email-protocol

```
MARK RODERICK
```

E-mails : découverte des protocoles SMTP, POP, IMAP et MAPI

RESEAU CERTA > Analyse de mails malveillants et sécurisation

Terme	Définition / Description
Spam	Courriers électroniques indésirables envoyés en masse, souvent à des fins publicitaires ou pour diffuser des logiciels malveillants.
Spear phishing	Une attaque de phishing **ciblée** vers un individu ou une organisation spécifique, utilisant des informations personnelles pour paraître légitime.
Whaling	(Chasse à la baleine) Une forme de phishing qui vise spécifiquement les **hauts dirigeants** d'entreprises (PDG, cadres) pour voler des données stratégiques ou financières.
Smishing	Tentative d'hameçonnage réalisée par **SMS**. Le pirate envoie un message texte contenant un lien frauduleux pour piéger l'utilisateur.
Vishing	Tentative d'hameçonnage réalisée par **téléphone** (appel vocal). L'attaquant se fait passer pour un conseiller bancaire ou un technicien pour soutirer des informations.
Mail spoofing	Usurpation de l'adresse e-mail de l'expéditeur. Le pirate modifie l'en-tête du message pour faire croire qu'il provient d'une source de confiance.

Le protocole SMTP

Le **SMTP** (Simple Mail Transfer Protocol) est le protocole standard utilisé pour **envoyer des e-mails**.
Le processus suit une chaîne de serveurs appelés **MTA** (Mail Transfer Agent) :

1. **L'envoi :** Votre appareil envoie l'e-mail à votre serveur de messagerie.
2. **L'aiguillage :** Votre serveur consulte le **DNS** (via l'enregistrement **MX**) pour trouver l'adresse du serveur du destinataire.
3. **Le transfert :** L'e-mail est transmis de serveur en serveur jusqu'à destination.

Les ports à retenir

- **25 :** Port historique (standard, mais souvent non sécurisé).
- **587 :** Port moderne et **sécurisé** (recommandé).
- **465 :** Ancien port sécurisé, encore utilisé par certains hébergeurs.

Le Relais SMTP

C'est un serveur intermédiaire. Il sert de "passerelle" pour aider des appareils (ex: un NAS*(Network Access Service)*, une imprimante) ou des applications à envoyer leurs messages vers le serveur de messagerie final.

Le protocole POP

Le **POP3** (Post Office Protocol v3) est un protocole de **réception** d'e-mails.

Comment ça marche ?

Il fonctionne sur le principe du **téléchargement** :

1. Votre client (Outlook, Thunderbird) se connecte au serveur.
2. Il **récupère** les messages et les stocke localement sur votre appareil.
3. Par défaut, il **supprime** les messages du serveur une fois téléchargés.

Points clés

- **Pas de synchronisation :** Si vous lisez un mail sur votre PC, il disparaît du serveur et ne sera pas visible sur votre smartphone.
- **Usage unique :** Il est idéal si vous n'utilisez qu'**un seul appareil** pour consulter vos mails et que vous voulez libérer de l'espace sur le serveur.

Les ports à retenir

- **110 :** Port standard (non sécurisé).
- **995 :** Port **sécurisé** (POP over SSL/TLS).

Le protocole IMAP

Le **IMAP** (Internet Message Access Protocol) est le protocole moderne de **synchronisation** des e-mails.

Comment ça marche ?

Contrairement au POP, l'IMAP ne se contente pas de télécharger les messages :

1. **Miroir :** Il crée une copie des e-mails sur vos appareils (PC, smartphone) tout en laissant l'original sur le serveur.

2. **Synchronisation totale :** Toutes vos actions (marquer comme lu, déplacer dans un dossier, supprimer) sont récutées partout. Si vous lisez un mail sur votre téléphone, il apparaîtra comme lu sur votre ordinateur.
3. **Accès hors ligne :** Même si les mails restent sur le serveur, votre logiciel garde une "mémoire cache" pour vous permettre de les consulter sans internet.

Pourquoi le choisir ?

- **Multi-appareils :** C'est la solution idéale pour utiliser la même boîte mail sur plusieurs équipements.
- **Sécurité des données :** Comme tout reste sur le serveur, une panne de votre ordinateur n'entraîne pas la perte de vos e-mails (sauvegarde centralisée).

Type	Port
STANDARD	143(ou 220)
Sécurisé (IMAPS)	993(Recommandé)

Le protocole MAPI

Le **MAPI** (Messaging Application Programming Interface) est le protocole **propriétaire de Microsoft**. C'est le standard pour faire communiquer **Outlook** avec un serveur **Exchange** (ou Microsoft 365).

Pourquoi est-il supérieur à l'IMAP ?

Contrairement au POP ou à l'IMAP qui ne gèrent que les messages, le MAPI est un outil **collaboratif complet**. Il synchronise :

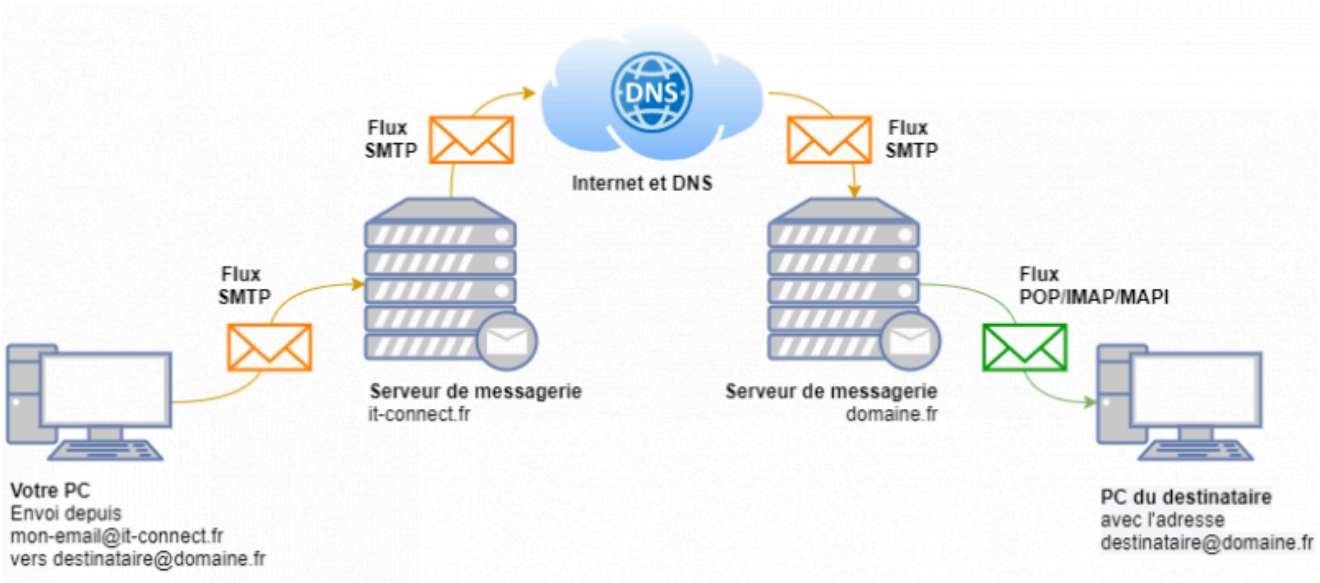
- Les e-mails.
- **Les calendriers** (rendez-vous, réunions).
- **Les contacts** (carnet d'adresses).

Le port à retenir

Comme il passe par des flux Web sécurisés (HTTPS), il utilise le port standard du Web :

- **443** (HTTPS sur TCP).
-

Schéma : envoi d'un e-mail



Abréviations à connaître

➡ **POP** - **P**ost **O**ffice **P**rotocol : télécharger e-mails sur le client

➡ **IMAP** - **I**nternet **M**essage **A**ccess **P**rotocol : synchroniser e-mails sur le client

➡ **MAPI** - **M**essaging **A**pplication **P**rogramming **I**nterface : protocole de communication client/serveur Exchange pour synchroniser les e-mails, le calendrier et les contacts

➡ **MUA** - **M**ail **U**ser **A**gent : client de messagerie (exemple : Outlook / Thunderbird)

➡ **MTA** - **M**ail **T**ransfer **A**gent : logiciel qui reçoit les e-mails d'un MUA dans le but de les acheminer

➡ **MDA** - **M**ail **D**elivery **A**gent : logiciel qui stocke les e-mails dans les boîtes aux lettres

Comprendre SPF

A. Qu'est-ce que SPF ?

Le **SPF** (Sender Policy Framework) est une sécurité DNS qui sert à **authentifier l'expéditeur** d'un e-mail.

À quoi ça sert ?

Son rôle principal est de lutter contre l'**usurpation d'identité** (spoofing). Il permet de vérifier que le serveur qui envoie l'e-mail a bien le droit de le faire au nom de votre domaine.

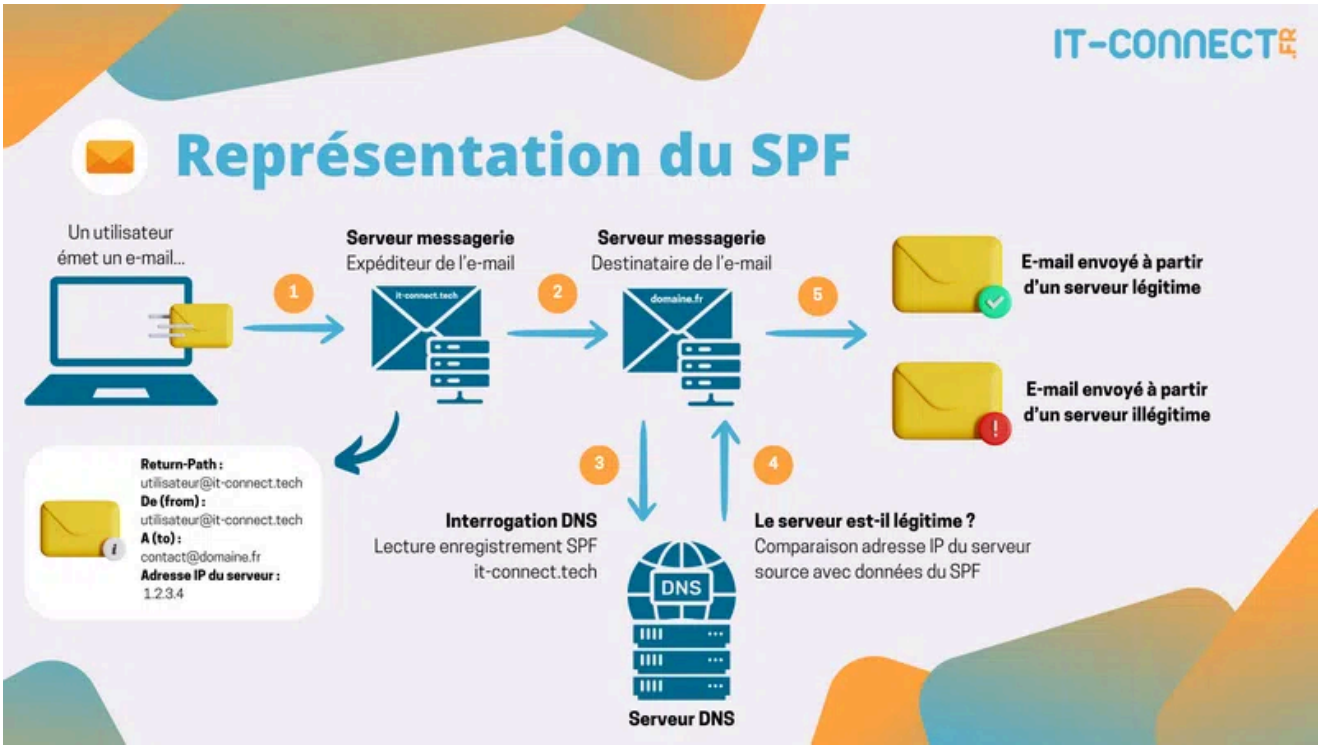
Comment ça marche ?

1. **La liste blanche :** Le propriétaire du domaine crée un enregistrement **DNS (type TXT)** listant les adresses IP autorisées à envoyer ses mails.
2. **La vérification :** Quand un serveur reçoit un e-mail, il regarde l'adresse IP de l'expéditeur.

3. **Le test :** Il interroge le DNS du domaine pour voir si cette IP est dans la "liste blanche".
4. **Le verdict :** * **IP autorisée :** Le mail est accepté.
    - **IP inconnue :** Le mail est rejeté ou envoyé en spam.

Le point technique important

Le SPF vérifie le champ technique **"Return-Path"** (l'adresse de retour) et non le champ "From" que vous voyez s'afficher. Comme cette protection peut être contournée, on utilise généralement le SPF en complément de **DKIM** et **DMARC**.



Comment mettre en place SPF ?

Étapes de configuration

1. **Inventaire :** Identifier toutes les adresses IP des serveurs autorisés à envoyer vos e-mails (votre serveur interne + services tiers comme les outils de newsletter).
2. **Rédaction :** Créer une ligne de texte spécifique regroupant ces adresses.
3. **Publication :** Ajouter cette ligne comme enregistrement de type **TXT** dans la **zone DNS publique** de votre domaine.

> **L'essentiel :** ***Le SPF est votre "liste blanche" officielle, publiée sur le web pour que les autres serveurs sachent qui est légitime.***

```
# Adresse IPv4
v=spf1 ip4:<adresse IPv4> -all
# Adresse IPv6
v=spf1 ip6:<adresse IPv6> -all
```

Comprendre DKIM

A. Qu'est-ce que DKIM ?

Le **DKIM** (DomainKeys Identified Mail) est le système de **signature numérique** qui garantit l'origine et l'intégrité de vos e-mails.

Comment ça marche ?

C'est un peu comme un sceau de cire moderne basé sur la cryptographie à clé publique :

1. **La signature (Clé Privée) :** Au moment de l'envoi, votre serveur signe l'e-mail avec une clé secrète. Cela crée une "empreinte" unique insérée dans l'en-tête du message.
2. **La publication (Clé Publique) :** Vous publiez la clé publique correspondante dans votre **DNS** (via un enregistrement **TXT**).
3. **La vérification :** Le serveur qui reçoit le mail récupère votre clé publique dans le DNS pour vérifier que la signature est valide.

Les deux garanties majeures

- **L'authenticité :** Elle prouve que le mail a bien été expédié par un serveur autorisé par votre domaine.
- **L'intégrité :** Elle garantit que le contenu du mail n'a pas été **modifié** ou falsifié pendant son transfert. Si un pirate change ne serait-ce qu'une virgule, l'empreinte ne correspond plus et la vérification échoue.