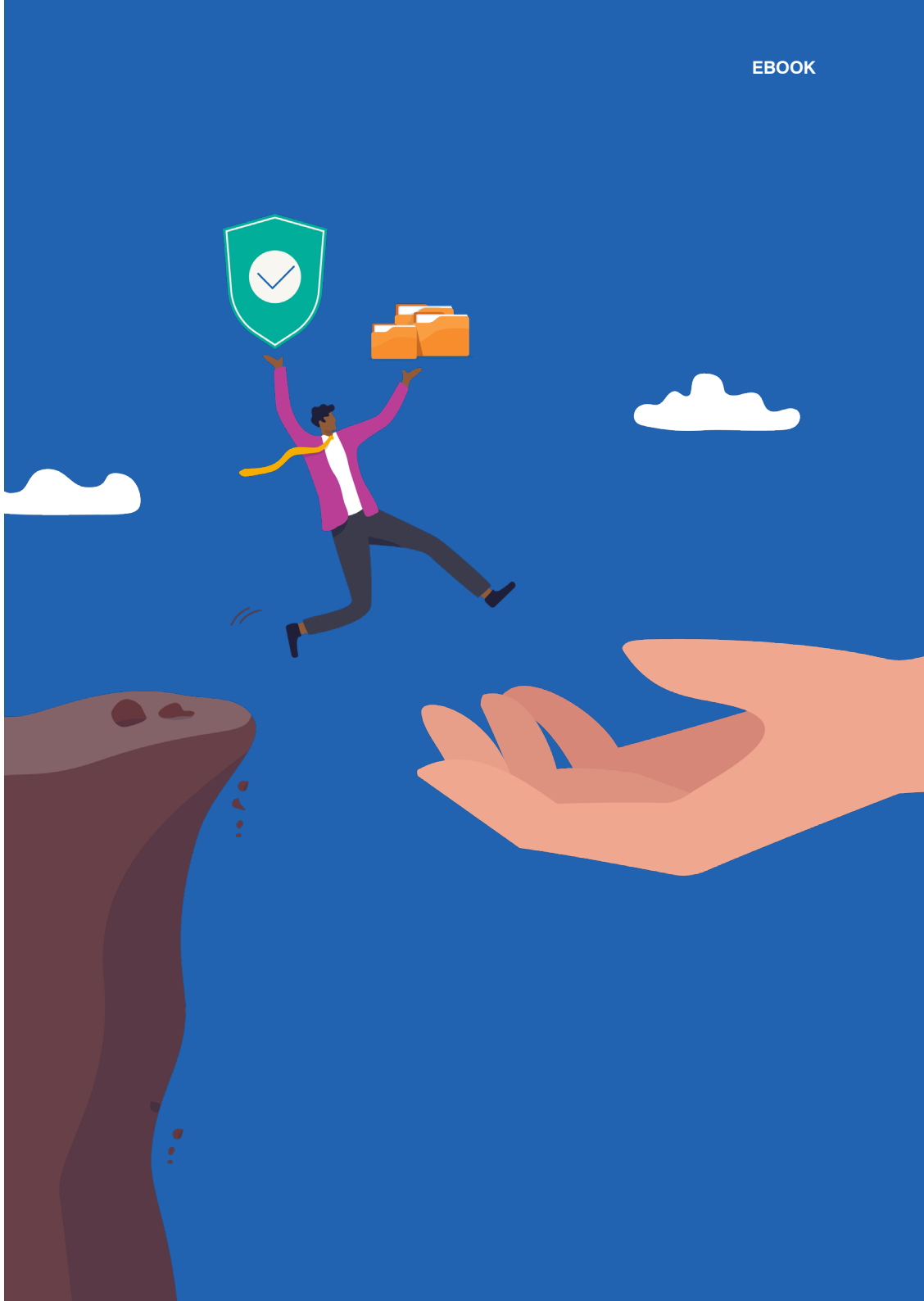
EBOOK

Prise en main de l'authentification DMARC

Comment l'authentification des emails peut sécuriser votre domaine de messagerie, prévenir le piratage de la messagerie en entreprise et protéger votre marque



proofpoint.

Introduction

La messagerie électronique représente un atout de taille pour les entreprises : elle est peu onéreuse évolutive et efficace pour générer des leads et des revenus. Malheureusement, les caractéristiques qui la rendent si populaire — simplicité d'utilisation, convivialité et transparence — en font également un vecteur d'attaque de choix pour les cybercriminels.

La fraude par email coûte aux entreprises du monde entier des milliards de dollars et peut mettre à mal la réputation d'une marque et la confiance des clients en quelques minutes. Les attaques par piratage de la messagerie en entreprise (BEC, Business Email Compromise) extrêmement ciblées et de faible envergure sont sans doute les plus dangereuses. D'après le FBI, elles ont coûté aux entreprises du monde entier 43 milliards de dollars depuis 2016[1].

1 FBI, « Business Email Compromise: The $43 Billion Scam » (Piratage de la messagerie en entreprise : des arnaques chiffrées à 43 milliards de dollars), mai 2022.

43 milliards $

Coût des attaques BEC pour les entreprises du monde entier depuis 2016 (Source : FBI)

180 000 $

Coût mondial moyen d'une attaque BEC (Source : FBI)

12 %

Hausse du nombre d'entreprises ayant signalé des attaques de phishing en 2021 par rapport à l'année précédente (Source : Proofpoint)

86 %

Pourcentage d'entreprises ayant déclaré avoir été victimes d'attaques de phishing en 2021 (Source : Proofpoint)

Créée par un groupe de fournisseurs de messagerie de premier plan en février 2012, la norme DMARC est à ce jour l'une des armes les plus puissantes et proactives pour lutter contre le phishing et l'usurpation d'identité.

Elle a transformé le paysage de la fraude par email en bousculant les stratégies de phishing établies de longue date et en forçant les cybercriminels à abandonner leurs cibles préférées. Elle recèle le potentiel de neutraliser toute une classe de fraudes.

Ce guide explique ce qu'est l'authentification DMARC, comment elle fonctionne, ses principaux avantages et pourquoi elle devrait être une composante essentielle de votre stratégie de défense de votre marque contre les attaques BEC et et un large éventail de menaces d'imposteurs.

SECTION 1

Qu'est-ce que l'authentification DMARC ?

Créée en 2012 par un consortium d'entreprises du secteur, la norme DMARC est un protocole ouvert d'authentification des emails qui protège la messagerie au niveau du domaine.

Reposant sur les normes SPF et DKIM, DMARC est la première et la seule technologie largement déployée qui permet de rendre le domaine d'expédition d'un email (ce que les utilisateurs voient dans leur client de messagerie) fiable.

DMARC

Domain-based

Message

Authentication

Reporting and...

Conformance

Norme ouverte d'authentification des emails

Lancée en 2012

Créée par plus de 20 entreprises

DMARC permet aux expéditeurs d'emails de...

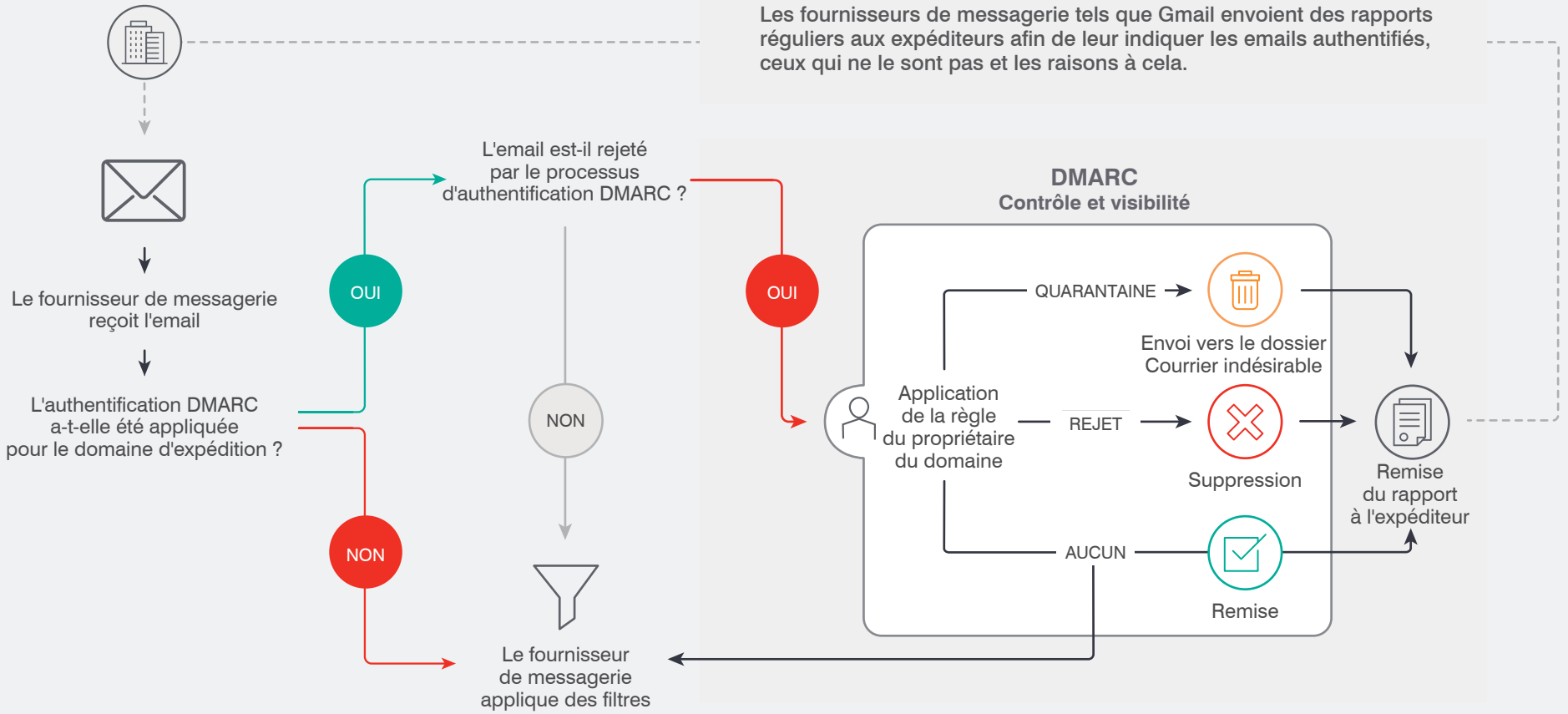
Reprendre le contrôle en authentifiant les messages légitimes pour leurs domaines d'envoi d'emails.

Indiquer aux fournisseurs de messagerie comment traiter les messages rejetés par le processus d'authentification au moyen d'un paramètre explicite. Ces messages peuvent soit être envoyés vers un dossier Courrier indésirable, soit rejetés directement, ce qui limite l'exposition des clients aux attaques.

Obtenir une visibilité sur le paysage des menaces email pour vous aider à identifier les menaces ciblant vos clients et à mieux protéger votre marque contre le phishing et l'usurpation d'identité.

SECTION 2

Fonctionnement de l'authentification DMARC



Paramètres DMARC

Aucun : l'ensemble de l'écosystème d'authentification des emails est surveillé pour identifier le trafic légitime.

Quarantaine : les messages rejetés par le processus d'authentification DMARC sont transférés vers le dossier Courrier indésirable.

Rejet : les messages rejetés par le processus d'authentification DMARC ne sont pas remis.

SECTION 3

Pourquoi mettre en œuvre l'authentification DMARC ?

DMARC permet aux expéditeurs de...

- Bénéficier d'une visibilité sur la personne qui envoie le message en votre nom, les emails authentifiés, ceux qui ne le sont pas et les raisons à cela
- Indiquer aux destinataires comment traiter les emails rejetés par le processus d'authentification
- Bloquer les attaques de phishing usurpant des domaines avant qu'elles n'atteignent les boîtes de réception des collaborateurs et des clients

« La norme DMARC est d'une efficacité redoutable. Dans le cadre d'une approche mixte de la lutte contre la fraude par email, l'authentification DMARC représente la pierre angulaire des contrôles techniques. Elle permet de rétablir la confiance des clients et de rendre le canal email aux marques légitimes et aux consommateurs. »

Edward Tucker, Head of Cyber Security, HM Revenue & Customs

DMARC permet aux destinataires de...

- Faire la distinction entre expéditeurs légitimes et expéditeurs malveillants
- Renforcer la fidélité des clients et la protection des collaborateurs
- Protéger et améliorer la réputation du canal email

« Des règles DMARC plus strictes renforcent la protection des utilisateurs et mettent les cybercriminels en difficulté. De surcroît, la vérification des expéditeurs sera synonyme d'innovation et de progrès pour toutes nos boîtes de réception. »

Jeff Bonforte, SVP of Communications Products, Yahoo!

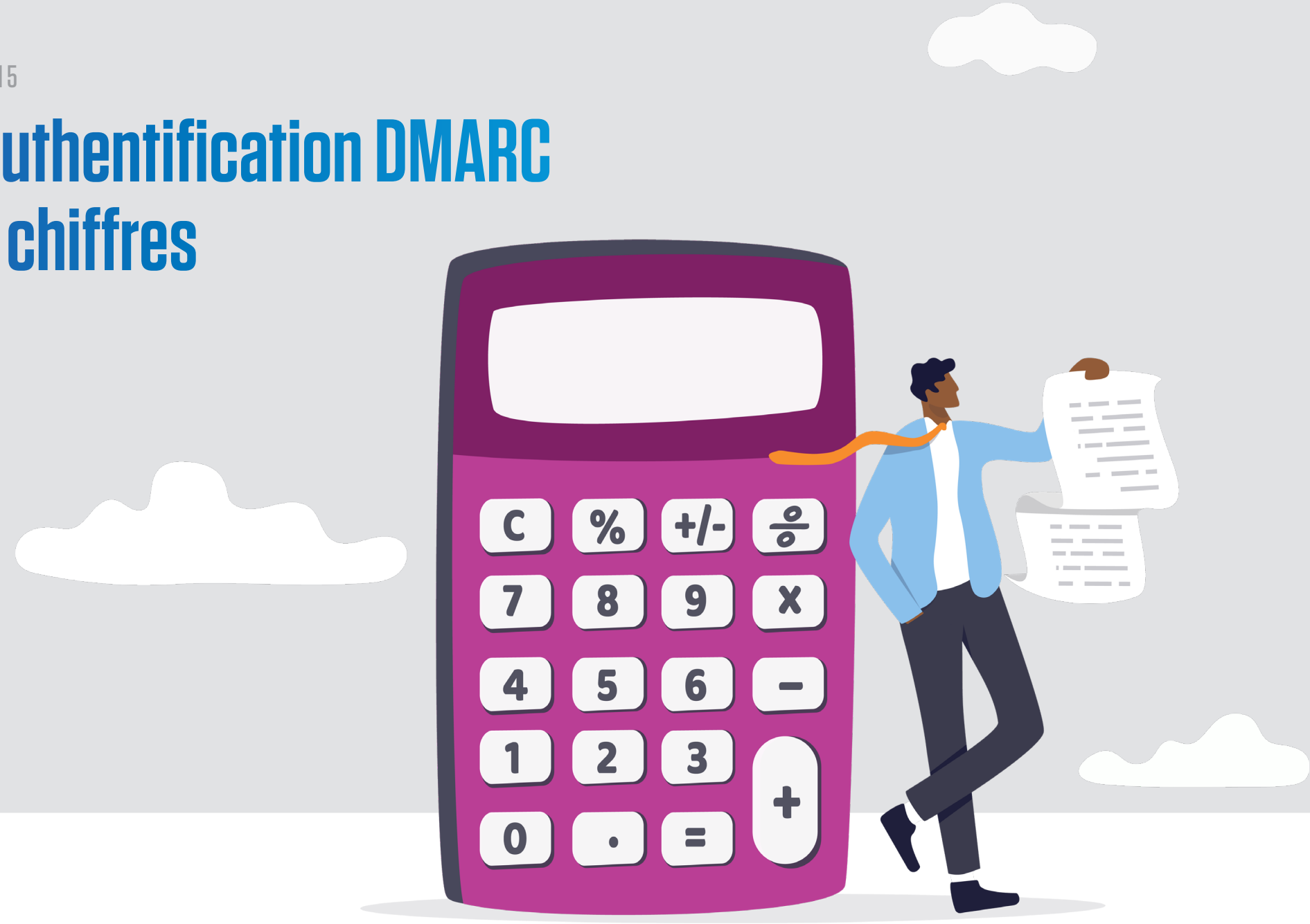
SECTION 4

Avantages de l'authentification DMARC

Protège les collaborateurs, les partenaires commerciaux, les particuliers et les marques.	DMARC neutralise toute une classe d'emails frauduleux avant qu'ils n'atteignent vos collaborateurs partenaires commerciaux et clients.
Offre une visibilité immédiate sur le paysage des menaces email.	Sans visibilité, aucun contrôle n'est possible. La mise en œuvre de l'authentification DMARC vous procure une visibilité instantanée sur les menaces qui ciblent votre entreprise. Elle détecte les attaques de phishing et d'usurpation de domaines qui mettent vos clients et la réputation de votre marque en péril.
Améliore le taux de remise des emails et l'engagement à l'égard de ceux-ci.	Près d'une attaque de phishing sur cinq entraîne une réduction du taux de remise, et une sur trois engendre une diminution de l'engagement. DMARC améliore le taux de remise des emails et l'engagement vis-à-vis des programmes de messagerie légitimes.
Réduit les coûts de service client.	En bloquant les attaques de phishing, DMARC réduit considérablement les coûts de service client. Le détaillant scandinave Blocket a observé une chute de 70 % du nombre de tickets de service client après la mise en œuvre de l'authentification DMARC.
Réduit les coûts de neutralisation des attaques de phishing.	Le phishing coûte aux marques 4,5 milliards de dollars chaque année. DMARC réduit les coûts liés à la fraude aux remboursements et à la neutralisation des attaques de phishing.

SECTION 5

L'authentification DMARC en chiffres

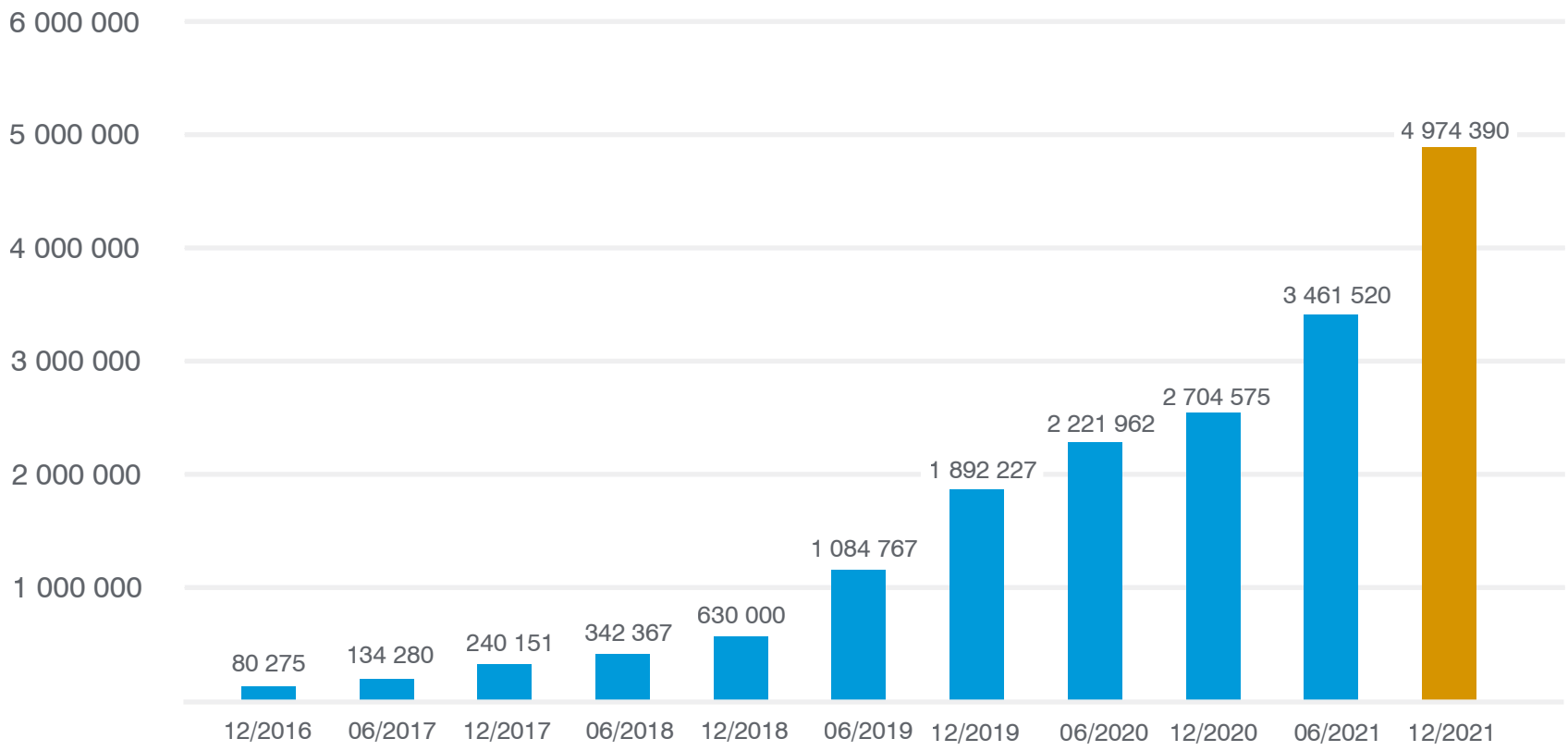


5 millions
d'enregistrements DMARC uniques sont actifs (en décembre 2021)

65 %
des entreprises du classement Global 2000 ont adopté l'authentification DMARC

26 %
des entreprises du classement Global 2000 ont mis en place une règle de rejet DMARC

Enregistrements DMARC valides confirmés via DNS



Source : DMARC.org

SECTION 6

L'authentification des emails en un coup d'œil

DMARC repose sur deux autres normes d'authentification des emails importantes : SPF et DKIM. Pour bien comprendre DMARC, vous devez également comprendre les avantages et les lacunes des normes SPF et DKIM.

	SPF	DKIM	DMARC
	(Sender Policy Framework) **www.open-spf.org**	(DomainKeys Identified Mail) **www.dkim.org**	(Domain-based Message Authentication, Reporting and Conformance) **www.dmarc.org**
Avantages	La norme SPF permet aux marques de préciser qui peut envoyer des emails pour le compte de leur domaine. Les marques répertorient les adresses IP des expéditeurs autorisés dans un enregistrement DNS. Si l'adresse IP qui envoie des emails pour le compte de la marque ne figure pas dans cet enregistrement SPF, le message est rejeté par le processus d'authentification SPF.	La norme DKIM permet aux entreprises de prendre la responsabilité de transmettre un message de sorte qu'il puisse être vérifié par le fournisseur de messagerie. Cette vérification repose sur l'authentification cryptographique de la signature numérique de l'email.	La norme DMARC permet de s'assurer que les emails légitimes sont authentifiés conformément aux normes DKIM et SPF établies de longue date et que les activités frauduleuses qui semblent émaner de domaines sous le contrôle d'une marque sont bloquées avant d'atteindre la boîte de réception du client.
Exemple d'enregistrement DNS	v=spf1 ip4:204.200.197.197 -all	v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4zOo3N	v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_agg@auth.yourdomain.com;ruf=mailto:dmarc_afrf@auth.yourdomain.com
Lacunes	• Le maintien à jour des enregistrements SPF à mesure que les marques changent de fournisseur de services et ajoutent des flux d'emails est compliqué. • Ce n'est pas parce qu'un message est rejeté par le processus d'authentification SPF qu'il sera toujours privé d'accès à la boîte de réception. • La norme SPF ne s'applique pas lorsqu'un message est transféré. • La norme SPF ne permet pas de protéger les marques contre les cybercriminels qui usurpent le nom d'affichage ou l'adresse email de l'expéditeur dans leur message.	• La norme DKIM est plus difficile à mettre en œuvre. Les expéditeurs sont donc moins nombreux à l'adopter. • L'absence de signature DKIM ne veut donc pas forcément dire que l'email est frauduleux et peut être le simple résultat de cette adoption moindre. • La norme DKIM ne permet pas à elle seule d'authentifier un expéditeur de manière fiable. • Le domaine DKIM n'est pas visible pour les utilisateurs finaux non techniques et ne permet pas de prévenir l'usurpation du domaine d'expédition visible.	• Bien qu'elle soit essentielle, l'authentification DMARC ne constitue pas une solution complète. • DMARC protège les marques contre seulement 30 % des attaques par email (menaces ciblant directement le domaine). • DMARC ne protège pas contre l'usurpation de l'identité de marque (y compris l'usurpation du nom d'affichage et les domaines similaires).

SECTION 7

Experts DMARC : Marques

Ces experts DMARC ont ouvert la voie à la généralisation de la norme. Ces pionniers de l'authentification DMARC sont en première ligne de la lutte contre la fraude par email et défendent de façon proactive leurs clients contre les cybercriminels.

« Ces dernières années, de plus en plus d'entreprises adoptent DMARC et l'authentification des emails.
Un nombre croissant de fournisseurs de services ajoutent à leurs offres le support nécessaire pour faciliter cette adoption. »

Steven Jones, DMARC.org

DMARC

Skrill

VISA

HM Revenue & Customs

IHG
InterContinental Hotels Group

RBS
The Royal Bank of Scotland

PCH Publishers Clearing House

USAA

FedEx

DELTA

blocket

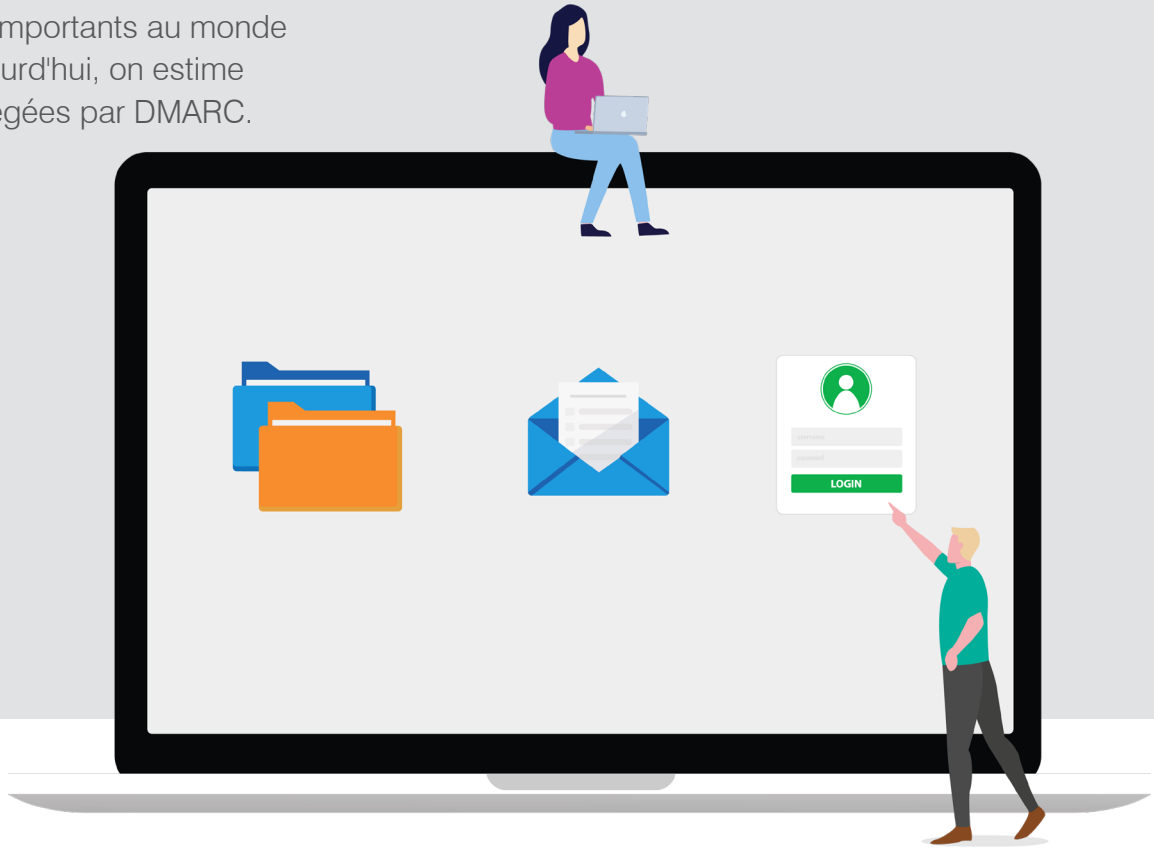
« Suite à l'implémentation d'une règle de rejet DMARC, le nombre de tickets de service client liés au phishing a chuté de plus de 70 %, permettant ainsi au personnel de se concentrer sur l'assistance aux clients ayant des demandes génératrices de revenus. »

Thomas Bäcker,
Head of Customer Security,
Blocket

SECTION 8

Experts DMARC : Fournisseurs de messagerie

Certains des fournisseurs de messagerie les plus importants au monde prennent en charge l'authentification DMARC. Aujourd'hui, on estime à 80 % les boîtes de réception de particuliers protégées par DMARC.



« Bientôt, tous les emails feront l'objet d'une authentification. La mise en œuvre d'une règle DMARC évite toute atteinte à la réputation d'un expéditeur en raison d'actions réalisées par des spammeurs. Si vous ne protégez pas votre domaine au moyen de l'authentification DMARC, vos messages seront de plus en plus susceptibles d'être envoyés directement dans un dossier Courrier indésirable, voire d'être rejetés. »

John Rae-Grant,
Product Manager, Google

« Du jour au lendemain, les cybercriminels qui usurpaient un compte Yahoo! Mail pour envoyer des emails frauduleux et lancer des tentatives de phishing ont été stoppés net. »

Jeff Bonforte,
SVP of Communications Products, Yahoo!

SECTION 9

Glossaire des balises DMARC

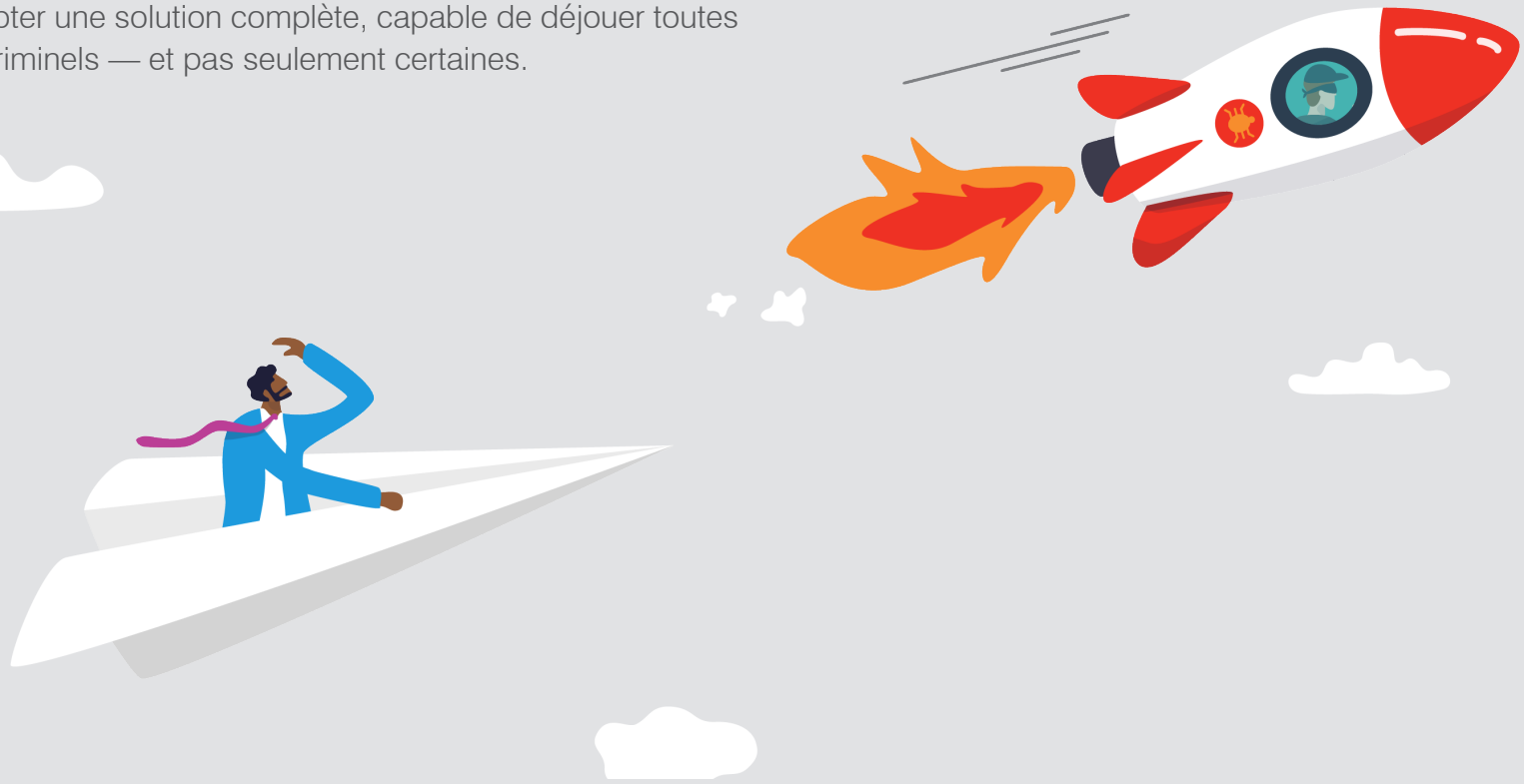
Nom de la balise	Finalité	Exemple
v	Version du protocole	v=DMARC1
p	Règle pour le domaine	p=quarantine
pct*	% des messages soumis au filtrage	pct=20
rua*	URI pour la transmission des rapports agrégés	rua=mailto:aggrep@exemple.com
sp*	Règle pour les sous-domaines du domaine	sp=reject
aspf*	Mode d'alignement pour SPF (strict ou relaxed)	aspf=r
ruf*	URI pour la transmission des rapports d'investigation numérique	ruf=mailto:aggrep@exemple.com
adkim*	Alignement pour DKIM (strict ou relaxed)	adkim=r
ri*	Nombre de secondes qui se sont écoulées entre l'envoi des rapports agrégés à l'expéditeur	ri=86400
fo*	Options pour la génération de rapports d'échec	fo=1

*Facultatif

SECTION 9

Lancez-vous : adoptez l'authentification DMARC

Les attaques BEC sont complexes et multidimensionnelles. C'est la raison pour laquelle vous devez adopter une solution complète, capable de déjouer toutes les tactiques des cybercriminels — et pas seulement certaines.



Bien qu'il n'existe pas de solution miracle contre les attaques BEC et EAC, le déploiement de l'authentification DMARC est un bon début. Il s'agit d'un élément essentiel de la lutte contre les imposteurs, en particulier ceux qui usurpent des domaines de messagerie de confiance. L'authentification DMARC est le moyen le plus efficace de lutter contre l'usurpation de domaines et d'empêcher des emails frauduleux d'utiliser votre domaine.

Chez Proofpoint, nous aidons certaines des marques les plus importantes au monde à déployer l'authentification DMARC. Et bien que chaque entreprise soit unique, la plupart suivent les étapes de déploiement présentées ci-dessous.

La première étape est très simple : créer un enregistrement DMARC dans le DNS et obtenir une visibilité sur l'ensemble de votre écosystème de messagerie.

Étape 1

Sélectionnez un domaine.

(Il peut s'agir de votre domaine de premier niveau ou d'un sous-domaine qui envoie beaucoup d'emails.)

Étape 2

Générez votre enregistrement à l'aide de notre **assistant de création d'enregistrements DMARC.** (Définissez la règle du destinataire des emails sur « none ».)

Étape 3

Demandez à l'administrateur de votre serveur d'ajouter votre enregistrement DMARC au DNS.

Étape 4

Commencez à recevoir des rapports DMARC concernant votre domaine.

Étape 5

Contactez notre équipe antifraude et nous vous aiderons à comprendre rapidement votre écosystème de messagerie.

Félicitations ! Vous avez fait un premier pas vers la lutte contre la fraude par email.

Pour en savoir plus sur la façon dont Proofpoint peut vous aider à lutter efficacement contre les attaques BEC et à protéger votre marque, visitez notre site à l'adresse **proofpoint.com/fr**.

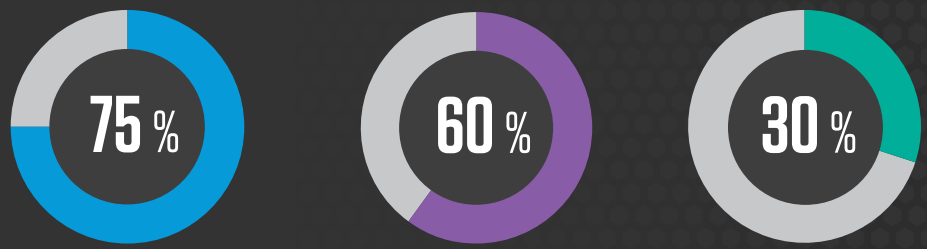
À propos de Proofpoint

Le graphique des menaces Nexus de Proofpoint compile les meilleures recherches sur la sécurité, technologies et données sur les menaces du secteur pour vous protéger tout au long du cycle des attaques. Aucun autre éditeur ne bénéficie d'une telle visibilité sur la façon dont les cyberattaques actuelles ciblent les personnes.

Chaque jour, nous analysons plus de :

2,6 Mrd D'EMAILS	**49 Mrd** D'URL	**1,9 Mrd** DE PIÈCES JOINTES
1,7 Mrd DE MESSAGES MOBILE	**430 Mio** DE DOMAINES WEB	**143 000** COMPTES DE RÉSEAUX SOCIAUX

Nos solutions ont été adoptées par plus de :



DU CLASSEMENT FORTUNE 100

DU CLASSEMENT FORTUNE 1000

DU CLASSEMENT FORTUNE GLOBAL 2000

8 000 GRANDES ENTREPRISES

200 000 PETITES ENTREPRISES

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0503-003-03-03 01/23