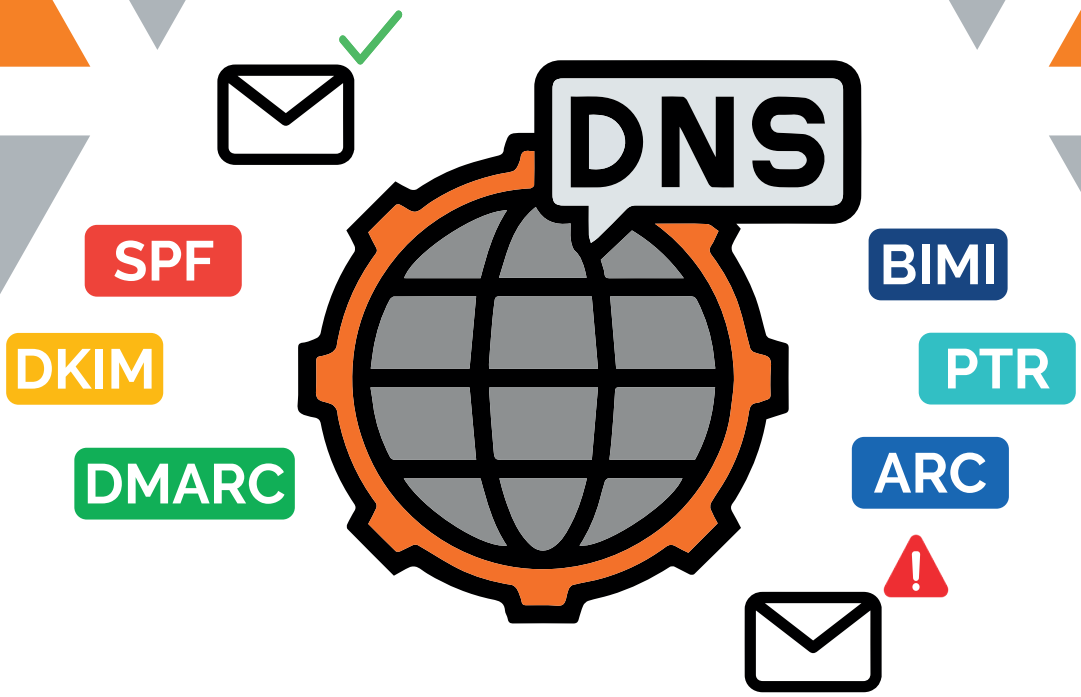
LIVRE BLANC



METTEZ AUX NORMES VOTRE MESSAGERIE PROFESSIONNELLE GRÂCE AU DNS

secuserve
email & security as a service

secuserve.fr
e-securemail.fr
optimails.fr

TABLE DES MATIÈRES

1. LA CONFORMITÉ DE VOTRE MESSAGE

La sécurité de vos communications en ligne est un impératif absolu. Les protocoles **SPF, DKIM et DMARC** pour votre **enregistrement DNS** sont des éléments concrets, garantissant l'authenticité des e-mails et renforçant leur sécurité.

LE SAVIEZ-VOUS ?

Une mauvaise configuration de ces protocoles dans votre DNS peut entraîner des problèmes majeurs, tels que la délivrabilité de vos messages ou l'usurpation de votre identité.

Voici les trois méthodes d'authentification d'un mail :

SPF

Sender Policy Framework (SPF) est une méthode d'authentification des courriels qui utilise des enregistrements DNS pour indiquer quels serveurs de messagerie sont autorisés à envoyer des courriels avec votre nom de domaine.

DKIM

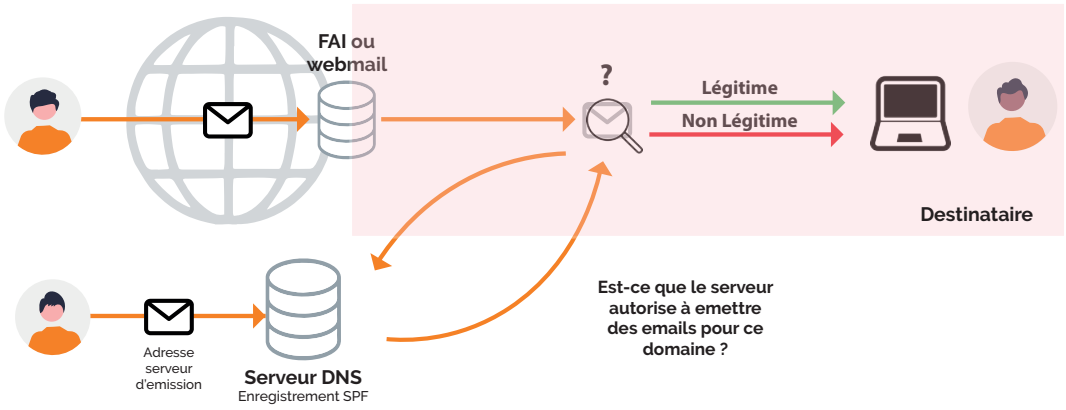
DomainKeys Identified Mail (DKIM) est une technique d'authentification du courrier électronique qui repose sur une signature numérique, dont la clé publique peut être consultée par le biais d'une recherche DNS. Elle permet de garantir qu'un courrier électronique a été envoyé par un serveur expéditeur autorisé et que le contenu du courrier électronique n'a pas été modifié au cours du processus.

DMARC

La méthode DMARC (Domain-based Message Authentication, Reporting & Conformance) permet aux propriétaires de domaines de publier une politique dans un enregistrement DNS qui spécifie les protocoles utilisés (SPF et DKIM) pour authentifier les messages électroniques envoyés à partir de leur domaine, et ce qu'il convient de faire avec les messages qui échouent à l'authentification.

1. LA CONFORMITÉ DE VOTRE MESSAGE

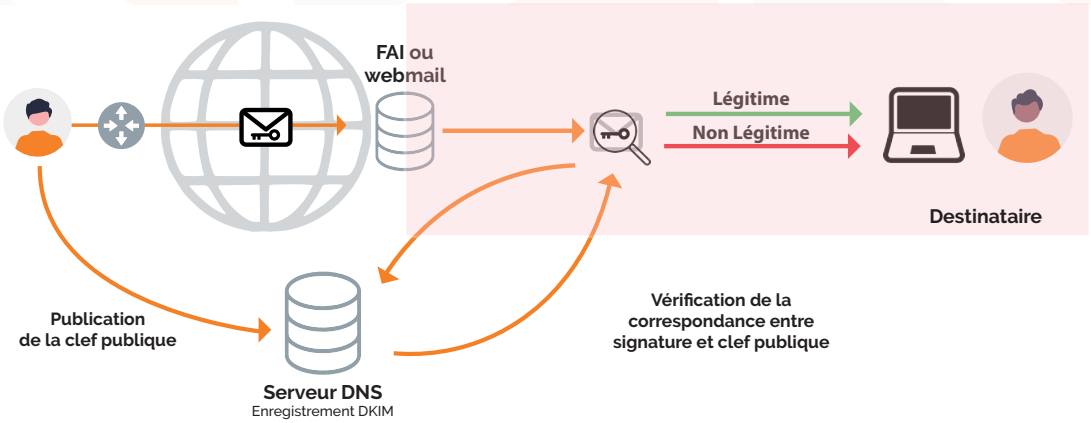
SPF



Exemple

```
"v=spf1
include:spf.
protection.out
look.com
include:includes
pf.security-mail.
net -all"
```

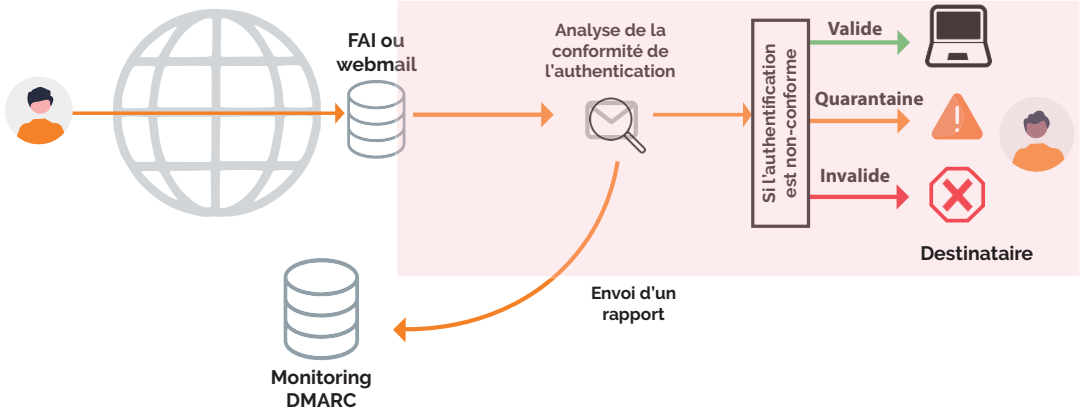
DKIM



Exemple

```
"v=DKIM1; k=rsa;
s=email;p=MIGfMAde
poxWjtuPxoe9efl
jie8era"
```

DMARC



Exemple

```
"v=DMARC1;
p=quarantine;
rua=mailto:
adresse@votre
domaine.com"
```

1. LA CONFORMITÉ DE VOTRE MESSAGE

QUELQUES PARAMÈTRES

SPF

Le champ all peut avoir **3 valeurs** :

-all N'autorise strictement aucun envoi autrement que par l'un des éléments listés.
~all Considère les envois par d'autres serveurs comme potentiellement illégitimes.
?all Signale qu'il existe des serveurs supplémentaires qui peuvent faire des envois.

DKIM

La longueur des clés DKIM :

Pendant des années, la longueur standard des clés DKIM était de 1024 bits, mais les pirates continuent à développer de nouvelles méthodes pour casser les clés DKIM. C'est pourquoi il recommandé d'utiliser des clés de 2048 bits.

DMARC

"_dmarc.example.com." fait référence au domaine spécifique dans lequel l'enregistrement DMARC est créé. Dans le cas présent, il s'agit de "exemple.com".

"IN TXT" indique qu'il s'agit d'un enregistrement de texte.

"v=DMARC1" signifie que la version de DMARC utilisée est la version 1.

"p=reject" définit la politique DMARC sur "reject", ce qui demande aux serveurs de messagerie de rejeter ou d'écarter les courriels qui échouent aux contrôles d'authentification DMARC.

"rua=mailto:dmarc@example.com"spécifie l'adresse électronique "dmarc@example.com" comme destination pour recevoir les rapports DMARC agrégés, qui fournissent des informations sur les résultats de l'authentification des courriers électroniques.

"ruf=mailto:forensics@example.com"désigne l'adresse électronique "forensics@example.com" comme destination pour recevoir les rapports DMARC, qui fournissent des informations détaillées sur les échecs d'authentification des courriers électroniques.

"sp=reject" définit la politique de sous-domaine sur "reject", garantissant que la politique DMARC s'applique également aux sous-domaines.

1. LA CONFORMITÉ DE VOTRE MESSAGE

LE PROTOCOLE ARC : LES MESSAGES RELAYES SONT FIABILISÉS

Malheureusement, lors d'un envoi d'e-mail, les systèmes d'authentification SPF & DKIM peut être confronter à des difficultés quand ceux-ci sont exposés à des redirections.

En effet, dans le cas **d'un transfert de message ou d'une redirection**, le contenu de l'e-mail ou de l'en-tête du message sont modifiés.

Ce qui compromet la fiabilité de la signature DMARC.

C'est ainsi que le protocole ARC entre en jeu !

ARC

Authenticated Received Chain (ARC) est un protocole d'authentification qui enregistre les résultats de bout-en-bout d'un e-mail **quand ce dernier passe par un flux de messagerie indirect (comme une liste de diffusion, un service de transfert d'e-mail, un serveur de relais ou encore un service de filtrage type SEG – Security Email Gateway).**

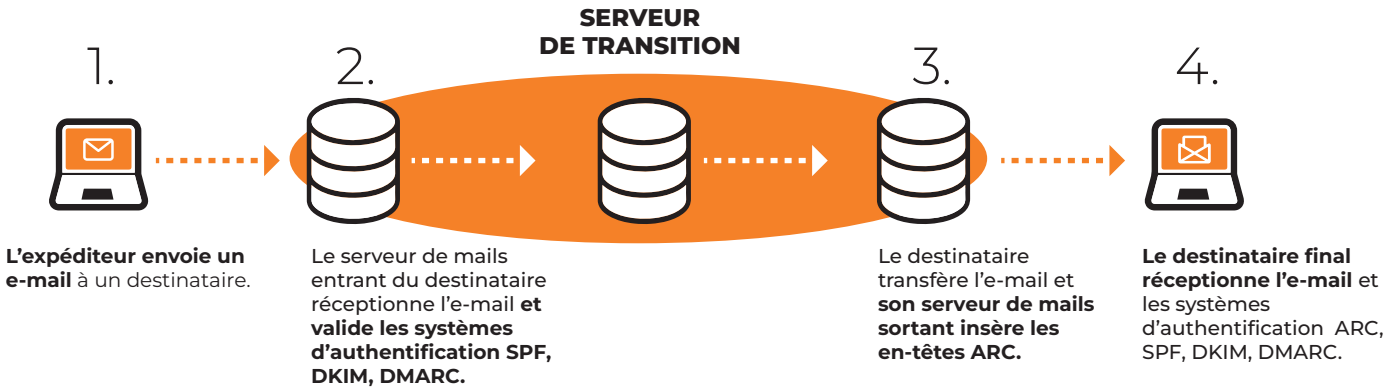
En d'autre termes, vous pouvez **attester la conformité de votre message** et réduire les échecs d'authentification des e-mails entrants dus à la modification des messages par les services de messagerie légitimes.

secuserve

1. LA CONFORMITÉ DE VOTRE MESSAGE

L'intégration de ARC constitue une amélioration sur la conformité de son message, ajoutant une couche supplémentaire en préservant l'authenticité de l'e-mail et de la passerelle de filtrage... (dans le cadre d'un service de filtrage par exemple).

Ce protocole a été développé dans le but de permettre à l'expéditeur de signer ses e-mails avec une **clé privée** et aux destinataires de vérifier cette signature à l'aide d'une **clé publique**, garantissant ainsi l'authenticité de l'expéditeur déclaré.



EXEMPLES

ARC

Si vous voulez être sûr que le protocole ARC est implémenté, il va falloir fouiller dans l'entête de vos e-mails sur votre messagerie et trouver les 3 tags suivants :

- **ARC-Authentication-Results**, soit l'état d'authentification dans lequel le message d'origine est reçu **(DMARC, SPF et DKIM)**.
- **ARC-Message-Signature**, soit la signature de type **DKIM** du message à l'expédition.
- **ARC-Seal**, soit la signature de type DKIM de la chaîne **ARC**.

Par exemple, on peut retrouver des informations comme le service de relayage par lequel votre email transite, il se trouve généralement sous la forme suivante :

```
from=******.nomduservice.com
```

1. LA CONFORMITÉ DE VOTRE MESSAGE

L'importance de la configuration SPF, DKIM et DMARC

Permet de certifier que vous êtes bien l'émetteur de l'email + Permet d'éviter l'usurpation de l'émetteur de l'email. + Permet de définir une politique de traitement des messages

Conformité

Cas d'utilisation : Interface e-securemail

Note : Lorsqu'il est disponible, chaque logiciel de filtrage email dispose de sa propre interface avec sa rubrique « Enregistrement DNS »

Paramétrer le protocole SPF :

1. Allez sur l'interface du service qui gère votre nom de domaine (Gandi, 1&1, OVH...)
2. Allez dans les paramètres de votre interface dans la rubrique «Enregistrement DNS».
3. Faites les démarches suivantes :

Ajouter l'enregistrement TXT
Récuperez l'enregistrement sur le portail Secuserve
Dans la rubrique «Activation du service e-securemail, copier l'adresse suivante **«v=spf1 include:includespf.secu-rity-mail.net -all»**
Ajouter dans la partie TXT sur votre interface.

Paramétrer le protocole DKIM :

1. Connectez-vous à votre interface e-securemail en cliquant sur le lien et rendez-vous au paramètre du domaine.
2. Cliquez sur « obtenir une clé publique » et copier la clé.
3. Retournez sur votre interface DNS du domaine
4. Faites les démarches suivantes

Ajouter l'enregistrement TXT
Saisir la première valeur correspondant au sous-domaine : **sec-sig-email._domainkey**
Coller la clé générée
5. Revenir sur la console d'aministration
6. Activer l'authentification DKIM.

Paramétrer le protocole DMARC : en s'appuyant sur le SPF & DKIM

1. Toujours sur l'interface du service où se stiue votre «enregistrement DNS»
2. Ajouter l'enregistrement TXT
3. Saisir dans le sous domaine les valeurs suivantes : «**_dmarc.votredomaine.com**» sur la zone de texte «Nom» et «**v=DMARC1 ; p=quarantine rua=mailto : rapport@votre-domaine.com**».

secuserve

Les cyberattaques ?! Lesquelles ?

LE SAVIEZ VOUS ?

La cybersécurité concerne toutes les structures (**TPE/PME, grandes entreprises, organisations publiques ou privées, etc**.) et tous les secteurs d'activité. Mais qui dit cybersécurité dit cyberattaques également. Avec un doublement du volume des données générées par les organisations tous les deux ans, il n'est pas surprenant que le risque augmente de façon exponentielle – ce que l'on a pu constater tout au long de 2022 avec une succession d'attaques cyber contre les établissements publics et/ou privés.

Dans le contexte actuel, nous devons anticiper une intensification des menaces cyber.
Les attaques par ransomware, fuites de données et usurpations d'identité continueront de prospérer. Bien que ces tactiques ne changent pas brusquement, des indices émergent des récentes intrusions.
Il est plausible que les pirates exploitent de nouvelles vulnérabilités dans l'écosystème grandissant d'objets connectés pour s'approprier nos informations confidentielles.

L'objectif crucial est de sensibiliser nos collaborateurs aux risques numériques. Le phishing, les malwares, l'arnaque au président et les attaques par mot de passe partagent une caractéristique commune : ils exploitent les erreurs humaines. Il est impératif de garantir que vos collaborateurs comprennent ces risques et soient bien informés sur les mesures de précaution. Et bien sûr, sécuriser sa messagerie grâce au DNS.

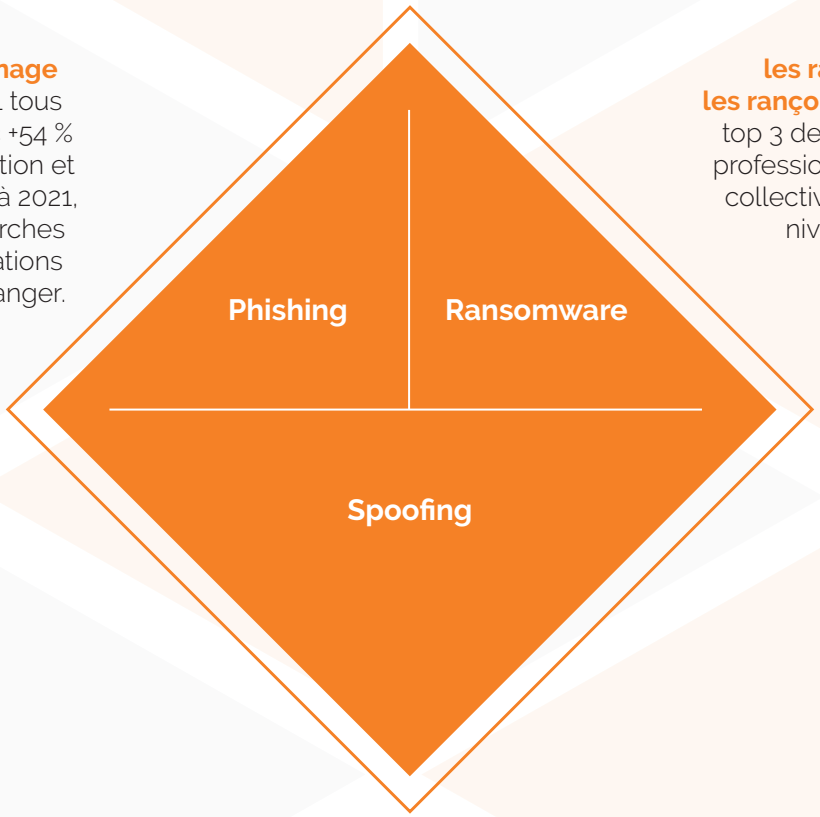
3. TYPES DE DANGER

Les principaux risques peuvent survenir avec des enregistrements DNS faussés ou inexistants.

Les domaines qui n'ont pas configuré correctement les protocoles SPF, DKIM et DMARC peuvent constater que leurs courriels sont mis en quarantaine comme spam ou ne sont pas remis à leurs destinataires. Ils risquent également de se faire usurper leur identité par des pirates.

POTENTIELLES MENACES

Phishing ou l'hameçonage constitue la menace n°1 tous publics confondus, avec +54 % de recherches d'information et d'assistance par rapport à 2021, soit 1,9 million de recherches d'assistance et consultations d'articles dédiés à ce danger.



les ransomwares ou les rançongiciels sont dans le top 3 des menaces pour les professionnels (entreprises et collectivités) et restent à un niveau très élevé.

Le spoofing ou L'usurpation d'identité touche plus de 210 000 Français chaque année.

Source : cybermalveillance.gouv.fr

3. TYPES DE DANGER

Phishing
(Hameçonnage)

L'hameçonnage, ou phishing, est la méthode des cybercriminels pour voler des informations personnelles et bancaires.

Étant donné que les tentatives de phishing sont transmises aux victimes sous la forme d'e-mails malveillants provenant de domaines d'entreprises usurpés ou falsifiés, l'e-mail malveillant échouera aux contrôles de vérification et, en fin de compte, à l'authentification **DMARC** en raison du mauvais alignement des domaines. DMARC mis en œuvre, le courriel est authentifié par rapport à **SPF** et **DKIM**.

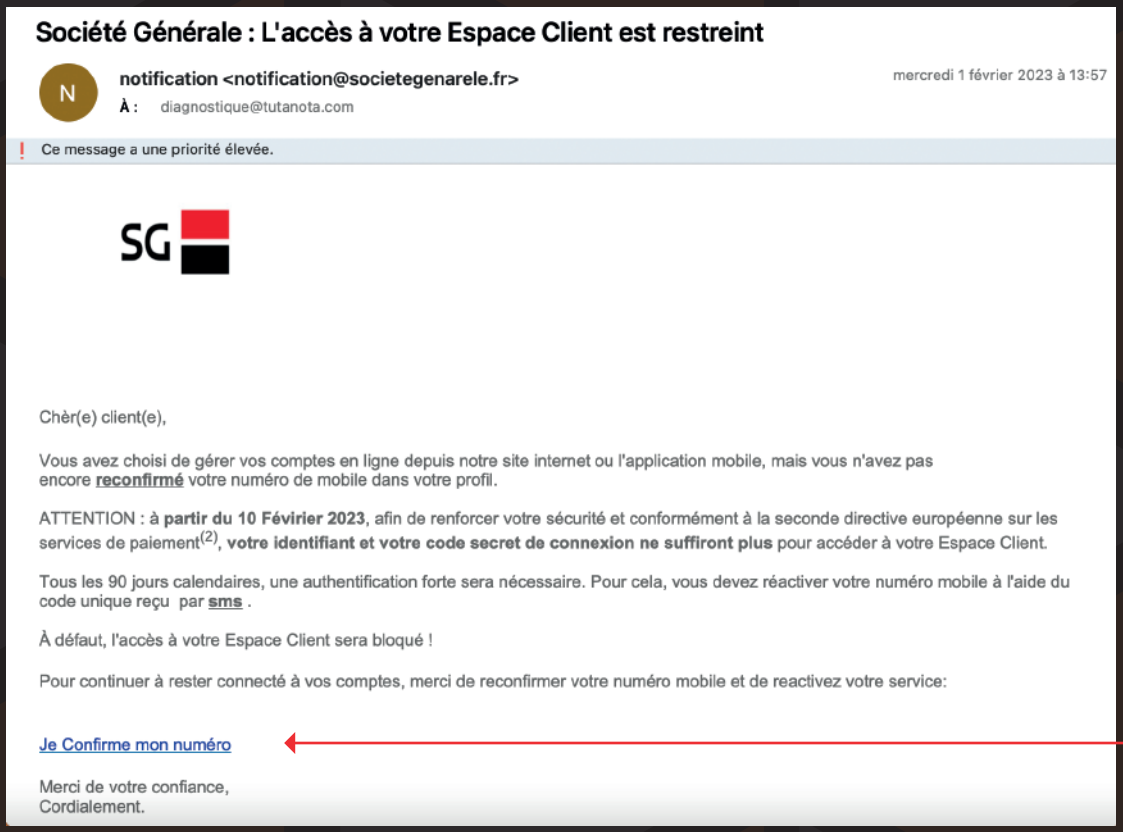
Comment agir ?

1. **METTRE EN PLACE UNE SOLUTION D'ANALYSE DE LIEN URL**

2. **SENSIBILISER VOS UTILISATEURS**
   Afin qu'ils survollent et prévisualisent les avant de cliquer.

3. **METTRE EN PLACE UN OUTIL DE RÉTROACTION**
   Afin de faciliter le signalement en cas de doute.

Exemple



Société Générale : L'accès à votre Espace Client est restreint

N **notification <notification@societegenarele.fr>** mercredi 1 février 2023 à 13:57
À : diagnostique@tutanota.com

! Ce message a une priorité élevée.

SG

Chèr(e) client(e),

Vous avez choisi de gérer vos comptes en ligne depuis notre site internet ou l'application mobile, mais vous n'avez pas encore **reconfirmé** votre numéro de mobile dans votre profil.

ATTENTION : à **partir du 10 Février 2023**, afin de renforcer votre sécurité et conformément à la seconde directive européenne sur les services de paiement[2], **votre identifiant et votre code secret de connexion ne suffiront plus** pour accéder à votre Espace Client.

Tous les 90 jours calendaires, une authentification forte sera nécessaire. Pour cela, vous devez réactiver votre numéro mobile à l'aide du code unique reçu par **sms** .

À défaut, l'accès à votre Espace Client sera bloqué !

Pour continuer à rester connecté à vos comptes, merci de reconfirmer votre numéro mobile et de reactivez votre service:

Je Confirme mon numéro

Merci de votre confiance,
Cordialement.

En général, si vous connaissez la destination d'un lien, vous pouvez repérer une tentative d'hameçonnage.

N'oubliez pas de survoler le lien avec votre souris pour vérifier le site vers lequel il redirige !

3. TYPES DE DANGER

Comment agir ?

1. **DÉBRANCHEZ LA MACHINE D'INTERNET** ou du réseau informatique.
2. **SIGNALEZ À CYBERMAVEILLANCE.FR**
3. **CONSERVEZ LES PREUVES** message(s) piégé(s), fichiers de journalisation (logs) de votre pare-feu, copies physiques des postes ou serveurs touchés.
4. **NOTIFIEZ L'INCIDENT À LA CNIL** s'il y a eu une violation de données personnelles.
5. **IDENTIFIEZ LA SOURCE DE L'INFECTION** prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire et réviser ou lancer votre PCA (Plan de Continuité).

Ransomware
(Rançongiciel)

Les rançongiciels ou ransomwares sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir l'accès. `

`

DMARC est la première ligne de défense contre les attaques de ransomware.
Il authentifie vos courriels en fonction des normes d'authentification SPF et DKIM, ce qui permet de filtrer les adresses IP malveillantes, les falsifications et les usurpations de domaine.

Exemple

ENC: Virement

PEDRO HENRIQUE BISPO FERREIRA <pedro.ferreira240@etec.sp.gov.br>

À : PEDRO HENRIQUE BISPO FERREIRA ; Cc : PEDRO HENRIQUE BISPO FERREIRA

Détails Nécessaires...
1 Mo

Télécharger • Aperçu

Bonjour,

Via cette correspondance, nous abordons la bonne nouvelle :

Vous trouverez les détails du bulletin ci-joint pour profiter de vos fonds.

Cordialement.

Présence d'une pièce-jointe pour un devis, ou une facture ou une candidature en cliquant dessus vous faîtes face à un risque de piratage.

secuserve

3. TYPES DE DANGER

Usurpation d'identité

Comment agir ?

L'usurpation d'identité ou spoofing se réfère à l'utilisation frauduleuse d'informations personnelles pour agir au nom d'une personne sans son consentement. Cette menace en ligne peut causer des dommages moraux et financiers.

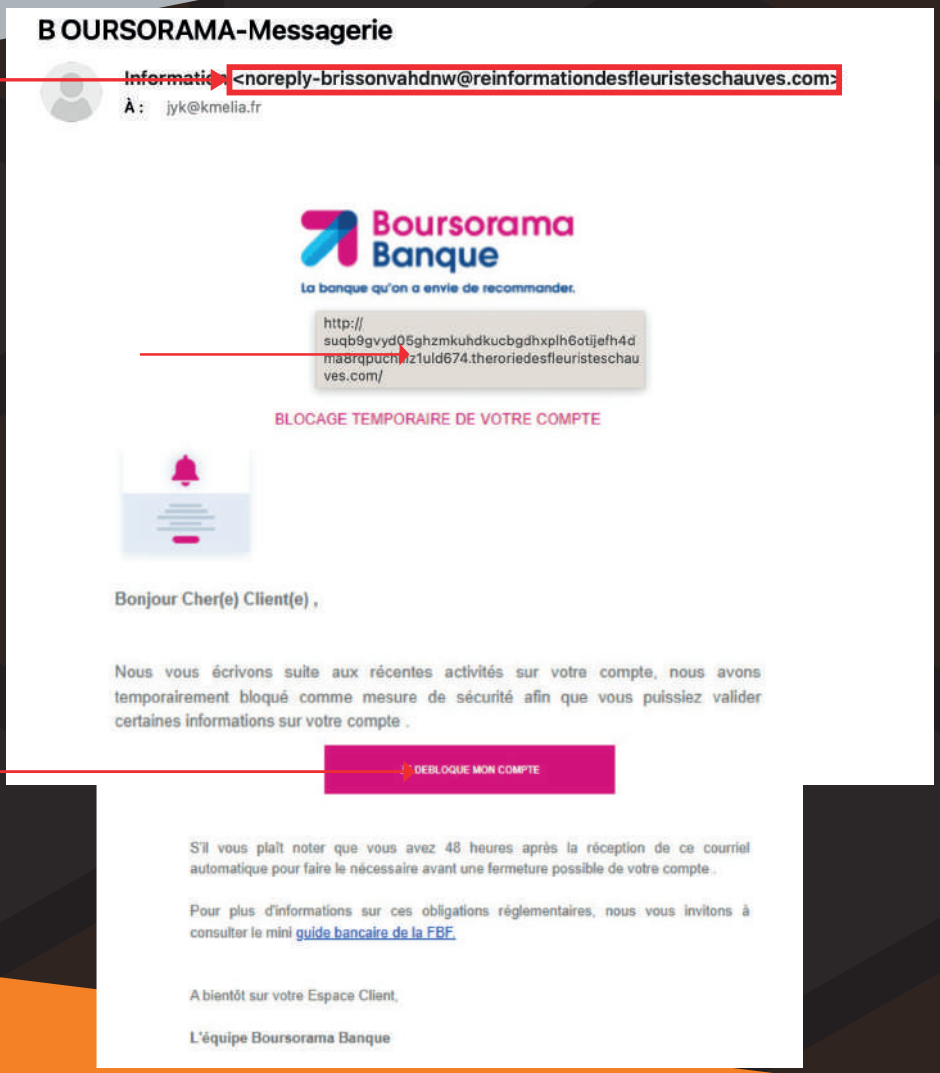
DMARC contribue à protéger votre marque contre l'usurpation d'identité, ce qui signifie que ces faux e-mails seront marqués comme spam ou ne seront pas transmis si les protocoles SPF et DKIM sont correctement configurés. (Le serveur récepteur essaiera de vérifier la source de l'envoi et la signature DKIM).

1. **VÉRIFIER SI L'ADRESSE DE PRÉSENTATION EST COHÉRENTE AVEC L'ADRESSE D'EMISSION.**

2. **FAITES ATTENTION AU TYPOSQUATTAGE** ou typosquatting.

3. **ASSUREZ-VOUS QUE L'ÉMETTEUR SOIT EN COHERENCE AVEC LE CONTENU DU MESSAGE.**

Exemple



Vérifiez l'adresse email de l'expéditeur et survolez les liens litigieux.

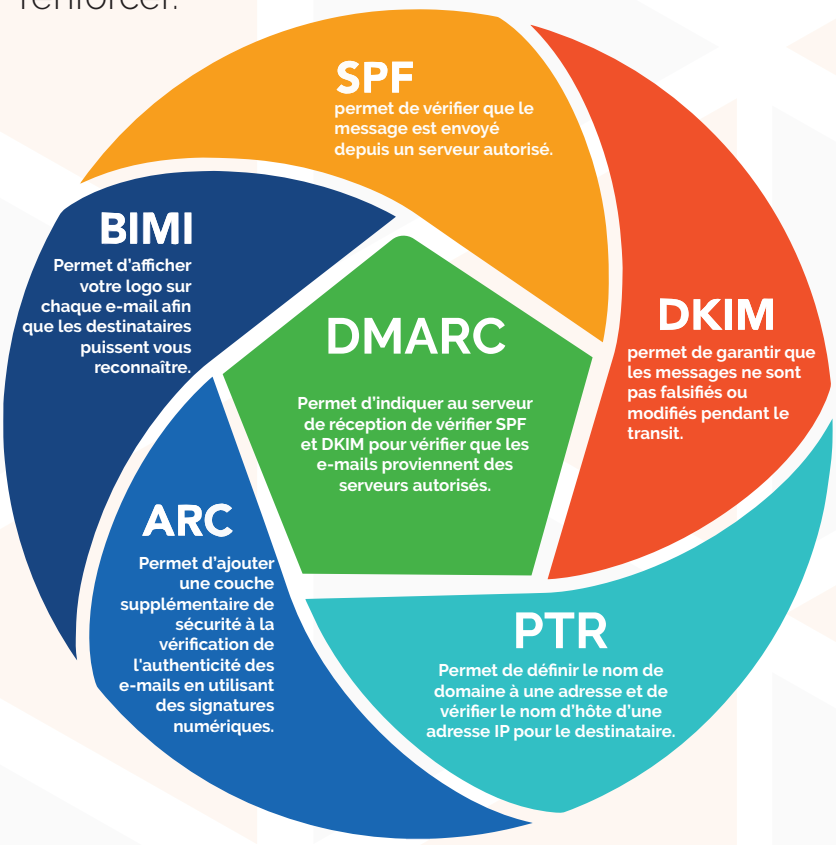
N'hésitez pas à lire les messages attentivement car ils contiennent souvent des fautes d'orthographe ou de grammaire...

secuserve
email & security as a service

4. CONCLUSION

Au sein de cette exploration des protocoles d'authentification DNS, chaque élément joue un rôle crucial dans la garantie de la validité des messages. La mise en place d'une stratégie de sécurité efficace pour les systèmes de messagerie requiert l'utilisation de multiples niveaux de protection.

Le **SPF**, en authentifiant les expéditeurs d'e-mails, le **DKIM** en signant les messages par cryptographie, et le **DMARC** en s'appuyant sur l'alignement, constituent des piliers essentiels pour assurer l'intégrité des en-têtes d'e-mails. Cependant, ces protocoles ne parviennent pas à éradiquer complètement les usurpations, d'où la nécessité de les renforcer.



Outre les trois protocoles majeurs (**SPF, DKIM, DMARC**), d'autres, tels que BIMI, PTR et ARC, viennent renforcer la sécurité des messageries.

BIMI, Brand Indicators for Message Identification coordonne les logos des expéditeurs,

PTR, Pointer Record résout les erreurs de syntaxe dans les dossiers DNS inverses.

ARC, Authenticated Received Chain suit l'authentification d'un e-mail à chaque étape de son traitement.

Ces éléments se révèlent tout aussi primordiaux que les précédents.
Dans le domaine des e-mails, les notions centrales sont la sécurité et la délivrabilité. Toutefois, il est indispensable de mettre en place une solution intégrale afin d'analyser le contenu de vos e-mails, vos pièces jointes et/ou URL, avec une capacité de rétroaction pour les utilisateurs.

Chez **Secuserve**, notre solution **e-securemail** est à votre service pour vous guider dans l'instauration d'une messagerie conforme et sécurisée.

e-securemail

LA SOLUTION DE FILTRAGE LA PLUS COMPLÈTE !

Protection complète des multiples menaces en constante évolution :
Virus, Vers, Hoaxes, SPAM, SCAM, Phishing, Pharming, Bombing,
Attaque en dénis de service, Usurpation d'identité, etc.
Authentification : SPF, DKIM, DMARC, **ARC (NOUVEAU !)**
MFA (multifacteurs)

Compatible avec

Microsoft 365

Taux de faux-positif < 0,01%
Garantie antivirus à 100%
Garantie anti-spam à 99%.

Gain conséquent en productivité :
Traitez uniquement les emails valides
Renforcez le confort d'utilisation et la délivrabilité
Disposez d'une haute disponibilité
Traçabilité en réception et en émission (100%)

Système de rétention des 30 derniers jours
Archivage de mail sur 1 année
Traçabilité totale du flux entrant et sortant

Evolution & innovation permanente :
Techniques et règles de filtrage régulièrement mises à jour, renforcées par **l'Intelligence Artificielle.**

+ 2500 règles de filtrage
Mise à jour régulière (toutes les 20 min) de la base virale de nos antivirus.

Une solution intégrale pour sécuriser votre messagerie

100% Saas — 100% Français

(DMARC, ARC) délivrabilité

antivirus renforcé (4x)

communication avancée

HÜmail technology

technologie antispam (16x)

extraction pièces jointes.

Conformité règlementaire

secuserve

SECUSERVE
c'est aussi....

+ Des solutions **100 % made in France**
+ de 12 000 entreprises protégées
+ 21 ans d'experience

secuserve
email & security as a service

Besoin d'un test ou d'un audit pour protéger votre messagerie ?

Alors contactez-nous !

Siège Social
74 Bd du 11 novembre 1918
69100 VILLEURBANNE
04 78 17 70 30

secuserve.fr
e-securemail.fr
optimails.fr

Agence de Paris
29 rue de Cléry
75002 PARIS
04 78 17 70 30