

PROOFPOINT AND CSC HELP BLOCKET REDUCE SUSPICIOUS MESSAGES BY 99%

blocket

THE CHALLENGE

- Protect a well-known brand against targeted attacks
- Detect and block phishing email attempts before they reach customers
- Prevent email-based threats from hurting brand reputation and revenue

THE SOLUTION

- Proofpoint Email Fraud Defense

THE RESULTS

- Gained visibility of attacks and threats
- Identified and addressed authentication issues on all mail streams
- Achieved a 99% drop in suspicious incoming email
- Reduced customer-service tickets related to phishing emails by 70%

THE COMPANY

Founded in 1996 and based in Stockholm, Sweden, Blocket AB owns and operates the country's biggest marketplace for selling and buying goods online through a classified advertising website (www.blocket.se). Blocket is one of the top ten most recognised brands in Sweden with 99% brand awareness. Every week, over 5 million unique visitors turn to Blocket to buy and sell second-hand items.

Nearly 8 out of 10 Swedes have bought or sold something through blocket.se. Like any well-known brand, Blocket is vulnerable to cybercriminals.

THE CHALLENGE

Email fraud was a big security challenge for the Blocket team—hurting its brand reputation and ultimately revenue. 'Aside from the hard cost of responding to the customer-service enquiries that were flooding in from phishing scams, brand trust was taking a big hit,' says Thomas Bäcker, Blocket's head of customer security.

'In any highly competitive marketplace, customer trust in your brand is business-critical,' Bäcker said. 'If you're actively working on building trust with customers, then you need to consider the impact of email fraud.'

Blocket had relied on awareness and education campaigns alone to help customers identify and report phishing emails. These efforts might have helped, but the number of customer-service phishing enquiries was still going up.

The customer-security team was tasked with exposing and eliminating the impact of these phishing emails before they could harm Blocket's business. When customer education alone was not enough, the company decided it needed a proactive solution that could detect and block phishing emails before they reached customers.

THE SOLUTION

Working with CSC, one of the world's largest business service providers, Blocket selected Proofpoint Email Fraud Defense. Initial efforts focused on gaining visibility of internal and external email authentication processes. The aim was to get a Domain Message Authentication Reporting & Conformance (DMARC) record in place. DMARC identifies all legitimate and suspicious email streams, helping Blocket to prevent impostors from hijacking its trusted domains.

Bäcker justified the investment by making a compelling business case.

'I told the executive team that each customer service ticket had a cost to the business, and that the only way to reduce those costs was to implement a solution like Proofpoint Email Fraud Defense,' he recounted. 'I demonstrated that my team was committed to delivering an ROI, both in terms of reducing phishing and increasing customer trust in the Blocket brand.'

Blocket used the data from the Proofpoint solution—over a period of three months, the firm got to the point where it could confidently deploy a DMARC 'reject' policy on its main sending domains without worrying that it would block legitimate email.

'In any highly competitive marketplace, customer trust in your brand is business-critical. If you're actively working on building trust with customers, then you need to consider the impact of email fraud.'

Thomas Bäcker
Head of Customer Security
Blocket

Stopping scammers from using Blocket's domain

DMARC stopped domain spoofing completely. But Proofpoint also helped to identify fraudulent emails using other techniques—including display-name spoofing and lookalike domains—which made fraudulent emails look as if they were from Blocket.

Among them was a survey scam. It asked people to submit personal information in exchange for a cash reward. (People who responded never got the money, but attackers got their personal information.) Proofpoint broadcast identified threats to CSC in real time, so if a phishing email was delivered, the malicious domain was eliminated before it could do any harm.

THE RESULTS

Blocket was able to identify and address authentication issues on all mail streams, ensuring that its DMARC policy wasn't hindering legitimate messages.

The benefits were immediate. Blocket gained true visibility of email attacks sent from its domains. And with Email Fraud Defense, the company can block the malicious use of its domains, protecting its employees, customers and business partners.

Blocket also saw a 99% drop in suspicious messages coming into its environment within three months of setting up a DMARC 'reject' policy. At the same time, customer-service tickets relating to email phishing dropped by 70% after implementing DMARC.

FIND OUT MORE

For more information, visit proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals to protect their users from the advanced attacks that target them (via email, mobile apps and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 per cent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and utilise both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.