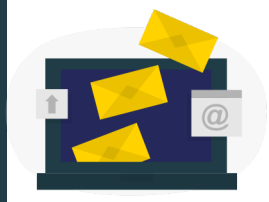
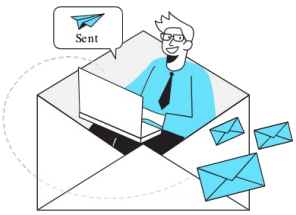
Fiche n°2

Sécurité

FICHE PRATIQUE



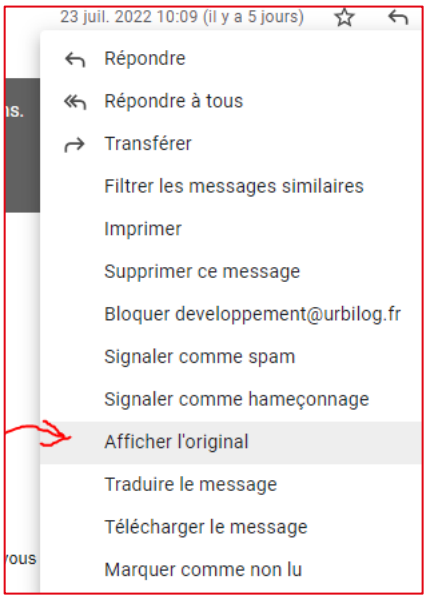
Comment vérifier si l'origine d'un mail est légitime ?



UTILISER L'OUTIL SPF (Sender Policy Framework)
>> Vérifier si l'expéditeur d'un courriel annoncé est légitime (si le nom indiqué est vrai).

1. Dans la fenêtre Gmail où le message a été ouvert, **appuyer sur les « … » en haut à droite**.

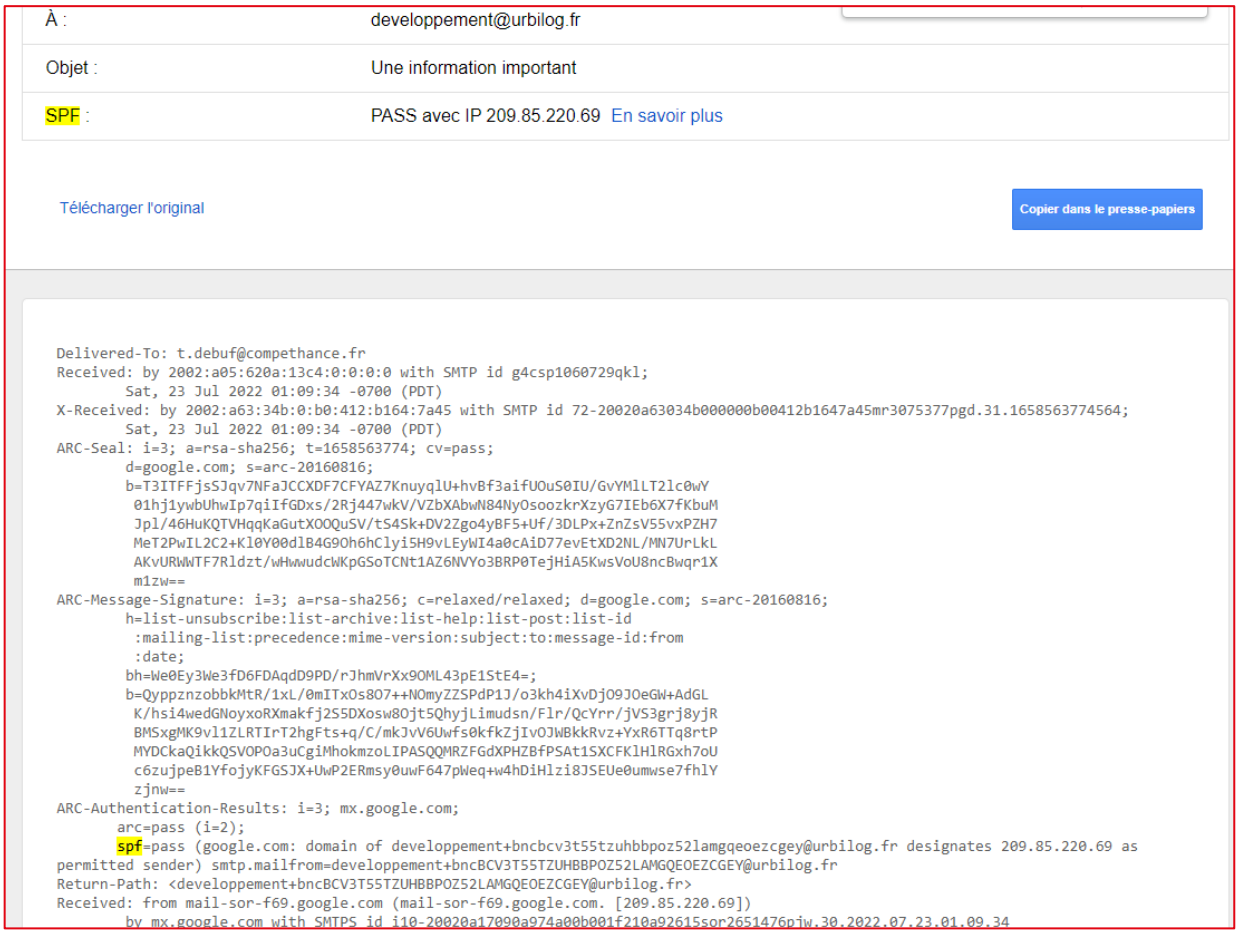
2. **Sélectionner « Afficher l'original »** pour ouvrir l'enveloppe technique du courriel.



Comment vérifier si l'origine d'un mail est légitime ?

FICHE PRATIQUE

3 **Rechercher** (Ctrl + F) **le mot-clé « SPF »** dans le corps du texte technique.



À :	developpement@urbilog.fr
Objet :	Une information important
SPF :	PASS avec IP 209.85.220.69 En savoir plus

Télécharger l'original — Copier dans le presse-papiers

```
Delivered-To: t.debuf@compethance.fr
Received: by 2002:a05:620a:13c4:0:0:0:0 with SMTP id g4csp1060729qkl;
        Sat, 23 Jul 2022 01:09:34 -0700 (PDT)
X-Received: by 2002:a63:34b:0:b0:412:b164:7a45 with SMTP id 72-20020a63034b000000b00412b1647a45mr3075377pgd.31.1658563774564;
        Sat, 23 Jul 2022 01:09:34 -0700 (PDT)
ARC-Seal: i=3; a=rsa-sha256; t=1658563774; cv=pass;
        d=google.com; s=arc-20160816;
        b=T3ITFFjsSJqv7NFaJCCXDF7CFYAZ7KnuyqlU+hvBf3aifUOuS0IU/GvYMlLT2lc0wY
         01hj1ywbUhwIp7qiIfGDxs/2Rj447wkV/VZbXAbwN84NyOsoozkrXzyG7IEb6X7fKbuM
         Jpl/46HuKQTVHqqKaGutXOOQuSV/tS4Sk+DV2Zgo4yBF5+Uf/3DLPx+ZnZsV55vxPZH7
         MeT2PwIL2C2+Kl0Y00dlB4G9Oh6hClyi5H9vLEyWI4a0cAiD77evEtXD2NL/MN7UrLkL
         AKvURWWTF7Rldzt/wHwwudcWKpGSoTCNt1AZ6NVYo3BRP0TejHiA5KwsVoU8ncBwqr1X
         m1zw==
ARC-Message-Signature: i=3; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=list-unsubscribe:list-archive:list-help:list-post:list-id
         :mailing-list:precedence:mime-version:subject:to:message-id:from
         :date;
        bh=We0Ey3We3fD6FDAqdD9PD/rJhmVrXx9OML43pE1StE4=;
        b=QyppznzobbkMtR/1xL/0mITxOs8O7++NOmyZZSPdP1J/o3kh4iXvDjO9JOeGW+AdGL
         K/hsi4wedGNoyxoRXmakfj2S5DXosw8Ojt5QhyjLimudsn/Flr/QcYrr/jVS3grj8yjR
         BMSxgMK9vl1ZLRTIrT2hgFts+q/C/mkJvV6Uwfs0kfkZjIvOJWBkkRvz+YxR6TTq8rtP
         MYDCkaQikkQSVOPOa3uCgiMhokmzoLIPASQQMRZFGdXPHZBfPSAt1SXCFKlHlRGxh7oU
         c6zujpeB1YfojyKFGSJX+UwP2ERmsy0uwF647pWeq+w4hDiHlzi8JSEUe0umwse7fhlY
         zjnw==
ARC-Authentication-Results: i=3; mx.google.com;
       arc=pass (i=2);
       spf=pass (google.com: domain of developpement+bncbcv3t55tzuhbbpoz52lamgqeoezcgey@urbilog.fr designates 209.85.220.69 as
permitted sender) smtp.mailfrom=developpement+bncBCV3T55TZUHBBPOZ52LAMGQEOEZCGEY@urbilog.fr
Return-Path: <developpement+bncBCV3T55TZUHBBPOZ52LAMGQEOEZCGEY@urbilog.fr>
Received: from mail-sor-f69.google.com (mail-sor-f69.google.com. [209.85.220.69])
        by mx.google.com with SMTPS id i10-20020a17090a974a00b001f210a92615sor2651476pjw.30.2022.07.23.01.09.34
```

4 **Être très vigilant si l'une des réponses SPF au moins est « Fail »** : il est possible que l'identité de l'expéditeur soit fausse.

```
X-Original-Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of developpement@urbilog.fr does not designate 164.100.146.28 as permitted
smtp.mailfrom=developpement@urbilog.fr
```

- *Il reste malheureusement des messages frauduleux sans « SPF Fail ».*
- *Il y a aussi de nombreux messages corrects qui ont des « SPF Fail » (leur configuration de messagerie n'est pas complètement conforme).*
- *Cependant, en cas de doute sur un message, le signal « SPF Fail » est un avertissement supplémentaire que ce message est suspect.*