



INGÉNIERIE SOCIALE l'usurpation d'adresse électronique

BAS_166



Ingénierie sociale : l'usurpation d'adresse électronique

🔴 Il peut arriver de recevoir un message d'erreur indiquant qu'un courriel « **n'a pas pu être distribué** », alors même que vous êtes certain de n'avoir rien envoyé. Le message parle d'un « **expéditeur inconnu** », d'un « **mail rejeté** », et contient parfois une pièce jointe censée montrer le message d'origine. La première réaction est souvent l'inquiétude et on se demande alors si notre boîte a été piratée. Dans ce nouvel épisode de la **Minute numérique**, nous démêlons ce qui se passe réellement, et comment réagir face à l'usurpation d'adresse électronique.

😬 Ce scénario est **une forme d'ingénierie sociale**, c'est-à-dire une manipulation qui ne s'attaque pas à votre ordinateur directement, mais à **votre comportement** : elle mise sur votre surprise ou votre inquiétude pour vous faire commettre une erreur. Ce type d'attaque reste relativement rare, mais elle peut être redoutable pour qui ne la connaît pas, en particulier lorsqu'elle touche une **boîte mail professionnelle, d'entreprise ou d'institution**, où la réception de notifications techniques paraît plus habituelle.

🔍 Dans la grande majorité des cas, votre boîte n'a pas été piratée. Ce que vous observez s'appelle une usurpation d'adresse : des personnes mal intentionnées ont utilisé **votre adresse électronique comme fausse adresse d'expéditeur pour envoyer des messages en votre nom à d'autres destinataires**. Ces messages étant refusés par les serveurs de messagerie, des alertes d'erreur automatiques vous sont renvoyées. Vous recevez donc des notifications concernant des courriels que vous n'avez jamais écrits.

⚠ Il existe cependant une **deuxième situation**, plus dangereuse pour vous. **Certains escrocs fabriquent de faux messages d'erreur de toutes pièces**, sans qu'il y ait eu aucun envoi réel. Le message est conçu pour vous inquiéter, vous inciter à **ouvrir une pièce jointe ou à cliquer sur un lien**, et ainsi accéder à vos informations personnelles si vous allez plus loin. C'est ce qu'on appelle de **l'hameçonnage**, ou « phishing ». Lorsque le message est conçu pour une personne précise, avec des détails personnels ou professionnels qui le rendent alors particulièrement crédible, on parle alors de « spear phishing », que l'on traduit par **harponnage**. Contrairement à l'hameçonnage classique qui vise le plus grand nombre, **le harponnage vous cible spécifiquement, ce qui le rend souvent plus difficile à détecter**.

😬 Dans tous les cas, ces attaques jouent sur les mêmes ressorts psychologiques, que les escrocs connaissent bien. **La surprise d'un message inattendu attire immédiatement l'attention**. L'inquiétude de voir son adresse utilisée sans son accord pousse à vouloir agir vite, souvent sans prendre le temps de réfléchir. Et la forme technique du message, qui imite une notification officielle de serveur, crée une illusion de sérieux qui encourage à ouvrir la pièce jointe ou à cliquer sur le lien. **Ces mêmes ressorts se retrouvent dans la plupart des arnaques numériques** : fausses factures, faux colis, fausses alertes de sécurité. Les connaître à l'avance, c'est déjà se protéger.

💡 La conduite à tenir est simple. **Ne jamais ouvrir les pièces jointes ni cliquer sur les liens contenus dans ce type de message**, même s'il semble sérieux ou officiel. Il faut **supprimer le message ou le signaler comme indésirable**. Si le phénomène se répète ou s'intensifie sur plusieurs jours, il est alors prudent de **changer le mot de passe de sa boîte mail et d'activer la validation en deux étapes**, une option disponible dans les paramètres de la plupart des services de messagerie, qui ajoute une vérification par SMS ou par une application de votre téléphone au moment de la connexion. Enfin, **n'hésitez pas à parler de ce type de message autour de vous**, à vos proches ou à vos collègues, en leur décrivant à quoi il ressemble et ce qu'il ne faut pas faire. **Plus ces mécanismes sont connus, moins ils sont efficaces**.

sos Si vous rencontrez des difficultés dans la manipulation des outils numériques, **la CCAPV propose des ateliers numériques d'accompagnement** gratuits et accessibles à tous, y compris aux professionnels, organisés sur tout le territoire de la CCAPV.

☎ Contactez le **Conseiller numérique de la CCAPV** au 07 88 85 43 71 ou par courriel : conseiller.numerique@ccapv.fr

🔗 Pour retrouver toutes les dates d'ateliers, rendez-vous sur le site de la CCAPV à cette adresse : ccapv.fr/services-publics/france-services/conseils-numeriques