CASE STUDY

QUINTESSENTIAL BRANDS GROUP

UNITED KINGDOM

CYREN EMAIL SECURITY PLUS

CYREN

Secure Email Gateway Solves Office 365 Phishing Problem

When phishing attacks increased, it was time to adopt new security controls.

Quintessential Brands Group is an independent international spirits business, with a portfolio of premium brands and world-class production facilities in the UK, Ireland and France.

INCREASING PHISHING ATTACKS EVADING EMAIL SECURITY

Like many companies today, for no specific reason related to their business, Quintessential Brands Group were suffering from a deluge of phishing attacks, both targeted and mass phishing campaigns. Also like many companies, the inevitable happened, and a small number of attacks were successful. At the time, they had been using Office 365 and relying on its native email security for around three years.

RESPONDING WITH PEOPLE, PROCESS AND TECHNOLOGY SECURITY CONTROLS

The leadership and IT team mobilized and put in place every appropriate measure to prevent and contain future attacks. This meant implementing more stringent people and process controls, as well as introducing new technology.

Ian Wells, Group IT Operations Manager, is responsible for the company's infrastructure, including securing it.

Ian's first step was to implement controls to respond to multi-stage account takeover attacks should a user's credentials be phished. He removed web access to Office 365 email to slow down and make it harder for an attacker to access the account. He then configured rules within Office 365 to trigger an alert when suspicious activity occurs in an account. For example, creating an email forwarding rule is a typical action performed by attackers who have control of an email account. This allows them to monitor email communications and understand how the business works, to prepare for the next stage of the attack.

Next, for highly targeted individuals, he implemented multi-factor authentication for Office 365. This would ensure that even if their credentials are phished, the attacker would be unable to access the account.

User education was introduced. All users received training on how to recognise a phishing email, and the consequences of falling for a phish. The internal communications function was leveraged to create an awareness campaign to get the message out to all users. Users were provided a process for reporting suspicious emails and a process was introduced for non-email verification of actions involving financial transactions.

Finally, a new, additional layer of security technology was introduced – Cyren Email Security.

> "Cyren Email Security does what every email security service should do."
>
> **Ian Wells,**
> **Group IT Operations Manager,**
> **Quintessential Brands Group**

Email Security

CASE STUDY:
QUINTESSENTIAL BRANDS GROUP

Email Security

PROVING VALUE WITH AN EMAIL SECURITY THREAT ASSESSMENT

Ian attended a Cyren webinar on how to supplement the native security provided by Office 365 and engaged with Cyren's security specialist team. He was assigned a dedicated systems engineer and decided to perform a free Email Security Gap Analysis.

The assessment was quickly deployed by creating a transport rule in Office 365 that copied to Cyren all the emails that had already been scanned, considered clean and delivered to users. Emails that were really clean were discarded, while others were classified as malware, zero-day threats, phishing, spam and newsletters. These were dropped into folders, on a dedicated email platform, for Ian to monitor.

The assessment, which normally runs for four weeks, showed compelling results in under two weeks. Office 365 had delivered to users 2,743 emails that were either malicious or unwanted. That equated to 6.2% of the total emails delivered to users in the two week period. Most worrying was that 32 of these were phishing emails and 2 contained zero-day malware.

20% REDUCTION IN IT STAFF TIME INVESTMENT

Ian uses Cyren's reporting dashboard to produce a report each month for his board of directors to understand the return that they are getting from Cyren. Drilling into the details, the most important result for Ian is the visibility of targeted phishing emails that comes from Cyren Impostor Protection, an integrated feature of Cyren's SaaS secure email gateway. At the moment this is only deployed for a small number of users and it blocks around four BEC attacks per-month that are targeting the executives.

Users are happy and their productivity has increased. The prior aggressive, but necessary policy of filtering greymail, such as newsletters, has now been relaxed, increasing user satisfaction. They no longer receive the same volume of phishing and spam emails and consequently do not have to spend time sifting through them and reporting them to the IT team.

The time spent by the IT team on email support has reduced by 20%, as they are no longer diverted by the task of checking and responding to suspected phishing emails.

Quintessential Brands has a policy to manually archive emails when users leave the business. Since there are no longer lots of unwanted emails sitting in inboxes, they are no longer archiving unneeded emails, making the process simpler and cheaper.

THE CHALLENGE

Quintessential Brands Group was suffering from both mass and targeted phishing attacks and experienced a breach. The response was to implement further process, people and technology security controls. The technology requirement was to add a more effective, specialized security service that would integrate seamlessly with Office 365 and provide the best possible phishing defense.

THE CYREN DIFFERENCE

- Proven effectiveness before purchase with a free Email Security Gap Analysis assessment
- In just two weeks, Cyren detected 2743 malicious or unwanted emails that Office 365 had delivered to users
- 6.2% of email delivered to users was malicious or unwanted
- On average Cyren now blocks 4 BEC attacks per month at the company
- The IT infrastructure team spend 20% less time dealing with email-related support
- User productivity has increased