Le Phishing (ou hameçonnage) est une technique qui consiste à dérober des informations confidentielles (mot de passe, numéro de carte de crédit…), à une victime afin de lui pour détourner des fonds. Pour cela, le fraudeur essaye de se faire passer pour un tiers de confiance. L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet, d'un message électronique.

Ces attaques par Phishing font de plus en plus de victimes et la messagerie professionnelle de l'académie est régulièrement la cible de telle attaque. Il convient d'ailleurs de souligner que les e-mails piégés adressés par des tiers se faisant passer pour votre banque, votre opérateur, un de vos collègues afin de détourner des informations personnelles sont de plus en plus trompeurs (le message est souvent personnalisé et sans faute d'orthographe), ce qui nécessite d'être vigilant.

Comment identifier les tentatives de Phishing ?

- Vous recevez un courriel alarmiste ou encore un prétendu remboursement en votre faveur qui semble provenir d'une source de confiance (banque, impôts, etc..). Vous êtes invité à vous rendre sur une page de formulaire afin de fournir des données personnelles.
- Vous recevez un courriel dans lequel il vous est demandé de « mettre à jour » ou de « confirmer suite à un incident technique » vos données, notamment bancaires.
- Vous recevez un mail de votre opérateur vous précisant que votre banque a refusé le dernier prélèvement en vous enjoignant de régler au plus vite votre facture.
- Vous recevez un mail de la boîte aux lettres I-prof avec un lien pour la consulter (fig 1)

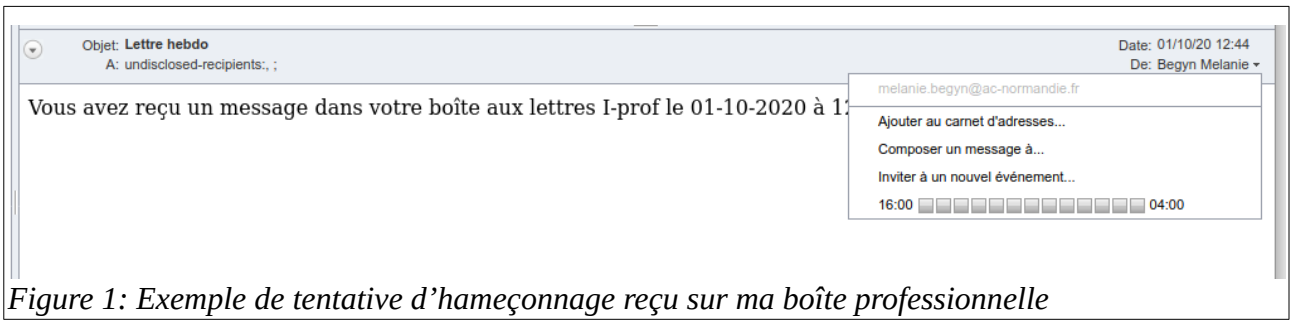

Figure 1: Exemple de tentative d'hameçonnage reçu sur ma boîte professionnelle

Le mode opératoire et les conséquences du phishing

Vous recevez un mail, un SMS d'une personne mal intentionnée qui se fait passer pour votre opérateur. En cliquant sur le lien présent dans le message frauduleux, vous êtes automatiquement renvoyé sur une page internet contrefaite, portant le logo de l'opérateur. Confiant, vous communiquez spontanément les informations qui vous sont réclamées, notamment l'identifiant, le mot de passe et/ou le numéro de carte bancaire.

Avec ces informations, le fraudeur peut agir de différentes façons :

- Retirer une nouvelle carte SIM dans une borne. En possession de la carte SIM, le fraudeur peut alors effectuer des communications depuis votre ligne ou contourner le principal dispositif de sécurité « 3D Secure ». Il récupère ainsi le code de sécurité envoyé par votre banque par SMS, pour effectuer une transaction financière depuis un site Internet. Il s'agit d'une « arnaque à la carte SIM »
- Récupérer le contrôle de votre adresse mail et envoyer à vos contacts un message de détresse pour l'achat de coupons PCS Mastercard ou Transcash.
- Commander un téléphone ou souscrire sur Internet un abonnement à votre nom avec vos identifiants.

Quels sont les bons réflexes pour se protéger du Phishing ?

- Prendre en compte les conseils qui figurent sur le site de votre opérateur,
- l'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message, et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;
- S'assurer que l'adresse du site (son URL) est bien l'adresse habituelle de l'interlocuteur ou l'organisme concerné,
- Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence (fig 2);

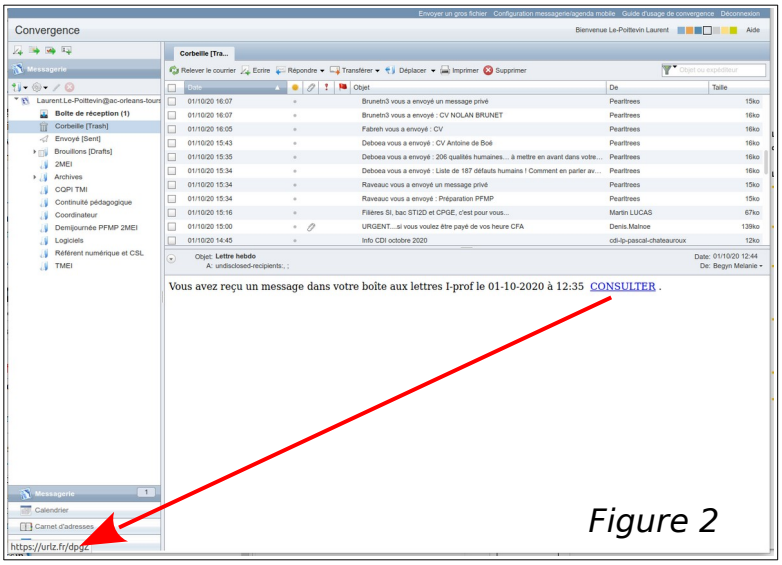

Figure 2

- Privilégier la saisie d'informations personnelles (coordonnées bancaires, identifiants, ..) sur des sites internet sécurisés .

Figure 3: Même si cela n'est pas une manière certaine de s'en assurer, depuis quelques années les navigateurs vous aident à déterminer si le site est sûr.

- Adopter la règle d'or de ne jamais communiquer vos informations personnelles (code secret, coordonnées bancaires..) à qui que ce soit,
- Changer régulièrement de mots de passe qui doivent être suffisamment complexes,
- S'assurer que votre antivirus est mis à jour régulièrement,
- Ne pas cliquer sur les liens contenus dans les courriers électroniques,
- Utiliser les fonctionnalités de protection contre l'hameçonnage et les logiciels malveillants proposés par les navigateurs internet,
- Installer un logiciel de filtre antispam – un filtre antispam est intégré au serveur ac-orleans-tours, mais vous pouvez en ajouter un sur un logiciel client tel que Mozilla Thunderbird avec le plug-in spamassassin,
- Rester vigilant lorsqu'un courriel demande des actions urgentes,
- En cas de doute, prendre contact immédiatement avec votre agence bancaire ou votre opérateur.
- N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts;
- N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.
- Par principe, les centres des impôts, les organismes sociaux (CAF, mutuelles, etc..), les banques ou les opérateurs ne demandent jamais, par courriel, de renseigner des données personnelles.

Pour en savoir plus
Site de la CNIL (Commission Nationale de l'Informatique et des Libertés) : https://www.cnil.fr
Site de la DGCCRF : fiche pratique sur le phishing https://www.economie.gouv.fr
Site d'information et d'assistance du gouvernement sur la cybermalveillance https://www.cybermalveillance.gouv.fr (vidéos pédagogiques disponibles pour alerter les particuliers, notamment sur les risques de phishing).