



Athona
Recruitment

Athona Recruitment Turns to Mimecast Impersonation Protect to Keep the Whalers at Bay

Following sophisticated new attacks, Athona Recruitment added Mimecast Impersonation Protect to its email security environment, and the service has proven highly effective in blocking whaling attacks.

Athona Recruitment is a leading UK recruitment agency, which provides staff to the medical, healthcare, nursing and education markets.

The business' market focus means it is required by law to hold a lot of personal information about the individuals it represents to potential employers – and keeping it safe is vitally important to Athona's reputation as a trusted consultant to candidates and client organizations alike.

It follows, then, that the security of its email systems is of paramount importance, since email remains the primary communications tool for its consultants, and is often used to gather confidential information.

At a Glance

Company

- Athona Recruitment (www.athona.com)
- Industry: Recruitment
- Number of email users: 150

Objectives

- Secure email communications against whaling attacks
- Protect the firm's reputation by keeping confidential information safe
- Strengthen security without adding significant complexity or additional administration

Results

- Mimecast Impersonation Protect scans emails in real time to detect and block whaling attacks
- The solution was immediately effective, blocking attacks on deployment
- The service has avoided false positives and not added any administrative burden

“ The fact that a business with fewer than 150 employees is being targeted by such sophisticated attacks means it is well worth the investment because the potential financial losses are huge. New risks are emerging all the time. Mimecast significantly strengthens our information security by helping us to stay one step ahead of new email borne threats.”

Michael Paul - IT Manager, Athona Recruitment

Robust Security

As a result, IT Manager Michael Paul, has long been focused on delivering a user friendly email service that is robust and reliable, and on keeping it up to date with the very latest security innovations.

In 2015, that led Michael to migrate Athona's email systems to the Mimecast cloud. The move delivered against Michael's primary aim – to simplify archiving – while also significantly enhancing security.

He said: “These additional benefits that I could bring to the business, including spam filtering, is what set Mimecast apart. It blocks about 40,000 illegitimate and malicious emails each week.

Emerging Threats

All the same, in an ever-evolving threat landscape, email security cannot stand still, and this has proven another benefit of the move to Mimecast.

“New risks are emerging all the time,” Michael explained. “Mimecast significantly strengthens our information security by helping us to stay one step ahead of new email borne threats.”

Whaling Attack

A recent example of this came after Athona was targeted by a whaling (CEO fraud) attack. Fortunately, the attack on Athona was foiled when a savvy finance manager reported the fraudulent emails to Michael.

Michael said: “The email appeared to come from the MD and was even written in the same style as legitimate emails from him, and was requesting an urgent money transfer, but the finance manager noticed that the sender's address did not match every detail of the MD's usual email address.

Impersonation Protect

Following this narrow escape, Michael remained concerned at the sophistication of the attack: “It is scary how focused these attacks are and how easy it would be for them to go undetected because the emails are so well crafted.”

With that in mind, Michael was keen to find a way to help defend Athona against socially engineered whaling attacks. He turned to Mimecast and was quickly given access to the beta program for Mimecast's Impersonation Protect – an anti-whaling service and part of the firm's cloud-based Targeted Threat Protection advanced email security service.

Impersonation Protect monitors all inbound email traffic and identifies key indicators of malware-less attacks being increasingly used by cyber criminals.

Combinations of these indicators, including display names, domain names and reputation and keywords, provide a robust way to recognize and block these attacks. Importantly the service is easy to set up and manage, so does not add significant complexity or additional workload.

“The best thing is that you configure just one policy and it’s working,” said Paul. “Problem solved with no staff training required.

Instantly Effective

Mimecast Impersonation Protect immediately lived up to its billing, blocking whaling attacks from the moment it was deployed. “Once it was deployed, the system detected the next attempted whaling attack by recognizing the MD’s name and other keywords in the message,” said Michael.

Meanwhile, Michael has been impressed by the service’s accuracy – there have been no false positives despite the high volume of emails and correspondents with similar or the same names from different organizations.

Overall, Michael is delighted with the value for money he has derived from the service: “The fact that a business with fewer than 150 employees is being targeted by such sophisticated attacks means it is well worth the investment because the potential financial losses are huge.”

In addition to Impersonation Protect, Mimecast’s Targeted Threat Protection service also offers protection against malicious links with real-time scanning and weaponized attachments using sandboxing or an option to convert files to a safe format without delaying delivery.