Case Study

Greater Manchester Mental Health Trust Enhances Anti-Phishing Defenses in Microsoft 365

NHS Greater Manchester Mental Health NHS Foundation Trust

Industry	Location
Healthcare	UK

Challenge

Protect busy healthcare professionals from advanced phishing threats without impacting clinical efficiency or distracting from patient care priorities.

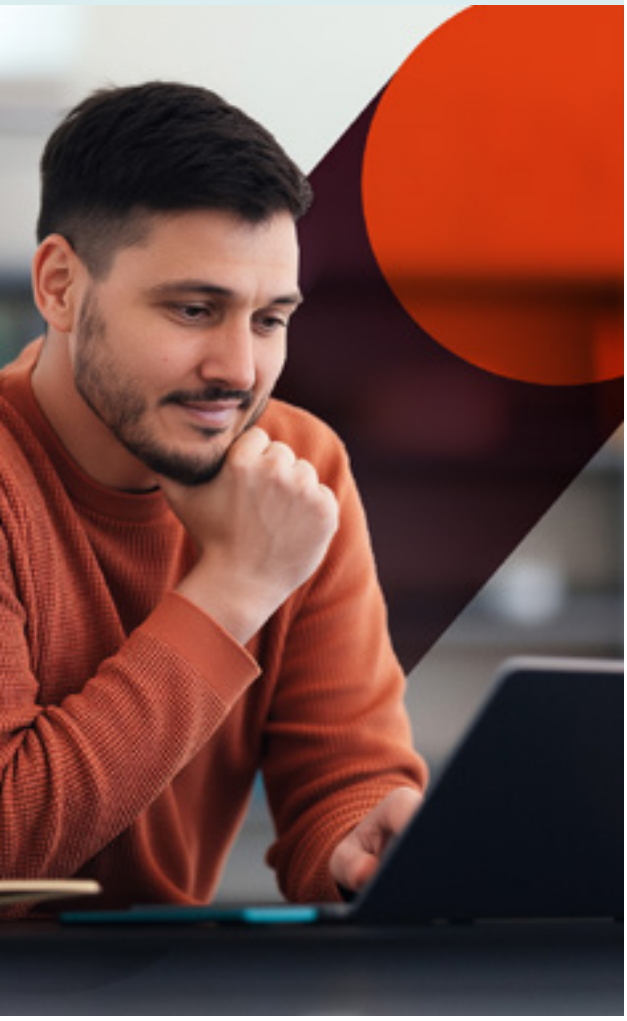
Greater Manchester Mental Health (GMMH), an NHS foundation trust in Northwest England, is one of the largest specialist mental health providers in the UK. GMMH employs approximately 8,000 people across multiple sites and as satellite remote workers, who use email to communicate with other healthcare professionals, patients and suppliers. As email is the most common channel for cyberattacks, email security is a top priority for GMMH to ensure they have the right defenses in place to protect busy healthcare professionals.

Enhancing Email Defenses Without Impacting Clinical Efficiency

"The majority of our employees are clinical-focused individuals who prioritize patient care and are not necessarily IT experts," GMMH Cyber Security Manager Kevin Orritt says. "We need to ensure we have the right defenses in place to protect them from the broad spectrum of phishing threats they face, without distracting them from their day-to-day work."

At a Glance

- Enhance Microsoft 365 Exchange Online Protection with additional anti-phishing layer
- Detect advanced phishing threats including BEC and impersonation attacks
- Dynamic anti-phishing banners that reinforce security training
- Seamless deployment across 8,000+ healthcare employees



Like most healthcare organizations, GMMH has migrated to Microsoft 365 and uses Exchange Online Protection (EOP) as an initial layer in their anti-phishing defenses. "We recognized that one layer is not enough to detect and neutralize the numerous advanced phishing threats targeting GMMH," Kevin says. "We therefore wanted to increase our technical defenses and, at the same time, find a platform that could reinforce our security training, as employees were becoming desensitized to the same static banners that were being displayed on every phishing email by EOP."

> *"We recognized that one layer is not enough to detect and neutralize the numerous advanced phishing threats targeting GMMH day-to-day work."*
>
> Kevin Orritt, Cyber Security Manager, GMMH

In particular, GMMH identified that they were at risk from attacks that contain new or emerging payloads not yet listed in EOP's definitions libraries, as well as phishing emails that don't contain a "traditional" payload, such as impersonation-based business email compromise (BEC) attacks requesting fraudulent changes to payroll. There was also a risk of phishing emails sent from compromised legitimate email accounts within their supply chain.

Intelligent Anti-phishing in Microsoft 365 That Reinforces Security Culture

GMMH contacted KnowBe4 and Softcat, a leading provider of IT technology solutions and services, that works with GMMH on strategic projects and implementations across their estate. Softcat's large Public Sector framework presence also allows for a simple and compliant way for GMMH to work with them. Following initial discussions, GMMH trialed the intelligent anti-phishing product, KnowBe4 Defend.

"The Defend trial was very easy to set up," Orritt says. "We onboarded approximately 100 users from within our IT team very quickly and, as the software is user-friendly and intuitive, everything went smoothly and we only received positive feedback. As a result, we were ready for a 'big bang' launch to our entire employee base within two months."

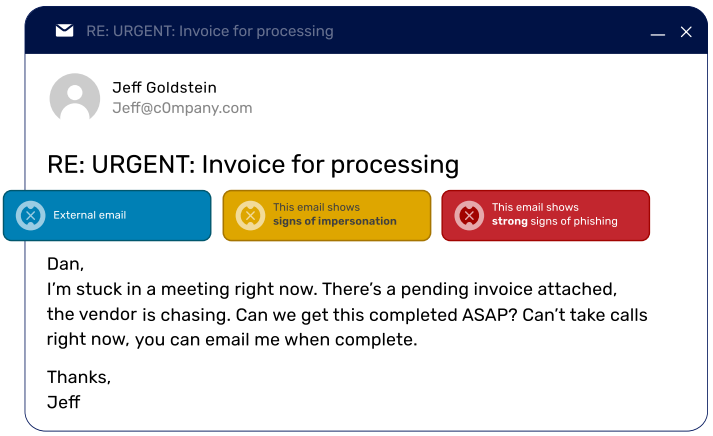
While evaluating Defend, the team spoke with a current KnowBe4 customer about their experience.

"They were incredibly positive about their experience using KnowBe4 – so much so that based on their recommendation, we subsequently evaluated and invested in KnowBe4 Prevent, which we're about to deploy!" Prevent uses machine learning technology to detect human error, such as misdirected emails and file attachments, and data exfiltration to enhance outbound email security.

In addition to detecting the advanced phishing threats that get through existing defenses, the GMMH team was also impressed by Defend's dynamic anti-phishing banners, compared to the static ones previously implemented. Using a heat-based warning system, the banners change color depending on the level of risk detected and provide informative target messages, making them highly engaging to end users.

"KnowBe4 Defend not only provides an additional layer of defense but also supplements our security awareness training. Defend's clickable banners allow employees to continuously develop their cybersecurity awareness."

Kevin Orritt, Cyber Security Manager, GMMH



Stylistic version of Defend banners

Improved Phishing Detection and Employee Awareness, While Reducing Administrative Overhead

After an initial light-touch internal communications campaign, deploying and managing Defend has proven to be a seamless process for GMMH. The team was particularly impressed with the technical expertise and approachability of the KnowBe4 and Softcat teams during the implementation.

"We're really pleased with the implementation of Defend," Orritt says. "The KnowBe4 Platform shows that we're now detecting a broader range of advanced phishing threats, including BEC and impersonation attacks. Defend is intuitive and easy to use, which meant GMMH's employees could benefit from it immediately, and it makes life easier for our administrators. You always expect helpdesk calls when you roll out new software – but KnowBe4 bucked the trend, and we didn't receive a single ticket! We've only had positive feedback from end users, and our Information Governance team is now keen to get Prevent deployed to see the benefits to our outbound email security. Both the KnowBe4 and Softcat teams made the process incredibly collaborative, and I look forward to continuing to work with them on this and future projects."

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