Strengthen Your Cyber Defenses Amid Rising Cybersecurity Threats

Several public bodies in New Mexico have recently experienced cyber incidents that have crippled operations and diverted scarce public resources. These incidents, coupled with recent changes in cybersecurity policy at the federal level demonstrate that it is crucial for public bodies to remain vigilant and proactive in protecting your digital infrastructure and data.

Cyber threats continue to evolve, exploiting vulnerabilities in networks, applications, and systems. A lapse in security can lead to data breaches, financial losses, and operational disruptions.

To enhance your cybersecurity posture, prioritize the following:

1. Maintain Cyber Hygiene – Regularly update software, use strong passwords, enable multi-factor authentication (MFA), and educate employees on phishing and social engineering threats.

2. Utilize Attack Surface Management (ASM) – Continuously monitor and assess your external digital footprint to identify and remediate vulnerabilities before attackers exploit them.

3. Conduct Penetration Testing (PT) – Simulate real-world cyberattacks to test your defenses and uncover weaknesses that need immediate attention.

4. Leverage Vulnerability Management as a Service (VMAAS) – Implement continuous scanning and remediation strategies to mitigate risks effectively and stay ahead of emerging threats.

Cybersecurity is a shared responsibility. Stay informed, be proactive, and use the right tools to protect your organization from potential attacks. The Office of Cybersecurity provides ASM, PT and VMAAS services (via Securin) at no cost to New Mexico's K-12s.

Stay safe, stay secure!

For more information on strengthening your cybersecurity strategy, contact the Office of Cybersecurity at nmcybersecurity@cyber.nm.gov