Sécurité et arnaques sur internet et les réseaux

Quelques conseils pour utiliser internet en sécurité

- Avoir un antivirus sur son ordinateur et faire les mises à jour de sécurité
- Protéger vos accès avec des mots de passe solides
- Utiliser de préférence un navigateur sécurisé Firefox, Opéra, Brave, Iridium… éviter Edge ou Chrome
- Acheter sur des sites connus ou référencés de préférence français en vérifiant bien leur adresse car il y des copies !
- Les paiements actuellement doivent toujours être faits au moyen d'une authentification forte ou double authentification
- Eviter les réseaux publics wifi publics ou inconnus mal sécurisés

Les arnaques par email

- L’hameçonnage ou phishing via le message électronique est la première menace pour les entreprises comme pour les particuliers. Elle repose essentiellement sur l’usurpation d’identité. En effet, les arnaqueurs se font passer pour une entité respectée avec une bonne visibilité et une excellente réputation (banques, administration, opérateur de téléphonie, etc…).
- Les escrocs du filoutage peuvent donc récupérer vos noms, prénoms, adresses postales ou virtuelles, numéros de téléphone, RIB, numéros de carte bancaire, mots de passe et nom d’utilisateur pour différents sites. … Les arnaqueurs volent ces données pour les revendre sur le marché noir ou encore pour une attaque directe comme le piratage de compte en ligne ou bancaire, l’usurpation d’identité.

Le contenu du mail

- Le plus souvent, le cybercriminel se fait passer pour un tiers de confiance, provoque un comportement d'inquiétude chez le destinataire afin de l'amener à cliquer sur un lien le renvoyant sur un faux site.
- Le mail peut être à connotation « alarmiste » tel qu'une demande de mise à jour ou de confirmation de données personnelles, une demande d'informations pour l'envoi d'un cadeau ou d'un appel aux dons. Le mail peut aussi avoir un contenu « alléchant » faisant croire au destinataire qu'il pourrait gagner un cadeau ou faire une bonne affaire. Pour en bénéficier cependant, il devra donner ses coordonnées personnelles et le plus souvent des informations bancaires.
- Le lien redirige vers un faux site qui peut utiliser frauduleusement le logo ou le nom d'une marque ou d'une entreprise et qui ne dispose pas du protocole de sécurité HTTPS à gauche de l'adresse du site.

L’adresse email frauduleuse

- L’adresse email peut fournir de bons indices permettant de confondre un email douteux. Il se compose généralement comme suit pour un particulier : identifiant + @ +nom de domaine. Certains noms de domaine sont gratuits comme gmail, yahoo, orange, laposte, hotmail, gmx….
- Une entreprise sérieuse n’utilise jamais une adresse email gratuite pour des raisons de sécurité. L’apparence d’une adresse email fiable devra généralement comprendre l’URL du site web de l’entreprise.
- Le corps d’un mail douteux peut comporter des fautes d’orthographes ou de syntaxes ainsi que des maladresses linguistiques. Il faut également faire attention à l’adresse de messagerie de l’expéditeur. Très souvent, le lien vers le faux site n’est pas le lien officiel de l’entreprise.

Les « Scams »

- Le « scam » abréviation de scamming en Anglais qui signifie escroquerie. C'est la fraude qui consiste à abuser de la crédulité des destinataires pour leur soutirer de l'argent.
- Une personne se présente dans le courrier se faisant passer pour un riche héritier vous promettant la fortune d'un proche ou d'un millionnaire décédé ou encore d'un homme d'affaires qui affirme disposer d'une forte somme d'argent. Il vous propose une combine alléchante vous demandant de lui prêter votre compte bancaire pour effectuer des transferts d'argent moyennant une commission importante.
- Les arnaqueurs n'hésitent pas à demander les coordonnées bancaires ou encore à demander l'envoi de petites sommes, insignifiantes, qui sont censées payer des frais de traitement de dossiers ou des frais administratifs imaginaires. Il s'agit généralement de modestes sommes qui n'éveilleront pas vos soupçons. Les victimes doivent envoyer des informations détaillées les concernant (passeport, données de comptes, etc…) pour soi-disant, récupérer des « fonds bloqués » sur des comptes bancaires.

Les arnaques par SMS

- Les SMS frauduleux qui arrivent sur votre téléphone ont le même objectif : vous inciter à cliquer sur un lien dirigeant vers un site pirate afin de récupérer vos informations personnelles ou professionnelles, comme vos mots de passe ou vos données bancaires.
- Cette fraude est appelé smishing pour les sms frauduleux. C’est ce qu’on appelle en français « l’hameçonnage ».
- Le point commun de ces SMS frauduleux c'est qu'ils sont toujours expédiés depuis un numéro de mobile.

Exemples d’arnaques par sms

- L’arnaque à la contravention. Les escrocs jouent sur la peur des poursuites en cas de non paiement d'une contravention en se faisant passer pour ANTAI, l'Agence nationale de traitement automatisé des infractions.
- L’arnaque à la livraison Chronopost ou autre société de livraison, parfois il faut payer une petite somme 1 ou 2 euros.
- L’arnaque à la vignette Crit’Air
- L’arnaque à la carte vitale : mise à jour, renouvellement…
- L’arnaque au compte formation
- L’arnaque au compte bancaire : compte qui va être fermé, opération en attente, compte Nickel…
- L’arnaque à une loterie ou concours
- L’arnaque à la demande d’aide d’un proche ou d’un ami..
- L’arnaque au remboursement : impôts, EDF…
- L’arnaque à la gendarmerie ou procureur de de la république
- Et bien d’autres encore….

Comment identifier un faux message texte

- Le message n’a aucune pertinence pour vous : le message semble complètement inattendu et n’est pas lié à une activité que vous avez récemment entreprise.
- Le message transmet un sentiment d’urgence : le message vous incite à agir rapidement pour éviter un certain type de sanction ou une fermeture de compte.
- Le message provient d’un numéro de téléphone inconnu : Le message provient d’un numéro de téléphone que vous ne reconnaissez pas ou d’un numéro de téléphone composé de cinq à six chiffres au lieu de 10.
- Le message contient des fautes d’orthographe et (ou) est parfois mal rédigé.
- Le message contient un lien suspect :
- *"Nous avons essayé de livrer votre colis LP83693627378FR, mais il n'y a aucun affranchissement. Suivez les instructions ici : https://bit.ly/eb8UH"*

Conseils pour effectuer un paiement sécurisé sur internet

Achetez sur un site de confiance

- Tout d'abord, le plus logique : n'achetez pas sur un site internet douteux. Préférez les sites internet connus et n'hésitez pas à consulter les pages « qui sommes-nous », « conditions de vente », « mentions légales » et autres.
- Si vous ne connaissez pas le site internet, renseignez-vous à l'avance sur des forums par exemple.
- Vous pouvez aussi vérifier la fiabilité du site sur ***https://franceverif.fr/*** ***ou https://fr.scamdoc.com/***

Assurez-vous que la page est sécurisée

- Ensuite, lorsque vous êtes prêt à acheter, assurez-vous que la page où vous allez entrer vos coordonnées bancaires est sécurisée. Pour cela, regardez au début de l'URL : vous devriez lire **« https »** au lieu du classique « http ». Cela signifie que la page cryptera vos données et vous assurera un paiement sécurisé. Juste avant l'adresse du site devrait également s'afficher une icône de cadenas. 🔒

Ne cochez pas l’option « mémoriser »

- Sur de nombreux sites marchands, lorsque vous entrerez vos informations bancaires, une petite case sera cochée : « mémoriser mes données ». Décochez-la de suite. Cela vous permettra d’éviter que vos coordonnées privées soient stockées quelque part et donc accessible par des personnes mal intentionnées.

Conservez vos factures et surveillez vos comptes

- Enfin, un conseil plutôt logique : surveillez toujours vos comptes, fréquemment. Gardez vos factures et preuves de paiement en lieu sûr. Cela vous permettra tout d'abord de faire une quelconque réclamation, un échange ou un remboursement de manière plus aisée. Et puis cela vous permettra de vérifier régulièrement si les retraits effectués sur votre compte en banque correspondent. En cas de doute, consultez votre banquier **immédiatement** afin d'en savoir un peu plus.

Paiement sécurisé sur internet

L’e-carte bleue

- La e-carte bleue repose sur un logiciel vous fournissant des numéros de carte bleue à usage unique afin d’effectuer vos achats sur internet. En fait, tout passe par votre banque. Votre compte bancaire est lié à cette « e-carte bleue », mais vous n’aurez pas à entrer vos véritables coordonnées bancaires.
- Vous aurez besoin de vous créer un compte de e-carte bleue ainsi qu’un identifiant et mot de passe pour vous connecter à la plateforme e-carte bleue de votre banque. Puis, chaque fois que vous souhaiterez effectuer un achat, vous n’aurez qu’à sélectionner l’option « paiement par e-carte bleue », puis aller sur la plateforme e-carte bleu de votre banque en parallèle. Entrez ensuite vos identifiants et mot de passe, puis le montant de l’achat désiré.

PayPal

- PayPal est un service permettant de payer et de recevoir de l'argent sans fournir ses coordonnées bancaire. PayPal nécessite la création d'un compte client, qui sera relié à votre compte en banque. Quand vous effectuez un paiement sécurisé sur internet, vous n'aurez qu'à sélectionner l'option PayPal lors du paiement sur le site marchand. Vous vous connecterez ainsi à PayPal grâce à votre identifiant et votre mot de passe, et c'est tout. Le paiement sera ainsi géré par PayPal.
- Ces solutions de paiement en ligne nécessitent une adresse email et un numéro de carte bancaire (vous le communiquez uniquement à PayPal lors de l'inscription).
- L'utilisation de PayPal est très facile une fois que votre compte est créé. Vous n'aurez plus à entrer aucun numéro de carte bleue, et c'est assez pratique et rapide.
- Le seul point négatif est que PayPal est malheureusement assez souvent victime de phishing. Il s'agit d'une méthode de piratage de données par usurpation d'identité. Cela prend notamment la forme d'e-mails vous invitant à confirmer vos coordonnées bancaires.

Paylib

- Paylib est basé sur à peu près le même principe que PayPal. Il s'agit d'un système de paiement sécurisé sur internet, se faisant via votre compte Paylib. Paylib est une option offerte par une multitude de banques, et qui fonctionne avec les différents partenaires de Paylib.
- Vous n'aurez plus à vous préoccuper d'entrer vos coordonnées bancaires sur internet, puisque vous n'aurez qu'à vous identifier via Paylib pour effectuer tout paiement sécurisé sur internet. En cas de doute ou souci, vous pourrez directement contacter votre banque, et que l'option Paylib vous offre les même garanties et assurances que celles pour votre carte bancaire.
- Paylib est disponible via certaines banques partenaires (BNP Paribas, la Société Générale, La Banque Postale, Boursorama…) Et c'est via votre compte dans l'une de ces banques que vous pourrez créer un compte Paylib et utiliser cette option.

Que faire si vous êtes victime d'une escroquerie en ligne ?

- Vous pouvez transférer le message au numéro 33 700, la plateforme de signalement des spams vocaux et SMS.
- Signalez les escroqueries auprès du site *internet-signalement.gouv.fr*, la plateforme de l'Office central de lutte contre la criminalité liée aux technologies de l'Information et de la communication.
- Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : vous pouvez contacter Info Escroqueries au 0 805 805 817 (appel gratuit depuis la France) du lundi au vendredi de 9h à 18h30.
- Rendez-vous sur cybermalveillance.gouv.fr, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Elle procure des informations sur les menaces numériques et les moyens de s'en protéger.