Prévention des arnaques sur INTERNET

Les malfaiteurs profitent de ces nouveaux outils pour mettre en place des dispositifs frauduleux de plus en plus sournois. Le principe du phishing consiste à récupérer des données personnelles de manière détournée. Tout ce qui vient d'internet n'est pas forcément vrai ! Nous vous aidons à reconnaître les situations à risque.

évitez les pièges des escrocs du web

Qu'est-ce que le phishing ?

Phishing est un terme anglais qui signifie **hameçonnage ou filoutage**. C'est la contraction des deux mots « phreaking » qui évoque le piratage des lignes téléphoniques et « fishing » qui veut dire pêche. Cette technique consiste à envoyer un **mail frauduleux** à un individu, en lui **faisant croire que ce courriel provient d'une institution, d'un établissement bancaire, d'un service de courrier électronique, d'une grande société, d'un site de vente aux enchères ou encore d'une entreprise de commerce en ligne.**

Par le biais de ce mail, le pirate **vous invite à cliquer sur un lien hypertexte pour vous connecter**. De ce fait, vous accédez à une page factice créée par le hacker où **il vous sera demandé vos données personnelles comme votre identifiant et votre mot de passe, ou encore**

votre numéro de compte bancaire. Une fois ces informations entre ses mains, il pourra les exploiter pour virer, par exemple, de l'argent à partir de votre compte bancaire vers le sien ou encore vendre les données qu'il aura collecté frauduleusement.

Comment se protéger du phishing ?

Voici quelques conseils pour éviter de tomber dans le piège de cette arnaque par mail.

• Dès que vous recevez ce genre de courriel provenant d'un site d'e-commerce ou d'une banque, vous devez vous demander tout de suite si vous avez effectivement communiqué votre adresse de messagerie à cet établissement.
Si la réponse est négative, vous pouvez être sûr qu'il s'agit d'une **tentative de phishing**. Dans l'affirmative, vérifiez si le mail indique des éléments qui pourraient vous aider à l'authentifier, comme le nom de l'agence ou le numéro de client. Si le courriel émane réellement de l'entreprise concernée, il contiendra certainement ce type de renseignements.

Bon à savoir : il est quasiment impossible qu'une banque, comme tout autre organisme officiel, demande des informations confidentielles et importantes dans un courrier électronique. En cas de doute, la meilleure solution est d'appeler directement votre agence par téléphone.

• Voici un autre indice qui devrait vous mettre la puce à l'oreille : la plupart du temps, ces messages sont rédigés par des pirates qui **maîtrisent mal les subtilités de la langue française**. Il est donc très probable que le courriel soit truffé de **fautes d'orthographe, de ponctuation, de tournure ou de syntaxe** .

• Pensez également à passer le curseur de votre souris sur le lien hypertexte, SANS CLIQUER. L'adresse va immédiatement apparaître et si le nom de domaine vous est inconnu, méfiez-vous, c'est une arnaque.

Bon à savoir : si votre ordinateur est équipé d'un firewall, il existe de grandes chances pour que le mail frauduleux soit considéré comme un **spam** et sera donc bloqué, car **indésirable**. Mais s'il parvient à se faufiler entre les mailles du filet, évitez de cliquer directement sur le lien. Copiez-le sur un nouvel onglet. Au moment de saisir vos données personnelles, vérifiez que le navigateur est bien en mode sécurisé (présence d'un petit cadenas sur la barre d'état et barre de navigateur commençant par https).

Si vous pensez avoir été victime d'une escroquerie, signalez-le aux autorités compétentes via la

plateforme « Pharos ». L'office central de lutte contre la criminalité et de la communication (OCLCTIC) se chargera de traiter votre signalement, en cas de contenu illicite.