MAÎTRISER

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE MESSAGERIE OS 7 ET PLUS

REMONTEZ À LA SOURCE D'UN MAIL

L'adresse IP de l'envoyeur apparaît toujours dans la source des messages.

Le message que vous venez de recevoir vous semble des plus douteux ? Voici comment mener l'enquête et identifier son auteur.

1 TROUVEZ L'ADRESSE IP DE L'EXPÉDITEUR...

Phishing, spam, faux amis, les mails renferment parfois des informations erronées, voire de vraies menaces sous forme de pièces jointes. Pour connaître l'identité de l'envoyeur, affichez l'en-tête complet du message. Dans Gmail, par exemple, ouvrez le courriel, cliquez sur les points situés à côté de la flèche de réponse dans le coin droit de la fenêtre de lecture, puis sur Afficher l'original. Avec Outlook, accédez aux options du mail et pointez sur Afficher la source du message. Lancez ensuite une recherche sur le terme IP à l'aide du raccourci clavier Ctrl + F. L'adresse de l'expéditeur doit figurer dans la partie Received ou Received-SPF. Gmail, lui, délivre cette info dans le résumé Message d'origine.

2 ... ET VÉRIFIEZ-EN L'ORIGINE

Copiez cette adresse, matérialisée par une suite de chiffres (194.158.98.82, par exemple). Connectez-vous ensuite sur bit. ly/2Hb7UWk, le programme de pistage d'IP en ligne SuperTool. Collez l'IP dans la zone de saisie, activez la flèche à droite du bouton MX Lookup, puis optez pour Reverse Lookup. Les résultats révèlent le patronyme de l'expéditeur dans la partie IP Adress ainsi que son nom de domaine.

Attention : si l’envoyeur recourt à un réseau privé virtuel, les infos de localisation seront faussées et pointeront vers le serveur relais utilisé pour brouiller les pistes.