Case Study

mimecast

UK bank chooses Mimecast to thwart customer phishing attacks

From continuous website cloning attacks to zero in just two months

This well-respected UK-based financial institution specializes in property and asset finance loans, and savings accounts for small to medium enterprises.

It all started with a phone call

The bank was alerted to its first known phishing scam towards the end of 2018 from an inbound phone call from a customer. Following this, the bank's website was cloned multiple times and used to legitimize other fraudulent activity.

Targets were sent letters or emails that directed them to a cloned website where they were encouraged to enter specific credentials to claim some inherited money, suggesting that there were funds waiting in their name.

At a Glance

- Regional UK bank
- £1bn in assets

Problem:

- Reputation and customer trust was being eroded as the banks website was being repeatedly cloned, with fraudsters tricking their customers into handing over credentials and other sensitive information.
- Two man days a week were being spent trying to manually detect and remediate these attacks.
- Takedown processes were adhoc, with the bank using slow and unresponsive ISP and legal routes with limited success.

Solution:

Mimecast Brand Exploit Protect

Benefits:

- Within 2 months, the bank eradicated all customer impacting attacks – if any threats were detected, they were taken down before they could target customers.
- Internal staff time was freed up due to the automated detection and managed response from Mimecast.
- Customer trust and the bank's reputation were restored.

> **"At the height of our issues with website cloning, we were spending as much as two days a week trying to handle cloned websites and attempting to take down threats."**
>
> *IT security and infrastructure manager*

Customer trust was on the line

Every business's worst nightmare is to be alerted to a problem by their own customers. These cloned websites were increasing in number, and the bank was worried about the impact this would have on their reputation and business if their name became associated with hacking or phishing scams. They needed to get ahead of the problem, show customers that it had the issue in hand, and be preventative in its approach.

No way to track the cloned sites

Without any monitoring in place, the bank began using manpower to manually search the web using Google Alerts in the hopes of coming across something suspicious. This approach was random and ineffectual, and if threats were uncovered, they were already live on the web and doing damage. The business had no idea how many new sites would appear, and when.

Slow takedowns

Without any monitoring in place, the bank began using manpower to manually search the web using Google Alerts in the hopes of coming across something suspicious. This approach was random and ineffectual, and if threats were uncovered, they were already live on the web and doing damage. The business had no idea how many new sites would appear, and when.

Huge manpower drain

Without any monitoring in place, the bank began using manpower to manually search the web using Google Alerts in the hopes of coming across something suspicious. This approach was random and ineffectual, and if threats were uncovered, they were already live on the web and doing damage. The business had no idea how many new sites would appear, and when.

From 3 at a time to zero cloned websites

Acknowledging the need speed up both detection and takedown of cloned websites, the bank set out to find a solution. Mimecast quickly became the banks preferred choice due to its reputation for being able to detect attacks early and take them down fast – compared with other vendors more focussed on brand and social media protection.

What put the decision beyond question, was that within 20 minutes of Mimecast being given the details of a live cloned site, Google and Microsoft were both showing the site as blocked, and the full DNS takedown was completed within 8 hours.

Since implementing the Brand Exploit Protect service, the bank has seen a massive drop in the number of attacks. In fact, only two months after starting to use the service, and following a year of continuous attacks, there have been no live cloned sites detected at all – a result far exceeding their expectations.

> **"For the first time, we were ahead of the game. Cloned websites were being detected and removed before they had a chance to target anyone, and without any internal resources or manpower on our part."**
>
> *IT security and Infrastructure manager*

Proactive, automated approach

Continuous monitoring has become a critical element of the company's approach, adding efficiency and expertise that gets ahead of the problem.

From 3 at a time to zero cloned websites

Speed of response

The resolution time for taking down cloned websites has gone from days or weeks to hours or minutes.

Targeted intelligence

Manual and random searching was resource-intensive and insufficient. Mimecast knows where to look, so threats are found and dealt with fast.

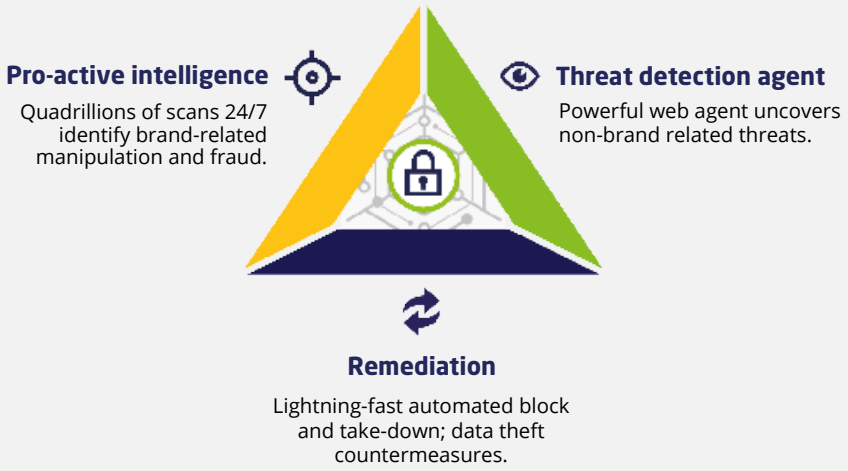
Protected reputation

The resolution time for taking down cloned websites has gone from days or weeks to hours or minutes.

No longer an easy target

Continuous monitoring has become a critical element of the company's approach, adding efficiency and expertise that gets ahead of the problem.

Mimecast Brand Exploit Protect



Find out more:

mimecast.com/products/brand-exploit-protect/