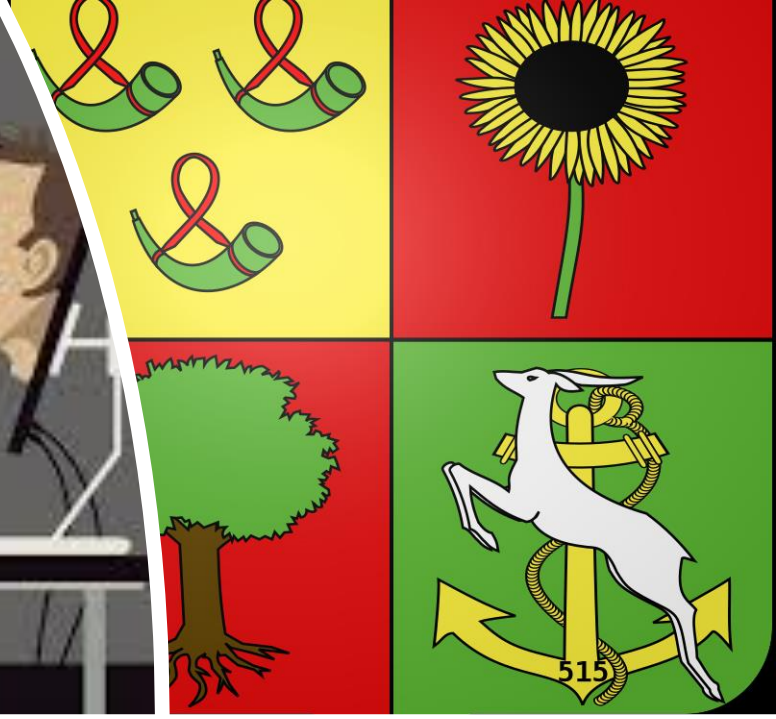
L'internet est un outil formidable. Sachons nous en servir.



Les arnaques classique de l’Internet

Les emails frauduleux : Les détecter, s’en défendre

Section Informatique, BLC, Brie

Pourquoi sommes nous ici ce soir ?

POURQUOI ?

Curiosité ? Inquiétude ? Regrets ?
Prudence ? Amusement ?

Objectif

Permettre à tous, quelque soit son niveau, de comprendre certains des dangers de l'internet.

COMMENT ?

Exemples
Interactivité
Questions Réponses

La créativité des arnaqueurs a toujours été leur force.
Comment s'en défendre ?

Comprendre les grands types d'arnaques

- **Le vol d'identité : (Le plus fréquent)**

Objectif : Usurper votre identité.
Méthode : Vous recevez un email vous demandant de vous connecter sur votre compte . Ce lien vous envoie sur un « site miroir ». Ou pièce jointe comportant un programme espion.
Type courant : Arnaque au colis, au message vocal, sécurité sociale, mutuelle, impôts, Paypal, …

➔Tant que vous n'avez pas vérifié le site ou vous croyez être, N'entrez pas vos identifiants de connection, et n'envoyez pas de copie de vos documents sur internet (carte d'identité, relevés de banque, passeport, etc.).

- **Arnaque à l'achat ou à la vente : (Courant)**

Sites cibles privilégiés : Les sites entre particuliers, comme eBay ou le bon coin.

En tant qu'acheteur, méfiez-vous des offres trop alléchantes et privilégiez le paiement en face à face.

En tant que vendeur : Méfiez-vous des clients qui exigent des moyens de paiement spécifiques (Attention le chèque de banque peut être falsifié), ou exigent de vous le paiement d'une somme d'argent pour "débloquer" leur paiement. N'envoyez votre objet que lorsque le paiement est clairement visible sur votre compte en banque. Attention aux chèques venant de l'étranger : Durée de compensation plus longue.

- **Arnaque à l'héritage , à la loterie: (Fréquent)**

Vous recevez un email vous annonçant que vous avez hérité, ou gagné à la loterie.

Ils réclament néanmoins que vous dépensiez une certaine somme pour couvrir des frais imaginaires.

N'envoyez jamais d'argent à quelqu'un qui vous aurait contacté sur internet, et ce pour quelque raison que ce soit !

Comprendre les grands types d'arnaques

- **Arnaque à la confiance , au sentiment (Très fréquent)**

Un ami , une personne proche vous contacte par email, et a besoin de votre d'aide de toute urgence. Naturellement, vous ne pouvez la joindre que par email. L'objectif est de vous soutirer de l'argent. N'envoyez jamais d'argent sans vous être assuré de l'identité de la personne.

- **Arnaque à l'emploi**

L'objectif est de vous faire payer des frais pour obtenir un emploi. L'email est alléchant, et vous allez enfin pouvoir travailler et gagner de l'argent . Il faut aller sur un site et à un moment , il vous sera demandé des frais couvrant des démarches imaginaires ….

- **Arnaque site de rencontre :**

Certaines escroqueries internet se déroulent sur les sites de rencontre. Bien souvent, l'escroc se fait passer pour une personne à la recherche de l'amour. Ce type d'arnaque implique souvent des scénario dramatiques, dans lesquels l'escroc finit par demander des sommes d'argent à la victime, pour X raisons (payer une rançon, payer le passeport, payer billet de train, des frais médicaux, etc). N'envoyez jamais d'argent à une personne rencontrée sur un site de rencontre, même si vous dialoguez ensemble depuis des semaines.

Comprendre les grands types d'arnaques

- **Arnaque au chantage :**

L'escroc cherche souvent à bien vous connaître, vous et votre entourage, notamment grâce aux réseaux sociaux. Il vous pousse à vous mettre dans une situation embarrassante, par exemple via une discussion webcam ou en exigeant des photos osées de vous. Puis, l'escroc menace de dévoiler les photos/vidéos/discussions embarrassantes à vos proches si vous ne lui envoyez pas une somme d'argent.

- **Arnaque téléphonique**

Un moyen d'obtenir des informations privées de plus en plus fréquent « catégorie arnaque sociale ». Ne Jamais donner d'identifiants, de mot de passe, de code de carte bleue par téléphone. Proposez de les rappeler.

Abrite aussi une forme de plus en plus répandue de tentative de vente forcée, d'escroquerie en tous genres. Peut devenir une gène terrible.

- **Et les autres**

L'inventivité des escrocs est leur fonds de commerce. De nouveaux types apparaissent régulièrement, d'autant plus que les arnaques se sont de plus en plus industrialisées.

D'un autre coté les outils de défense, antivirus, sécurité des logiciels, amélioration des mécanismes d'authentification s'améliorent tous les jours. Ex : validation a deux étapes pour paiement sur internet (Site Web + Code sur mobile). Ou e-carte bleue à usage unique.

Ne pas oublier qu'Internet apporte une richesse incroyable de services dont nous profitons tous.➔ Internet, Oui, avec circonspection.

Trois exemples …

de	"Portait D'assuré Vitale" <contact@bromaniasaqs.com>
à	Lucien.mart@orange.fr
date	31/07/18 05:48
objet	**Bénéficier De Votre Nouvelle Carte Vitale v3 Dès Maintenant !!**

Service-Public.fr
Le site officiel de l'administration française

Bonjour,

le service public, a enfin dévoilé sa nouvelle carte vitale V3. La nouvelle carte vitale bénéficie des dernières avancées technologiques en matière de sécurité , Fiable, pratique et sûre, votre carte Vitale est à présenter à tous les professionnels de santé. Plus de feuille de soins à envoyer, plus de vignette à coller, elle vous garantit le remboursement de vos soins sous 24h.

COMMENT OBTENIR VOTRE NOUVELLE CARTE VITALE V3?

C'est très simple à réaliser remplir le formulaire ci-dessous et cela ne vous prendra qu'une minute.

INSCRIVEZ-VOUS EN LIGNE ?

Vous recevrez votre nouvelle carte Vitale V3 sous 24h

Vous avez mis ce matin un meuble sur le bon coin, et vous recevez un SMS

19h42 : SMS du 06 xx xx xx x4
Bjr. Vos meubles postés en vente sur leboncoin sont toujours disponibles ? Si oui , donnez moi plus d'infos sur l'état actuel et prix final. Afin de mieux échanger, me joindre directement par mail à aymode2900@gmail.com. Cordialement M.Berdal

Alain , un bon camarade vient de vous envoyer un email

Bonjour,

Comment vas-tu? Pouvons-nous échanger par mail ?

En ce qui me concerne, le moral n'est pas au beau fixe, des soucis de santé avec le téI hors-service . . .

Puis-je te demander un service ?

PS : Je souhaiterais également que cela reste entre-nous stp ? !

Alain

La base du mécanisme : Vous faire agir.

- L’hameçonnage (Phishing), c’est quoi ?
- Les techniques de l’hameçonnage
- Comment les détecter :
  - Notions générales
  - Deux notions de base : Adresse Internet ; Adresse email
  - Application sur des exemples d’hameçonnage
- Quelques sites utiles
- Quelques suggestions de sécurité

L'Hameçonnage (Phishing)

L'hameçonnage est une pratique internet très courante, consistant à provoquer votre réaction : (le poisson qui mord l'appât) : Aller sur un site Web, Ouvrir une pièce jointe, Envoyer de l'argent, ..

Ex : Vous recevez un e-mail, un SMS, un coup de fil, dans lesquels l'émetteur se fait passer pour un organisme reconnu (EDF, PayPal, Banque, la police, un site marchand bien connu , etc.) et vous demande de cliquer sur un lien vous connecter à votre espace personnel pour corriger une erreur, ou d'ouvrir une pièce jointe.

Le lien pointe sur un site miroir : Site qui imite (parfois à la perfection) le site officiel , mais à en fait été créé par des escrocs. Si vous y entrez vos données, les escrocs vont les recevoir et les réutiliser immédiatement.
La pièce jointe peut contenir un virus, un logiciel malveillant, un adware (*)

* Un adware est un logiciel permettant à son éditeur de générer des revenus publicitaires et qui est le plus souvent installé à l'insu de l'Internaute.

Techniques de l'hameçonnage

- **Le message** reçu joue le plus souvent sur :

  Une information de gain (L'appât), Une information de remboursement. (L'intérêt)

  La vérification de sécurité (Vérifier vos coordonnées bancaires , modification de votre mot de passe , …)

  L'empathie (Une personne a besoin d'aide),

  L'urgence (Votre électricité sera coupée si vous ne réagissez pas très vite),

  L'indignation (On vous informe qu'une somme indue va être prélevée sur votre compte)

  La peur de perdre (Prélèvement d'une somme supérieure à ce que vous devez)

  La peur (Vous risquez d'être poursuivi si vous ne payez pas)

  L'obligation légale (Vous devez aider la police, vous mettre en conformité à la loi, email des impôts, …)

  Ou à l'opposé, Le truc totalement banal (vous avez reçu un message vocal, …)

Déclencher une émotion

Circonstances inhabituelles

- **Méthode** : Rien ne peut se faire sans votre aide ! L'escroc a besoin que :

  Vous ouvriez une pièce jointe

  Vous alliez sur un site Web miroir.

  Que vous le contactiez sur une adresse mail car son téléphone ne marche pas

➔ Règle d'or :

Tant que vous n'êtes pas sûr de QUI vous envoie un message, Ne JAMAIS ouvrir une pièce jointe ou cliquer sur un des liens du message (que ce soit sur le PC ou sur le portable)

➔ La règle est simple et belle, mais COMMENT vérifier ?

Comment savoir si un message est authentique ?

Deux notions sont nécessaires :

Structure d’une adresse de messagerie électronique.

Structure d’une adresse internet.

Structure d'une adresse email.

Source : Wikipedia

jean.dupond@orange.fr contact-client@laredoute.com
patrick.dejean@macif.fr helen32@gmail.fr
ne-pas-repondre@dgfip.finances.gouv.fr

Une adresse email est constituée des trois éléments suivants, dans cet ordre :

- une *partie locale*, identifiant généralement une personne (lucas, Jean.Dupont, joe123) ou un nom de service (info, vente, postmaster) . jean.dupond@orange.fr
- le caractère séparateur @ (arobase), signifiant *at* en anglais ; jean.dupond@orange.fr
- Le nom du serveur de messagerie de l'émetteur : jean.dupond@orange.fr

- Il est essentiel de différencier les types d'adresses de messagerie, identifiées à partir du nom du serveur de messagerie
  - Adresses gratuites (gmail.com, outlook.fr, yahoo.mail , free.fr, ..) ➔ Jamais utilisés par les entreprises et services publics !
  - Adresses privées (laposte.net, orange.fr, …)
  - Adresses professionnelles (edf.fr , cnav.fr , monabank.com , priceminister.com, …)

Vérifier l'adresse de l'émetteur du message

- Par défaut, les outils vous affichent le nom de l'émetteur, pas son adresse mail.
- Il faut bien comprendre la différence entre le nom affiché et l'adresse mail de l'émetteur (visible en passant la souris sur le nom affiché)
  - Nom Affiché : Agricole Service Plus
  - Adresse émetteur : michel-dejean@orange.fr

- Comment voir l'adresse réelle ?

  Cela dépend de l'outil utilisé pour lire le message

  - Sur certains webmail (*) : l'adresse est automatiquement affichée (Dépend du fournisseur de messagerie).
  - Sur d'autre, il faut passer votre souris sur le nom de l'émetteur du message, un pop up vous donnera l'adresse réelle.
  - Sur Iphone : Il faut cliquer sur le nom de l'émetteur du message

Cohérence : Le nom affiché est-il en lien avec l'adresse de l'émetteur ?

Si non, probablement mail malveillant

Si oui, vérifiez les points suivants

Cohérence : L'adresse de l'émetteur est-elle cohérente par rapport au message ?

Si vous recevez un message de « La Redoute », l'email vient-il du domaine « La Redoute » ?

Si vous recevez un message de votre notaire, l'email vient-il du domaine « notaires.fr » ?

Question : Le message est-il personnel ou générique ?

* webmail : Page Web pour lire vos mails

Exemple!

de	"Portait D'assuré Vitale" <contact@bromaniasaqs.com>
à	Lucien.mart@orange.fr
date	31/07/18 05:48
objet	**Bénéficier De Votre Nouvelle Carte Vitale v3 Dès Maintenant !!**

Service-Public.fr
Le site officiel de l'administration française

Bonjour,

le service public, a enfin dévoilé sa nouvelle carte vitale V3. La nouvelle carte vitale bénéficie des dernières avancées technologiques en matière de sécurité , Fiable, pratique et sûre, votre carte Vitale est à présenter à tous les professionnels de santé. Plus de feuille de soins à envoyer, plus de vignette à coller, elle vous garantit le remboursement de vos soins sous 24h.

COMMENT OBTENIR VOTRE NOUVELLE CARTE VITALE V3?

C'est très simple à réaliser remplir le formulaire ci-dessous et cela ne vous prendra qu'une minute.

INSCRIVEZ-VOUS EN LIGNE ?

Vous recevrez votre nouvelle carte Vitale V3 sous 24h

- Adresse émetteur :

"Portait D'assuré Vitale"
contact@bromaniasaqs.com

➔Le nom affiché n'est pas en lien avec l'adresse de l'émetteur !

➔Message non personnel !

Soyez aussi vigilants vis-à-vis des adresses connues

Un escroc peut utiliser une adresse email ressemblant à la véritable adresse d'un de vos proches

- Par changement d'une lettre
  - Ex : jean.duchemin@laposte.net va devenir jean-duchemin@laposte.net
- Par permutation d'une lettre
  - Ex : jean.duchemin@laposte.net va devenir jaen.duchemin@laposte.net
- Par oubli d'une lettre
  - Ex : jean.duchemin@laposte.net va devenir jean.duchemn@laposte.net
- Par pointage sur un autre domaine
  - Ex : jean.duchemin@laposte.net va devenir jean.duchemin@maposte.fr
- Par affichage de la bonne adresse, mais la réponse se fera sur une autre.
  - En cliquant sur répondre, vous verrez la véritable adresse email.
- Par hacking de la boite : utilisation de la véritable adresse
  - La boite mail a été piratée (700 Millions d'adresses emails piratées 01 Sept 2017)

Savoir lire une adresse Internet

Vérifier une adresse courte :
https://checkshorturl.com/expand.php

- Une **adresse Internet** se compose souvent d'un préfixe "www" (World Wide Web – sous domaine) suivi d'un nom de domaine. Ce nom de domaine est lui-même composé d'une chaîne de caractères et d'une extension. Viennent ensuite des informations internes au site web.

https: //www.secours-catholique.org/ https: //fr.unesco.org/priorityafrica https://www.impots.gouv.fr/portail/particulier

https://www.bdangouleme.com/palmares-2020 https://www.ameli.fr/ https://www.ameli.fr/charente/

WWW.Nom de domaine : **Unique au monde .**
Un nom de domaine doit être acheté auprès d'une organisation nationale sous le contrôle d'une organisation supra nationale.

Extension : caractérise le type de domaine (à l'origine)

.com Organisations commerciales
.edu Éducation
.gov et .gouv Gouvernement
.net Networks (réseau)
.org Organisations à but non lucratif
.fr 2 lettres identifiant le pays (DE : Allemagne, UK, Angleterre, …)

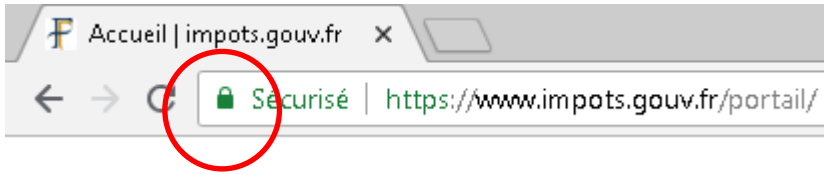
Protocole : HTTP : Hyper Text Transfer Protocol -- HTTPS : HTTP Sécurisé

http : non sécurisé (le site n'est pas vérifié et l'échange est en clair) ➔ Site accédé en clair, donc aucune sécurité.
https : L'identité du serveur est validée via un certificat et les échanges sont cryptés ➔ Site normalement non dangereux car l'échange avec le site est crypté
A RETENIR : HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable

Affichage d’un site sécurisé : Signalé par un Cadenas

- Internet Explorer

- Chrome



- Firefox :

Click sur cadenas donne informations relatives à la sécurité de l’accès au site Web

Noms de domaine : L'écosystème des entreprises

- Les entreprises **achètent** leur nom de domaine, et ce nom sert généralement à héberger tous leurs sites . (Seules certaines micro entreprises ne le font pas)

- Exemple : Orange ➔ Nom de domaine : orange.fr
  - Espace client : https://espaceclientv3.orange.fr/
  - Messagerie : https://messagerie.orange.fr/
  - Boutique : https://boutique.orange.fr/
  - Portail : https://www.orange.fr/portail

Comment reconnaitre un lien ?

Passez votre souris dessus, sans cliquer, et le pointeur de souris deviendra quelque chose comme … 

Sur la plupart des navigateurs (Edge, Chrome, Firefox) l'adresse du lien s'affiche en bas à gauche de l'écran.

Exercice : passez votre souris sur les liens ci-dessous .

Ex : Un Lien … Autre Lien

Comment détecter si un site est sûr?

- Vérifier s'il est dans le domaine de l'entreprise qui vous contacte
  - S'il n'y est pas, alors 99% de chances que le site soit frauduleux.
  - Sauf cas exceptionnel dûment expliqué, une entreprise ne vous enverra jamais un email à partir d'une adresse email hors de son domaine, ni ne vous enverra sur un site dans un autre domaine.

- Vérifier s'il est en HTTPS
  - Rares sont les entreprises étant restées en HTTP.
  - S'il est en HTTP : Ne communiquez AUCUNE donnée personnelle, encore mois une info sensible. (HTTP : communication non cryptée)

- Si vous avez un doute, contactez l'entreprise émettrice par un autre moyen. (Recherche du site de l'entreprise, appel téléphonique)

➔Ne vous précipitez pas ! Dites-vous bien que si quelque chose est réellement important, les entreprises sauront vous joindre

➔Nota : il existe des plug-in a mettre sur les navigateurs pour qualifier la réputation des sites (ex : Web Of Trust sur Chrome)

Outils à votre disposition

- Le plus puissant : Votre bon sens
  - Soyez attentifs.
  - Vérifier les adresse émetteurs, et les liens.
  - Demandez l'avis de vos proches.
  - En cas de doute, abstenez vous.
- Vérifier sur Internet si le message est une arnaque ou un hoax (*).
  - Saisir le texte (sans cliquer sur le lien) , dans un moteur de recherche et regardez le résultat. Vous serez vite renseignés.
- Règle de base : Prenez votre temps
  - Les seuls urgences sont en contact direct. Il n'y a jamais d'urgence via une communication asynchrone. (Vous avez essayé de faire venir les pompiers en envoyant un mail ?)

* : **Hoax :**
Anglicisme informatique qui signifie "canulard, bobard, intox qui circule sur Internet". Il s'agit donc d'un mensonge créé de toutes pièces sur le web.

Arnaques téléphoniques

Voir le site Bloctel : http://www.bloctel.gouv.fr/
(De sérieux doutes quand à l'efficacité de cette mission gouvernementale.)

- Objectif :
  - Vous soutirer des données confidentielles ou vous vendre ce dont vous n'avez aucunement besoin
    - Message souvent très rapide se terminant par une question précise : Exemple
      - Bonjour c'est Valérie de la société Environnement vert, nous sommes missionnés par EDF pour vérifier comment votre maison est isolée. Alors quelle est la surface de votre logement …
    - Et c'est parti pour des questions/réponses avec quelqu'un que vous ne connaissez pas.
    - Moyen radical : proposez de répondre à leurs questions, mais quand vous les aurez rappelés.
  - Vous faire rappeler un numéro surtaxé
    - Cas typique : votre tel sonne, et quand vous décrochez, raccrochage immédiat. Ou message du genre :
      - « Pour prendre possession de votre colis, vous devez rappeler le numéro (089XXXXXXX). »
      - « Vous avez entrepris une démarche administrative : vous êtes invité à appeler le (089XXXXXXX), votre dossier est le 7733. »
      - « Gagnez un téléphone, un voyage : pour cela appelez le (089XXXXXXX). »
    - Vous rappelez et … vous payez car le numéro est surtaxé: Les numéros suivants sont surtaxés
      - les numéros à 10 chiffres commençant par 081 ou 082 ou 089 ;
      - les numéros à 4 chiffres commençant par 1 ou 3 ;
      - les numéros à 6 chiffres commençant par 118.
  - Vous vendre ce dont vous n'avez pas besoin.
    - Pour ma part, je demande une confirmation de leur offre par courrier. Ou pour ceux qui insistent trop, je passe en mode contre attaque.
- **Règle simple :**
  - Vérifiez l'identité de votre appelant – proposez de le rappeler.
  - Toujours vous demander mais pourquoi ces gens ont-ils besoin de connaitre cela
  - Ne jamais communiquer de données privées par téléphone. (et surtout pas un N° de CB)

Savoir, c’est commencer à se protéger : Continuez à vous renseigner

- De nombreux sites vous permettent de creuser le sujet avec des exemples. Prenez le temps d’y jeter un œil.

- Des sites donnant un certain nombre de types d’arnaques
  https://wiki.signal-arnaques.com/Accueil
  https://arnaqueinternet.com/
  https://www.arobase.org/arnaques
  https://www.signal-arnaques.com/
  Google : « hameçonnage »

- Un dernier, avec de très nombreux exemples d’emails frauduleux
  http://vadeker.net/reponses/arnaques/spammers_scammers_arnaques.html

Lutter contre : Pharos et ARCEP

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Pharos : Gendarmerie

- Plate forme Pharos : signalement en ligne de contenus illicites. Pédophilie, corruption de mineur, incitation à la haine raciale, provocation à la discrimination, menace ou incitation à la violence, trafic illicite, mise en danger des personnes mais aussi escroqueries et arnaques financières
- https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action
  - Les signalements sont traités par des policiers et des gendarmes rattachés à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire.
  - En 2018, 1 584 130 signalements traités depuis la création de Pharos, en 2009.
  - En moyenne, 4 395 signalements sont effectués par semaine, dont :
    - 57 % concerne des escroqueries
    - 11,2 % des atteintes aux mineurs
    - 7,7 % des discriminations.

arcep
autorité de régulation
des communications électroniques,
des postes et de la distribution de la presse

ARCEP : Autorité de régulation des telecoms https://jalerte.arcep.fr/home

Et si vous voulez en savoir plus ..

- Venez nous rejoindre à la section informatique de la BLC !

Arnaques Internet

Les détecter, s’en défendre

Bibliothèque, Groupe Informatique, Brie

Exemple de message frauduleux

De: "service@paypal.fr" <security@security.com>
Envoyé: 13/09/2008 18:57
A: mel.vadeker@caramail.com
Objet: Attention! Votre compte PayPal a ete limite!

PayPal

Chers PayPal,

Vous avez indique que vous avez oublie votre mot de passe PayPal.

Cliquez sur le lien ci-dessous pour verifier cette adresse e-mail et de creer un nouveau mot de passe:

Cliquez sur le lien pour verifier ton compte

Si vous n'avez pas demande ce message, s'il vous plaît nous contacter A l'adresse 08707 307 191.

Merci

Je vous prie d'agreer,
PayPal

Type de plus en plus courant et souvent magnifiquement réalisé. Tout semble vrai. (hormis fautes de Français)
Indicateurs :
==> Domaine émetteur : security.com (hosté par Amazon.com)
==> email anonyme : pas de nom de destinataire.
➔ Au fait, avez-vous vraiment demandé la réinitialisation de votre mot de passe paypal ?
==> L'analyse du lien permet d'éventer la supercherie : Il pointe sur un site miroir

L’arnaque à la vente

Un scénario :

- **Vous vendez un bien (ex: Téléphone portable) disons pour 200 € sur un site comme le bon coin.**
- **Quelqu’un vous contacte (de l’étranger) et pour réserver le bien, vous envoie un chèque couvrant largement le prix du bien, et le montant pour l’expédition, disons 1500 € dans notre exemple (parfois beaucoup plus).**
- **Vous recevez le chèque, vous l’encaissez et vous êtes satisfait de cette vente. Joie** ☺
- **Votre acheteur vous demande de lui expédier le bien et de rembourser rapidement le trop perçu par virement western union, ou coupon carte prépayée.**
- **Vous expédiez le bien (Frais expédition 150 €) et honnêtement, faites un virement western union du solde : (1500 – 200 – 150 = 1150 €).**
- **Perdu ! : Le chèque est dans une banque étrangère et sous trois à quatre semaines, il reviendra avec la mention « chèque non provisionné ». Vous paierez donc en plus des frais de chèque impayé.**

Une autre arnaque le bon coin, paiement par paypal expliquée.

- https://www.abcargent.com/arnaque-le-bon-coin-paypal/

Arnaque a la vente : Mon expérience

Vendredi 16h00, je publie quelques annonces sur le bon coin pour vendre du mobilier en prévision de mon déménagement.
Le texte donne un prix et stipule : « annonce en ligne ➔ produit disponible »
Le numéro de tel n'est pas visible directement sur l'annonce, il faut cliquer pour le voir.

19h42 : SMS du 06 xx xx xx 94
Bjr. Vos meubles postés en vente sur leboncoin sont toujours disponibles ? Si oui , donnez moi plus d'infos sur l'état actuel et prix final. Afin de mieux échanger, me joindre directement par mail à aymode00@gmail.com. Cordialement M.Berdal

20:06 : SMS de 21084
De blanc sophia
Bsr, votre Armoire est tjrs dispo ? Si oui me confirmé le prix ferme et me répondre a mon adresse mail perso : perot74@gmail.com

22:10 : SMS de : Noreply
De mes avigny
Bjrs, Votre offre (ameublement) est-elle toujours disponible a la vente?
Si oui me le faire savoir uniquement à mon adresse email : mmesavigny02@gmail.com

21:01 : SMS du 21087
De thomat sylvie
Bsr, votre Armoire est tjrs dispo ? Si oui me confirmé le prix ferme et me répondre a mon adresse mail perso : lagracefabienne@outlook.fr

L’arnaque classique à la confiance (dite Nigérianne)

- Vous recevez un premier email souvent reçu d’une personne **que vous connaissez bien**. Email envoyé souvent à partir d’une adresse email proche de la véritable adresse email de votre ami (ou boite mail piratée) .

> Bonjour,
>
> Comment vas-tu? Pouvons-nous échanger par mail ?
> En ce qui me concerne, le moral n'est pas au beau fixe, des soucis de (santé) avec le téI hors-service . . .
> Puis-je te demander un service ?
> PS : Je souhaiterais également que cela reste entre-nous stp ? !
>
> Alain

Ingrédients : Appel à l’aide + Téléphone hors service + Discrétion
Vous répondez un mail chaleureux, et cela ne rate pas !

Une réponse révélatrice

Je te remercie pour ta réponse,

Pour tout te dire … bla bla bla bla bla bla bla bla bla…. J'ai des soucis de santé... bla bla bla bla bla bla bla bla bla ..., ne t'inquiète pas s'il te plaît.

Mais je t'écris, car j'ai une sérieuse demande à te faire . bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla

J'ai du mal à trouver des TlCKETS (P .C.S Master card) bla bla bla bla bla bla bla bla bla . Ces recharges sont vendues chez les buralistes(TABAC) où dans les kiosques à journaux, j'en ai besoin maintenant,

J'ai s'il te plaît besoin de 10 TlCKETS P C S Masterd card de 250 € pour ma carte prépayée bla bla bla
Bla bla bla bla bla bla

NB: pour le remboursement joint moi ton RIB, je te fais un virement maintenant à l'instant.
Je t'appellerai dès que mon portable sera en service Je compte sur ta discrétion.
Merci pour ta confiance. J'attends ta réponse au plus vite.
Alain

Arnaque téléphonique : Infos utiles

- **Connaitre un peu plus en détail 3 arnaques classiques**
  - **L'arnaque à l'abonnement :**
    https://info.signal-arnaques.com/encyclopedie-des-arnaques/arnaque-a-labonnement-fictif/
  - **Le Ping Call :**
    https://www.prixtel.com/decouvrir-PRIXTEL/actualite/news/mefiez-vous-de-larnaque-a-lappel-en-absence-ou-ping-call/
  - **Le SMS Surtaxé :**
    https://www.prixtel.com/decouvrir-PRIXTEL/actualite/news/comment-eviter-le-piege-des-sms-surtaxes/
- **Connaitre le cout d'un numéro SVA (Service Valeur Ajouté) :**
  http://www.infosva.org/
- **Signaler un SPAM ou Message vocal indésirable (ou le transférer vers le N° 33700)**
  https://www.33700.fr/

Même si les SMS surtaxés sont facturés par votre opérateur mobile, toute contestation doit être faite à l'éditeur du service.
Votre opérateur n'a qu'un rôle d'intermédiaire et il n'est pas en mesure de distinguer les services auxquels vous avez souscrits des arnaques.
Pour ne plus recevoir de SMS de sa part, il suffit de répondre au SMS indésirable avec le mot **STOP**. Le fournisseur de service a alors l'obligation de ne plus vous envoyer de SMS.