

# PROOFPOINT ET CSC AIDENT BLOCKET À RÉDUIRE LES MESSAGES SUSPECTS DE 99 %

## blocket

### LE PROBLÈME

- Protéger une marque réputée contre les attaques ciblées
- Détecter et bloquer les tentatives de phishing par e-mail avant qu'elles n'atteignent les clients
- Empêcher la fraude à la messagerie de nuire à la réputation de la marque et au revenu de l'enseigne

### LA SOLUTION

- Proofpoint Email Fraud Defense

### RÉSULTATS

- Meilleure visibilité des attaques et des menaces
- Identification et résolution des problèmes d'authentification sur tous les flux de messagerie
- Baisse de 99 % des e-mails entrants suspects
- Réduction de 70 % du nombre de tickets du service client liés aux e-mails de phishing

### LA SOCIÉTÉ

Fondée en 1996 et basée à Stockholm en Suède, Blocket AB exploite la plus grosse plateforme du pays pour la vente et l'achat de biens en ligne via un site Web publicitaire classifié ([www.blocket.se](http://www.blocket.se)). Blocket compte parmi les dix marques les plus reconnues en Suède avec une notoriété de 99 %. Chaque semaine, plus de 5 millions de visiteurs uniques se rendent sur Blocket pour acheter et vendre des articles d'occasion.

Près de 8 suédois sur 10 ont déjà acheté ou vendu quelque chose sur [blocket.se](http://blocket.se). Comme toutes les marques très connues, Blocket est vulnérable face aux cybercriminels.

### LE PROBLÈME

La fraude par courrier électronique posait un important problème de sécurité à l'équipe de Blocket, en nuisant à la réputation de la marque et donc au chiffre d'affaires. En plus du coût exorbitant du service client pour répondre à toutes les demandes générées par les escroqueries de type phishing, la confiance en la marque accusait le coup, déclare Thomas Bäcker, chef de la sécurité des clients chez Blocket.

“Notre marché est très concurrentiel, la confiance des clients est donc primordiale pour l'entreprise,” ajoute Bäcker. “Si vous cherchez activement à améliorer la confiance de vos clients, vous devez tenir compte de l'impact de la fraude à la messagerie.”

Blocket comptait uniquement sur des campagnes de sensibilisation et d'éducation pour aider ses clients à repérer et signaler les e-mails de phishing. Ces efforts ont peut-être légèrement amélioré la situation, mais le nombre d'appels au service client pour des problèmes de phishing continuait d'augmenter.

L'équipe de sécurité était chargée d'exposer ces e-mails de phishing et d'éliminer leurs effets désastreux avant qu'ils ne parviennent à nuire à l'activité de Blocket. Comme se contenter de sensibiliser les clients ne suffisait pas, l'entreprise a décidé d'adopter une solution proactive, capable de détecter et bloquer les e-mails de phishing avant qu'ils n'atteignent les clients.

### LA SOLUTION

En collaborant avec CSC, l'un des plus grands fournisseurs de services aux entreprises au monde, Blocket a choisi la solution Proofpoint Email Fraud Defense. Les efforts initiaux portaient sur une meilleure visibilité des processus d'authentification des e-mails, internes et externes. L'objectif était d'implémenter la norme DMARC (Domain Message Authentication Reporting & Conformance). DMARC identifie tous les flux d'e-mails, légitimes et suspects, ce qui aide Blocket à empêcher les imposteurs de pirater ses domaines officiels.

Bäcker a justifié l'investissement au travers d'une étude de cas convaincante.

“J'ai expliqué à l'équipe d'encadrement que chaque ticket du service client avait un coût pour l'entreprise, et que le seul moyen de réduire ces coûts était d'implémenter une solution comme Proofpoint Email Fraud Defense,” explique-t-il. “J'ai démontré que mon équipe s'engageait à atteindre un retour sur investissement, à la fois en termes de réduction du phishing et d'augmentation de la confiance des clients dans la marque Blocket.”

---

**“Dans un marché très concurrentiel, la confiance des clients dans votre marque est primordiale pour votre entreprise. Si vous cherchez activement à améliorer la confiance de vos clients, vous devez tenir compte de l'impact de la fraude à la messagerie.”**

Thomas Bäcker,  
Responsable de la sécurité  
des clients chez Blocket

---

Blocket a exploité les données de la solution Proofpoint pendant une période de trois mois, et est parvenue à déployer en toute confiance une règle de “rejet” DMARC dans ses principaux domaines d’envoi, sans crainte de bloquer les e-mails légitimes.

### **Empêcher les fraudeurs d’exploiter le domaine de Blocket**

DMARC stoppe entièrement toute usurpation de nom de domaine. Cependant, Proofpoint les a également aidé à identifier les e-mails frauduleux à l’aide d’autres techniques, dont l’usurpation des noms d’affichage et les sosies de nom de domaine, qui font croire que des e-mails frauduleux proviennent de Blocket.

Parmi ces menaces, se trouvait une enquête frauduleuse. Elle demandait des données personnelles aux individus en échange d’une récompense en argent. (Ceux qui y ont répondu n’ont jamais encaissé d’argent, mais les attaquants avaient obtenu leurs données personnelles.) Proofpoint communiquait les menaces identifiées à CSC en temps réel. Ainsi, en cas de réception d’un e-mail de phishing, le domaine malveillant était éliminé avant de pouvoir nuire.

## **LES RÉSULTATS**

Blocket était désormais capable d’identifier et de résoudre les problèmes d’authentification sur tous les flux de messagerie, tout en garantissant que sa règle DMARC ne bloquait pas les messages légitimes.

Les bénéfices ont été immédiats. Blocket pouvait voir toutes les attaques de la messagerie envoyées à partir de ses domaines. De plus, avec Proofpoint Email Fraud Defense, l’entreprise peut bloquer tout usage malveillant de ses domaines, et protéger ses employés, clients et partenaires commerciaux.

Trois mois après avoir instauré la règle de rejet DMARC, Blocket a également observé une baisse de 99 % des messages suspects pénétrant dans son environnement. Dans le même temps, le nombre de tickets du service client liés au phishing de la messagerie a diminué de 70 % après l’implémentation de DMARC.

## **EN SAVOIR PLUS**

Pour plus d’informations, visitez [proofpoint.com](https://proofpoint.com)

### **À PROPOS DE PROOFPOINT**

Proofpoint Inc. (NASDAQ:PFPT), leader spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger les modes de travail modernes de leurs employés face aux menaces avancées, et de se conformer aux réglementations en vigueur. Grâce à Proofpoint, les professionnels de la sécurité sont en mesure d’accéder à des renseignements et outils capables de protéger les utilisateurs et leurs données contre les attaques menées par courrier électronique, sur les réseaux sociaux ou via des appareils mobiles. De nombreuses entreprises de toutes tailles, dont plus de la moitié de celles figurant dans le classement Fortune 100, exploitent des solutions Proofpoint. Celles-ci sont conçues spécialement pour les environnements mobiles et de réseaux sociaux. Elles tirent parti de la technologie cloud et d’une plateforme d’analyse du Big Data pour lutter contre les menaces avancées modernes.

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d’autres pays. Toutes les autres marques contenues dans le présent document sont la propriété de leurs détenteurs respectifs.