SNO
A smarter tomorrow.



Fortifying Against Cyber Threats - How SNO Works to Protect Clients from Cyber-Crime



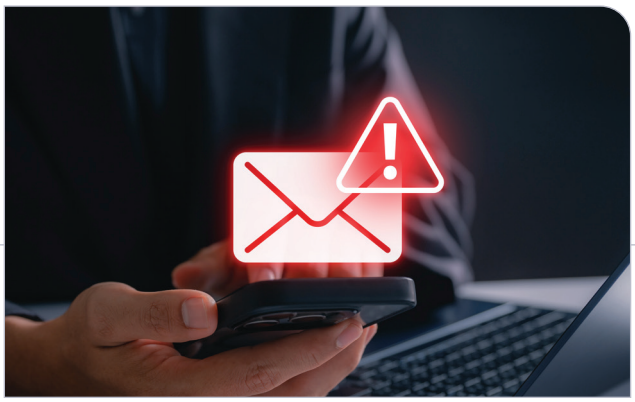
Introduction

In today's digital landscape, cyber-crime remains a persistent threat to businesses of all sizes, but especially to small and medium-sized businesses (SMBs). With the rise of remote work and digital operations, ensuring network security has become more critical than ever. SNO specializes in managed, network, desktop, and remote device services tailored for SMBs, allowing IT teams to focus on business growth rather than security challenges. This case study explores a recent phishing attack attempt thwarted by SNO, illustrating the company's robust security measures and the value they provide to clients.

Challenge

The threat landscape for SMBs is increasingly complex, with cyber-criminals employing sophisticated tactics to infiltrate systems. According to a 2022 report by Cybersecurity Ventures, global cyber-crime costs were forecast to reach $10.5 trillion annually by 2025. SMBs are particularly vulnerable due to limited resources and expertise in cybersecurity.

In this case, a SNO-managed services client with operations across multiple countries and remote employees in various time zones faced a significant threat. A phishing attack targeted an LA-based employee, threatening to compromise sensitive data and disrupt global operations. The attack was a two-part strategy: an Adversary in The Middle (AiTM) attack capturing the employee's credentials and MFA code, followed by malware deployment on the user's device.





Global cyber-crime costs were forecast to reach

$10.5 trillion

annually by 2025

Source: Cybersecurity Ventures

Solution

SNO's comprehensive security approach combines proactive monitoring, rapid response, and robust preventative measures. Their UK-based Operations Centre operates 24/7, providing round-the-clock vigilance and support. The company is certified with ISO20000 and ISO27001, ensuring adherence to the highest standards of security and service management.

Key Security Features:

Network and Endpoint Monitoring: Constant surveillance of network traffic and endpoints to detect anomalies.

Multi-Factor Authentication (MFA): Enhanced login security to thwart unauthorized access.

Incident Response Protocols: Swift actions to contain and mitigate threats.

User Training: Regular training sessions to educate employees about phishing and other cyber threats.

Implementation

When the phishing email was sent to the LA-based employee at 14:38 local time, it was engineered to bypass conventional protection systems. However, SNO's sophisticated monitoring systems detected the anomaly when the attacker attempted to log into the user's Microsoft 365 account from an unusual location in Virginia, using a Linux-based device.

Response Timeline:

1. **Alert and Investigation:** At 22:43 UK time, SNO's Operations Centre received an alert about the suspicious login attempt. An analyst immediately investigated and contacted the user, confirming the login attempt was unauthorized.
2. **Immediate Action:** Within 30 minutes, SNO blocked further login attempts, revoked active sessions, removed the user's personal email from MFA, and quarantined the device for further inspection.
3. **Preventative Measures:** Over the next two hours, multiple login attempts were blocked. A full suite of tests on the user's laptop revealed malware, prompting a complete wipe and reinstall. The user's access was swiftly reinstated post-reinstallation.

Within **30** minutes

SNO blocked further login attempts



Over the next **2** Hours

multiple login attempts were blocked

Results

SNO's timely intervention prevented a potentially devastating breach that could have compromised the client's global operations. The security measures not only thwarted the immediate threat but also safeguarded other employees from similar phishing emails that had bypassed initial defenses.

Benefits Achieved:

- **Prevention of Data Breach:** Quick detection and response ensured no data was compromised.
- **Business Continuity:** Minimal disruption to the client's operations, maintaining trust and operational efficiency.
- **Enhanced Security Posture:** Post-incident analysis and reinforcement of security measures mitigated future risks.

Conclusion

SNO's proactive and comprehensive approach to cybersecurity underscores the importance of robust IT and network management for SMBs. By dedicating resources to continuous monitoring and rapid response, SNO empowers IT teams to focus on strategic initiatives while safeguarding against cyber threats.

This case study highlights how SNO's managed services not only protect against cyber-crime but also enable businesses to operate securely and efficiently in an increasingly digital world. For SMBs seeking to enhance their security posture, SNO offers tailored solutions that align with business goals, ensuring peace of mind and a secure path to growth.



CLIENT PERSPECTIVE

"SNO's rapid response contained the threat before it could affect our wider operations. Their round-the-clock monitoring and decisive action gave us confidence that the incident was under control."

IT DIRECTOR, GLOBAL MANAGED SERVICES CLIENT