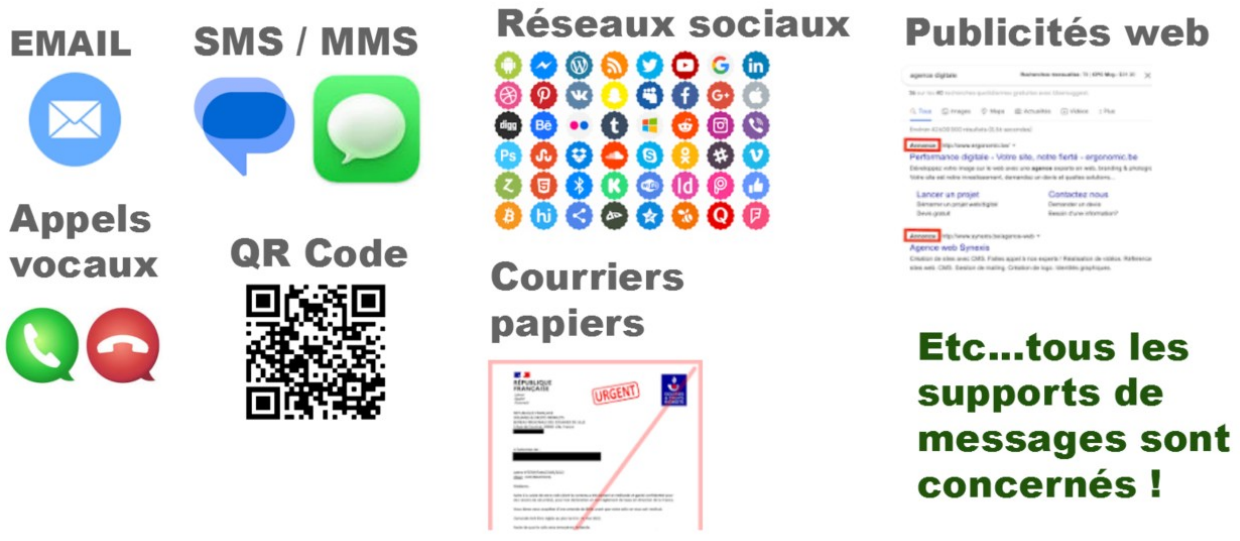
Technologie : 5e	Chapitre 4 : Cybersécurité	
2025-2026	**L'hameçonnage - "Phishing" en anglais** **Synthèse**	

L'hameçonnage (**phishing en anglai**s) est une technique qui consiste à envoyer un message visant à tromper son destinataire en l'amenant vers des ressources malveillantes pour collecter des données personnelles, puis réaliser des arnaques ou des cyber-attaques.

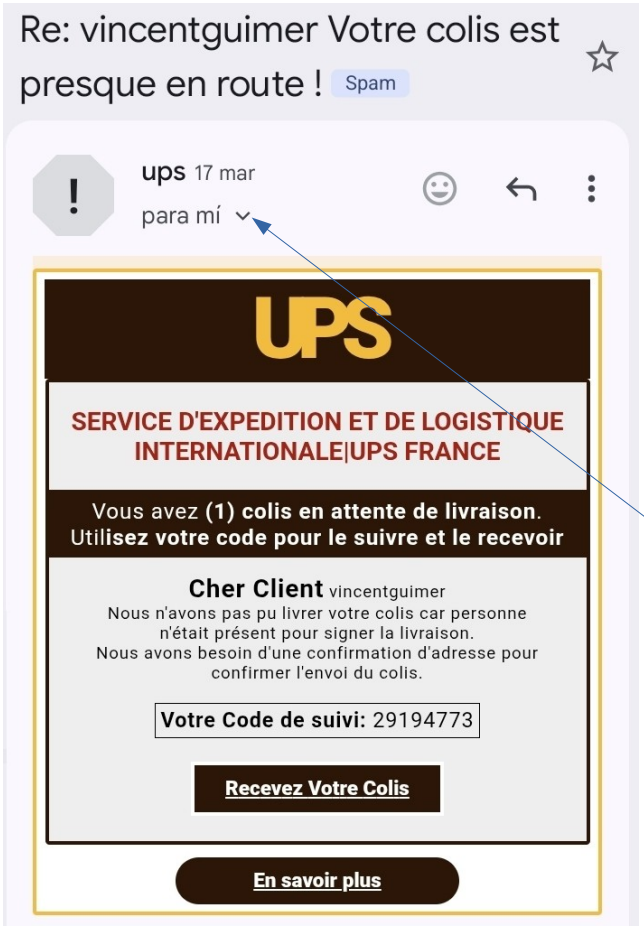
Voici les 5 signes de danger d'un faux email de hameçonnage (phishing) :

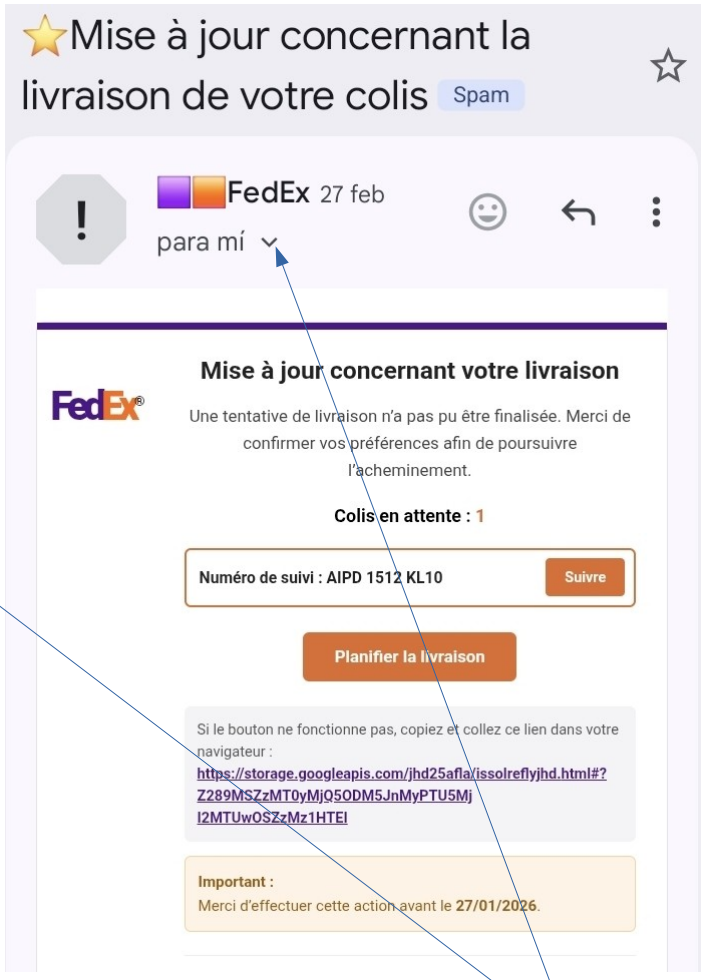
Indices d'alerte	Explication

Attention, le hameçonnage (phishing) peut aussi être fait par un autre moyen de communication que les emails :

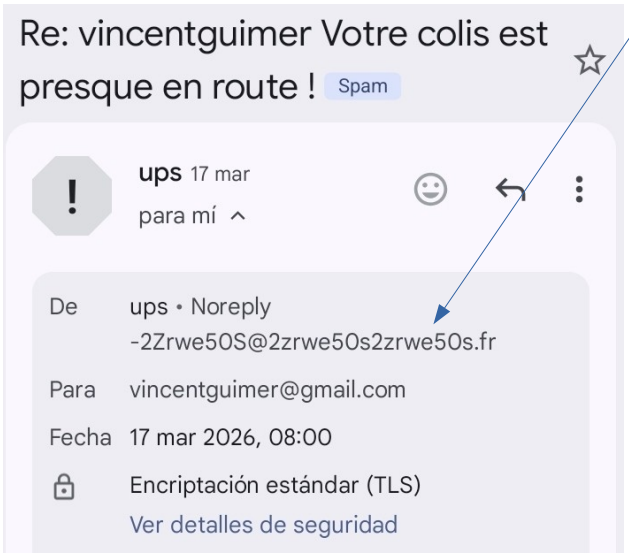


Exemples d'emails reçus qui sont clairement du hameçonnage (phishing) :





Utilisation d'un logo officiel, de mon nom, mais il suffit de cliquer sur la flèche pour faire apparaitre l'adresse email réelle de l'expéditeur qui est clairement fausse



Complément : le "Quishing"

https://www.youtube.com/watch?v=wUgRh7WO_rw

https://www.youtube.com/watch?v=-Go9bvdhLpk

Le « quishing » (contraction de QR code et phishing) consiste à remplacer de vrais QR codes par des faux, redirigeant vers des sites frauduleux pour voler des données bancaires ou personnelles. Un exemple courant est le collage d'un faux code dans des lieux publics, volant des centaines d'euros aux victimes.

Exemples concrets d'utilisation :

Bornes de recharge électrique : Des fraudeurs collent un faux QR code sur celui d'une borne. La victime, en voulant payer sa recharge, scanne le code et est dirigée vers un site factice qui subtilise ses coordonnées bancaires.

Parking : Dans les centres-villes, de faux QR codes remplacent les originaux, incitant à payer le stationnement sur un site frauduleux.

Faux avis de passage (envoi de colis) : Des malfaiteurs déposent de faux avis dans les boîtes aux lettres. Le QR code promet un suivi de colis mais mène à un site de phishing.

Restaurants et terrasses : Les QR codes des menus sur les tables sont recouverts, redirigeant vers un site frauduleux pour obtenir des informations personnelles.

Audioguides touristiques : Des faux QR codes sont affichés près de monuments, proposant un "audioguide gratuit" qui installe des logiciels malveillants ou vole des données.

Comment se protéger :

- Vérifiez si le QR code est une **étiquette collée** par-dessus le vrai QR code.
- Vérifiez l'URL du site avant de saisir des informations.
- Privilégiez les applications officielles ou l'adresse URL manuelle.

En résumé : comment mieux protéger ses données personnelles :

1. Créer des mots de passe solides et différents pour chaque compte
2. Mettre à jour les appareils et logiciels régulièrement
3. En ligne, en dire le moins possible sur soi
4. Conserver une copie de ses données en lieu sûr
5. Se méfier des messages inattendus et alarmants
6. Eviter les contenus ou logiciels piratés
7. Eviter de scanner des QR codes dans des lieux publics sans vérifier avant si c'est un faux.

LES RISQUES DU PHISHING

1 L'Effet boule de neige, c'est-à-dire l'envoi de mails frauduleux à vos contacts

2 L'usurpation d'identité numérique

3 La compromission de comptes professionnels, scolaires, personnels

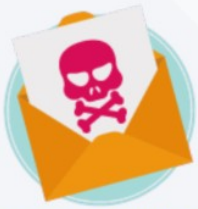
4 L'atteinte à la réputation

5 Le vol de données sensibles (personnelles, bancaires, familiales, etc.)

LES BONS REFLEXES

1 Vérifiez l'expéditeur du message, et le langage employé *(caractère d'urgence, émotion, bonnes affaires, etc.)*

2 Vérifiez les liens dans le courriel avant de cliquer dessus, *dans le but d'identifier si le site est légitime ou non*



3 Ne communiquez jamais d'information sensible suite à un message ou un appel

4 Au moindre doute, contactez directement l'organisme concerné pour confirmer

5 N'hésitez pas à contacter l'expéditeur (si connu), *via* un canal autre que celui d'origine *(une adresse de messagerie peut aussi être falsifiée)*

6 Activez la double authentification