Case Study

KnowBe4 Shields City of Edinburgh Council from Attacks that Evade SEG Detection

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Industry	Location
Government	Scotland

Challenge

Close a critical gap in their security stack in the face of evolving phishing threats

Providing a range of public services to approximately half a million citizens, The City of Edinburgh Council needs the right security defenses in place to protect their systems and data from sophisticated cyber threats.

“With a workforce of nearly 8,000 corporate employees, it’s inevitable we encounter varying levels of technical abilities and security awareness,” says Mark Burtenshaw, ICT Manager for Security and Compliance at The City of Edinburgh Council. “Given this, our top concern lies with phishing attacks that don’t use traditional payloads, such as advanced spear phishing emails targeted at our top executives and VIPs. Ensuring our employees can identify this type of sophisticated threat is vital for our security strategy.”

With phishing threats constantly evolving and having noted the devastating impact on other local authorities in the UK, the security team at The City of Edinburgh Council became aware of a gap in their email security tech stack.

At a Glance

- 98% of detected attacks bypassed Microsoft 365
- 42% of detected attacks were sent from compromised accounts
- Measurable reduction in interactions with phishing simulations

"Too many advanced phishing threats were getting past Microsoft 365's native defenses and our secure email gateway (SEG)," Burtenshaw says. "We needed to implement an intelligent anti-phishing platform that could detect advanced attacks, while remaining user-friendly for employees of differing technical abilities."

Intelligently Detecting Threats That Bypass Microsoft 365

Following a successful pilot, in August 2023 The City of Edinburgh Council rolled out KnowBe4 Defend across all 8,000 users to identify and neutralize advanced threats that were bypassing Microsoft 365 and their SEG.

Seamlessly integrating with Microsoft 365, Defend harnesses pre-generative and zero-trust detection models, as well as linguistic, contextual, and behavioral analysis, to identify advanced inbound threats. Inspecting every inbound email, Defend displays dynamic heat-based banners that alert users to risk, providing easy-to-understand advice that supports security awareness training without creating user friction.

> *"The banners have also dramatically increased employees' everyday vigilance to phishing attacks."*
>
> **Mark Burtenshaw**
> ICT Manager Security and Compliance,
> The City of Edinburgh Council

"Defend's banners are incredibly intuitive," Burtenshaw says. "They give our users clear advice that we couldn't get from our existing email security tools, and have noticeably improved employees' resilience to phishing attacks."

In addition, Burtenshaw and the team found that Defend had a positive impact on their internal phishing simulation campaigns. Burtenshaw says "The banners have dramatically increased employees' everyday vigilance to phishing attacks. They receive real-time nudges based on threats that are targeting them – providing in-the-moment training that enhances their security awareness. As a result, we have seen a dramatic decrease in the number of employees interacting with our phishing simulations."

Defend Now Detecting 98% More Attacks

Data taken from Defend for a 90-day period shows that a staggering 98% of phishing attacks targeting the council had bypassed Microsoft 365 and SEG detection, and were identified and neutralized by Defend. Of the attacks that evaded Microsoft's native detection, 42% came from compromised accounts, 24% used advanced obfuscation techniques and 49% carried a phishing hyperlink as their payload.

“Defend’s value is proven every day in the statistics shown in its threat intelligence dashboard,” Burtenshaw says “Before we implemented Defend, Microsoft 365 and our SEG were only catching 2% of attacks targeting the council – which was something that kept the security team up at night! With Defend in place, not only can the team quickly respond to known attacks with Defend’s remediation capabilities, but I can rest easy knowing employees aren’t able to interact with advanced phishing threats.”

> *“Defend’s value is proven every day in the statistics shown in its threat intelligence dashboard.”*
>
> **Mark Burtenshaw,**
> ICT Manager Security and Compliance,
> The City of Edinburgh Council

The team at The City of Edinburgh Council were also impressed with the ongoing product innovation. “It’s clear that KnowBe4 is continuously evolving,” Burtenshaw says, “Not only is the product always improving over time through its self-learning technology, but unlike other vendors I’ve worked with in the past, new developments are consistently being made available to customers.”

With a view to implementing the entire KnowBe4 Cloud Email Security platform to include outbound email protection and encryption, Burtenshaw says: “It’s a game-changing improvement on any email security tool we’ve implemented with Microsoft 365 – and now I can’t imagine going back.”

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com