CDG10 CDG Marne 52 CENTRE DE GESTION FONCTION PUBLIQUE TERRITORIALE

# FOCUS SÉCURITÉ RGPD N°4
# LE PHISHING

## HAMMEÇONNAGE, *PHISHING* : KEZAKO ?

**L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à vous leurrer pour vous inciter à mener une action ou à communiquer des données personnelles (identifiants, mots de passe, etc.) et/ou bancaires en se faisant passer notamment pour un tiers de confiance.**

**Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur, de site de commerce en ligne, d'administrations, etc.**

***La technique d'hameçonnage s'appuie sur 3 leviers pour endormir votre vigilance***

**La convoitise ou l'intérêt :**
*« Vous êtes notre heureux gagnant d'un iphone d'une valeur de 1 000 €, vous n'avez que les frais d'expédition à payer… »*

**La pression, la peur ou l'urgence :**
*« Votre compte va être désactivé dans 1j, pour le réactiver cliquez ici… »*

**Une apparence de légitimité :**
*« Bonjour M. Pigeon, je suis votre conseiller de la Banque BigPognon, il faudrait que vous actualisiez vos informations de contact sur notre site, lien ici »* avec un site parfaitement contrefait.

**La personnalisation du phishing :** votre nom, votre banque, un message attendu (attente réelle de livraison), la réutilisation d'un vrai message précédent (boite mail piratée d'un contact) **rend plus difficile la détection.**

**LEVIER D'INTÉRÊT**

**ENDORMISSEMENT DE LA VIGILANCE**

**CIBLAGE**

**LEVIER DE LÉGITIMITÉ**

*« Quand j'étais **en arrêt maladie**, j'ai reçu un mail de la sécurité sociale m'annonçant un remboursement de 200 € de frais de santé **que j'attendais**. J'ai **cliqué sur le lien** et je suis arrivé sur **un site qui avait l'air officiel**. Ce site me proposait d'être **remboursé immédiatement** si je donnais **mon numéro de carte bancaire**. Je ne me suis pas méfié et je l'ai fait mais le remboursement n'est jamais arrivé.*
*J'ai contacté la sécurité sociale pour me renseigner et le conseiller m'a annoncé que je m'étais fait arnaquer. J'ai immédiatement prévenu ma banque pour bloquer ma carte, mais plusieurs prélèvements avaient déjà été faits sur mon compte. »*

## UNE TECHNIQUE LUCRATIVE EN CONSTANTE AMÉLIORATION

Si les tentatives d'hameçonnage étaient grossières il y a quelques années (mail générique en franglais avec de nombreuses fautes), aujourd'hui, **les tentatives sont de mieux en mieux réalisées** (logo officiel, personnalisation, provenance cohérentes, adresse expéditeur cachée, site parfaitement contrefait, etc.).

Les cybercriminels exploitent **l'ingénierie sociale**, les informations issues **d'exfiltration de fichiers**, les courriels et contact issues de **boites mail piratées**, les informations accessibles sur les **réseaux sociaux** pour mieux cibler les victimes et endormir leur vigilance.

**Pour en savoir + :**
Fiche jointe sur l'hammeçonnage
Excellent dossier de Cybermalveillance.gouv.fr
Avec notamment :
Comment reconnaître un mail d'hameçonnage ?
Comment signaler un hameçonnage ?

***Ça vous rappelle quelqu'un ?***