- Carlos n'a plus accès à son compte, ce qui indique qu'il a probablement été piraté : le message reçu par Jeanne aurait donc été rédigé par un cybercriminel
- Ce message invite à cliquer sur un lien
- Le lien n'est pas clair et on ne sait pas sur quoi on va arriver

Réponses :

Situation

- Le numéro de téléphone de l'émetteur du SMS est un numéro de téléphone portable : il commence par 06, ce qui est inhabituel pour une société de livraison
- Le message incite à cliquer sur un lien
- Le message est vague et ne donne pas d'informations précises

Réponses :

Situation

- Le mail demande l'envoi d'une somme d'argent
- Le mail ne donne pas de détails, il n'y a pas de précision sur la nature du « souci»
- La rédaction du mail est maladroite et il y a des fautes d'orthographe pouvant être inhabituelles
- Le mail insiste sur l'urgence et un besoin de discrétion non justifié

Réponses :

Situation

- Une adresse mail d'origine suspecte
- Une mention du caractère obligatoire
- Une mention d'urgence sous peine d'une sanction
- Une incitation à cliquer sur un lien

Réponses :

Situation

Situation

Élise reçoit un mail d'un proche

Boîte de réception

De : jean.pattel@monmail.com

À : elise.pattel@monmail.com

Sujet : Besoin de ton aide !

Je suis en Espagne pour conclure une affaire importante. Malheureusement, j'ai eu un souci et n'ai plus de téléphone. Je te donerai plus de détail à mon retour.

J'aimerais s'il te plaît, que tu me vienne en aide en m'achetant au bureau de tabac 4 coupons de rechargement PCS de 250€ puis transmets moi les codes de chaque coupon. Je te rembourserais dés mon retour,

S'il te plait je comte sur ta discrétion,
Je reste dans l'attente de tes nouvelles,

Merci encore d'avance

Jean

Situation

Paula reçoit un mail bancaire

Boîte de réception

De : E-service Clients CG <CG_secure4.noreply@radiopwn.com

À : Paula@monmail.com

Sujet : Au sujet de la sécurité de votre compte !

SÉCURITÉ RENFORCÉE POUR CONSULTER VOS COMPTES EN LIGNE

Chère cliente, cher client,

Conformément à la loi PSD2 pour la sécurité des paiements en ligne et afin d'arrêter l'utilisation frauduleuse des cartes bancaires sur Internet, notre équipe est dotée d'un dispositif de contrôle des transactions.

Ce service est entièrement gratuit !

Remarque : cette opération est obligatoire et à faire sous 48H sous peine de suspension de votre compte.

ME CONNECTER

Situation

Carlos reçoit un SMS de Jeanne

JEANNE

Bonjour Carlos ! Tu m'as dit que tu n'arrivais plus à te connecter à ton profil Facebook, pourtant je viens de recevoir un message de toi sur Facebook qui me disait :

« Salut ! J'ai découvert une super playlist, va l'écouter ! https://bit.ly/2N9ez3X »

Tu as pu ré-accéder à ton compte ? C'est bien toi qui m'a envoyé ce message ?

Répondre

Situation

Khadija reçoit un SMS

+33 6 39 98 24 32

Chronopost :

L'acheminement de votre colis a rencontré une erreur.

Mettez à jour votre livraison via :

http://colis-chrnopost-online.com/

Répondre

Menace

L'hameçonnage (phishing) *dans la vraie vie*

Une personne vient sonner à la porte de la victime : elle se présente comme un agent spécialisé en placements financiers dont la société est certifiée par le ministère des Finances…

« Nous sommes mandatés pour vous proposer des investissements à hauts rendements et totalement déduits d'impôts. Si vous voulez en profiter, il faut rapidement constituer un dossier car ces mesures expirent la semaine prochaine ».

La victime fait entrer l'intéressé et après lui avoir signé un document dans lequel elle renseigne toutes ses informations bancaires, elle lui remet une grosse somme d'argent devant être placée.

Résultat : Elle a transmis tous ces éléments à un parfait inconnu qui lui a dérobé son argent et risque de réutiliser ses informations financières pour d'autres escroqueries !

Situation

Réponses :

- L'adresse du site ne correspond pas à l'adresse officielle du site des impôts
- Les impôts n'ont pas besoin de ce type d'informations : ils les ont déjà
- Un remboursement des impôts se fait par virement automatique sur votre compte

Situation

Réponses :

- L'ordinateur semble bloqué sur cet écran
- Le message est alarmant et insiste sur l'urgence de la situation
- Bertrand est incité à appeler un numéro inconnu

Situation

Réponses :

- L'application est un jeu mobile : le besoin d'avoir autant d'autorisations n'est pas justifié et est suspect
- L'application n'a pas été téléchargée sur un site officiel

Situation

Fatou croit envoyer des documents aux Impôts

impots.gouv

https://1pot.com/mon-compte

Site officielle des Impôts

Pour obtenir votre remboursement, veuillez fournir les documents suivants :

- Une copie de votre carte d'identité
  Déposez votre document ici
- Un justificatif de domicile
  Déposez votre document ici
- Votre dernier bulletin de paye
  Déposez votre document ici

Situation

Bertrand navigue sur Internet. Soudain, une fenêtre apparaît

**** ATTENTION ! ****

Votre ordinateur a été bloqué :
votre ordinateur nous a alerté, il a été infecté par un virus. Vos informations personnelles sont en train d'être volées ; vous devez nous contacter immédiatement pour recevoir de l'aide de notre équipe d'ingénieurs.

Appelez-nous dans moins de 5 min pour la réparation de votre ordinateur.

> 03 53 01 08 65 (appel gratuit)

OK

Menace

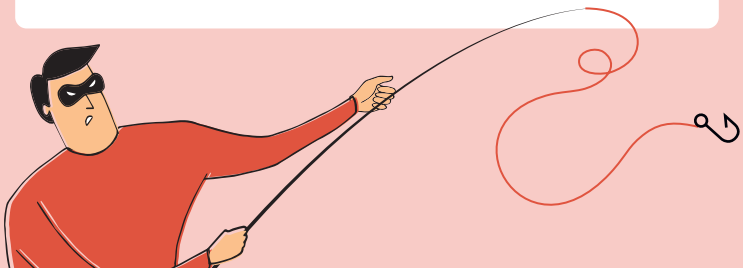
Hameçonnage (phishing)

Pourquoi ?

Voler des informations sensibles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

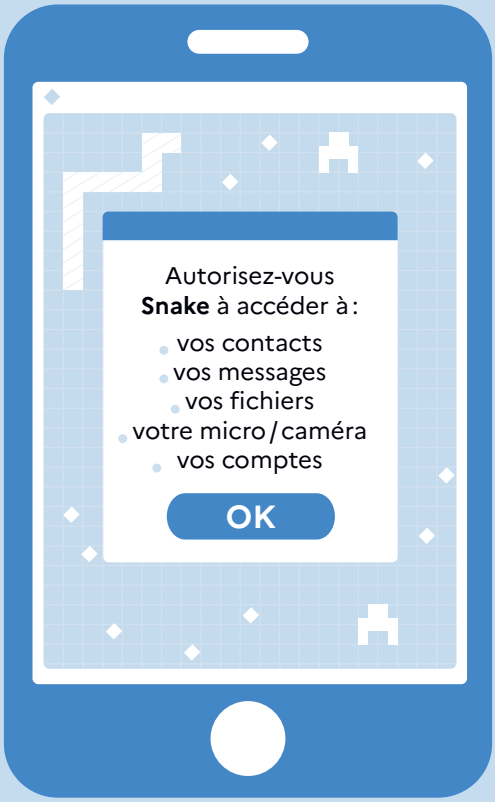
Comment ?

Faux message, SMS ou appel téléphonique d'un cybercriminel qui se fait passer pour une banque, un opérateur téléphonique, un site de commerce, un réseau social, une administration...



Situation

Helena a téléchargé un jeu mobile sur un site qu'elle ne connaît pas. Quand elle l'ouvre, une fenêtre apparaît



Un motocycliste gare sa moto devant chez lui pour déposer ses courses au lieu de la mettre dans son garage comme d'habitude. Un voisin avec lequel il est en conflit voit la moto et enfonce un clou sur le côté du pneu avant.

Après avoir rangé ses courses, la victime reprend sa moto pour aller au cinéma. Sur la route, lors d'un virage, le pneu éclate sous l'effet du clou.

Résultat : La victime perd le contrôle de son véhicule et se retrouve à l'hôpital aux soins intensifs.

Le virus informatique
dans la vraie vie

Menace

Alors qu'il gare sa voiture, un inconnu interpelle le conducteur : « Attention ! Au bruit que fait votre moteur, votre voiture doit avoir un énorme problème ! Si vous ne faite rien vous risquez de mettre votre vie en danger ! Laissez-moi regarder, je suis garagiste : je peux vous réparer votre voiture en urgence ».

Paniqué et n'y connaissant rien, le conducteur laisse la personne bricoler trente minutes dans son moteur. Celle-ci demandant à être payée pour cette réparation, il lui remet une somme conséquente.

Résultat : La victime a payé très cher une prestation infondée à ce soit-disant « garagiste », alors que sa voiture n'avait aucun problème !

L'arnaque au faux support technique
dans la vraie vie

Menace

La victime a remis un dossier complet à un escroc pour la location d'un appartement (copies de document d'identité, bulletins de salaire, avis d'imposition, justificatif de domicile…). L'escroc a utilisé ces documents pour usurper son identité et souscrire à des crédits à la consommation.

Résultat : Les banques font rembourser à la victime les crédits dont elle n'arrive pas à justifier l'origine. Elle se retrouve à découvert et interdite bancaire.

Le vol de données
dans la vraie vie

Menace

La victime possède une voiture qu'elle ne ferme jamais. Elle est stationnée devant chez elle et comme son quartier est tranquille, elle y laisse même les clés sous le siège conducteur.

Un soir, un inconnu s'empare du véhicule et après avoir grillé trois feux rouges renverse un cycliste avant de s'enfuir.

Résultat : les caméras de vidéoprotection ont bien filmé la scène et même si le visage du conducteur est flou, on relève l'immatriculation ! Devinez qui va devoir s'expliquer ?

Le piratage de compte *dans la vraie vie*

Menace

Menace

Vol de données

Pourquoi ?

Utiliser des informations personnelles dérobées (identité, mot de passe, données bancaires…) pour en faire un usage frauduleux.

Comment ?

Diverses techniques peuvent être employées pour dérober les données : hameçonnage, piratage de compte, infection par un virus…

Menace

Piratage de compte

Pourquoi ?

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux.

Comment ?

Prise de contrôle d'un ou plusieurs comptes en ligne, en raison d'un mot de passe trop simple, communiqué sans le savoir suite à un message frauduleux ou utilisé sur plusieurs sites dont l'un a été piraté.

Menace

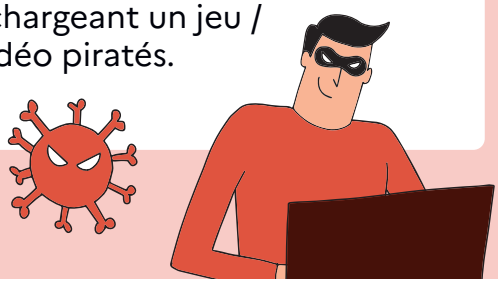
Virus informatique

Pourquoi ?

Perturber le fonctionnement d'un appareil ou porter atteinte à ses données : vol ou destruction d'informations (documents, mots de passe, messages) ; espionnage ; utilisation de l'appareil pour en attaquer d'autres.

Comment ?

Un appareil peut être infecté par diverses méthodes : en cliquant sur un lien ou une pièce jointe piégés ; en navigant sur un site malveillant ou en téléchargeant un jeu / logiciel / vidéo piratés.



Menace

Arnaque au faux support technique

Pourquoi ?

Inciter la victime à payer un pseudo-dépannage informatique et en profiter pour lui dérober ses informations personnelles et bancaires.

Comment ?

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement avec un écran qui paraît bloqué.

Risque

Exemple de vol de données d'identité :

Avec les documents d'identité dérobés, le cybercriminel peut ouvrir un compte bancaire à votre nom qui servira à des activités frauduleuses, souscrire un crédit que vous devrez rembourser, louer une voiture…

Risque

Exemple de vol de données bancaires :

Avec des données bancaires dérobées, le cybercriminel peut effectuer des virements ou réaliser des achats en ligne qui seront débités de votre compte bancaire.

Risque

Exemple de perte de données :

Un rançongiciel est un type de virus utilisé par les cybercriminels pour chiffrer les données, les rendant illisibles pour la victime.

Pour pouvoir les récupérer, la victime se verra demander le paiement d'une rançon par les pirates.

Risque

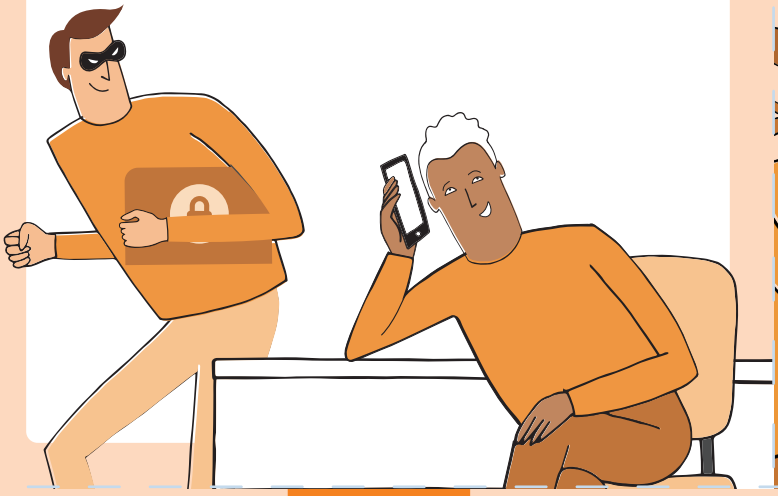
Exemples d'usurpation d'identité :

En fonction des informations recueillies, les escrocs peuvent commettre diverses infractions en se faisant passer pour la victime : escroquerie des proches, faux profil sur les réseaux sociaux, détournement d'allocations, souscription de crédit, ouverture de compte bancaire…

Risque

Vol de données d'identité

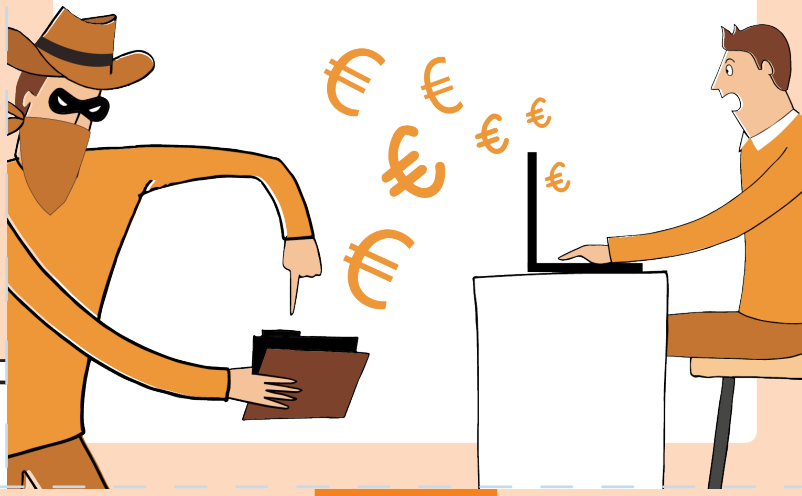
En étant trompée par hameçonnage (par mail, SMS ou appel téléphonique), une personne peut être amenée à communiquer des informations ou documents d'identité (copie de la carte d'identité, bulletins de paye, avis d'imposition, justificatif de domicile…).



Risque

Vol de données bancaires

En étant trompée par hameçonnage (par mail, SMS ou appel téléphonique), une personne peut être amenée à communiquer des informations bancaires (numéros de carte, code d'accès à son compte, ou encore des codes reçus par SMS de sa banque…).



Risque

Perte de données

Suite au piratage d'un compte ou à l'infection d'un appareil par un virus, un cybercriminel peut modifier, supprimer ou rendre illisibles les données de la victime.

Risque

Usurpation d'identité

L'usurpation d'identité est un délit qui désigne l'utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses.

Risque

Exemples d'escroquerie financière :

- Le cybercriminel tente de se faire passer pour vous (par mail, SMS, compte de réseau social piraté) et contacte des personnes de votre entourage pour essayer de les arnaquer.
- L'escroc fait semblant de dépanner la victime à distance pour lui facturer l'intervention, des logiciels anti-virus et/ou des abonnements fictifs.
- Le cybercriminel publie une annonce frauduleuse de location pour récupérer le montant de la caution en fournissant les documents qu'il a récupérés auprès d'une autre victime.

Bonne pratique

Bonne pratique

Bonne pratique

Bonne pratique

1

Ne communiquez jamais d'informations personnelles et bancaires demandées par messagerie ou par téléphone (mots de passe, numéro de sécurité sociale, code de validation par SMS…).

Aucune administration ou société commerciale sérieuse ne vous demandera ce type d'informations par mail, SMS ou téléphone.

Risque

Escroquerie financière

L'escroquerie financière a comme objectif de tromper la victime pour lui soutirer de l'argent en utilisant différents prétextes qui peuvent jouer sur la crainte, l'urgence, l'empathie, l'attrait du gain…

Bonne pratique

2

Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou SMS qui peuvent infecter votre appareil ou vous mener vers une page de phishing.

Vérifiez bien l'adresse du site avant de renseigner des données. En cas de doute, saisissez directement dans votre navigateur l'adresse du site concerné.

Bonne pratique

8

Ne communiquez que le minimum d'informations nécessaires sur les sites ou services en ligne. Désabonnez-vous ou supprimez les comptes (services, applications, sites internet) que vous n'utilisez plus.

Bonne pratique

Bonne pratique

Bonne pratique

Bonne pratique

Bonne pratique

7

N'enregistrez pas vos coordonnées de carte bancaire pour des achats ponctuels sur un site internet.

Si vous les avez enregistrées, **supprimez-les.**

Bonne pratique

9

Ne communiquez pas de documents d'identité de manière inconsidérée (pièce d'identité, fiche de paie, avis d'imposition, RIB, etc.).
Seuls des personnes ou organismes authentifiés avec certitude (administrations, bailleur, employeur...) peuvent avoir besoin de certains de ces documents.

Bonne pratique

10

Faites les mises à jour de vos appareils, applications et logiciels dès qu'elles sont proposées pour corriger leurs failles de sécurité qui peuvent être utilisées par des cybercriminels.

Bonne pratique

4

En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

Bonne pratique

Bonne pratique

Bonne pratique

Bonne pratique

Bonne pratique

11

Utilisez un antivirus sur vos appareils (ordinateur, téléphone mobile, tablette). Vérifiez régulièrement qu'il est bien à jour et faites des analyses pour vous assurer que vos appareils ne sont pas infectés.

Bonne pratique

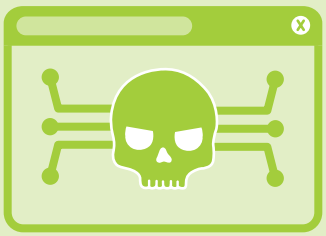
5

Utilisez des mots de passes différents et complexes pour chaque site et application utilisés.

Si un de vos comptes était piraté, les cybercriminels pourraient accéder à vos autres comptes qui utilisent le même mot de passe.

Bonne pratique

12



Évitez les sites internet non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent infecter votre appareil avec un virus.

Bonne pratique

6

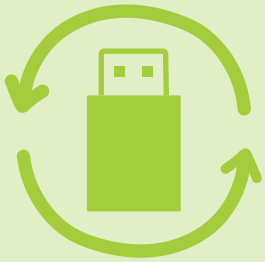
Activez la double authentification lorsque les sites ou les services le permettent, pour augmenter le niveau de sécurité de vos comptes. Il peut s'agir d'un code provisoire reçu par SMS ou par courrier électronique.

Bonne pratique

Bonne pratique

Bonne pratique

3



Sauvegardez régulièrement vos données pour pourvoir les retrouver en cas de panne, perte, vol, destruction ou piratage de vos appareils.

Bonne pratique

13

N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses. Ils pourraient contenir des virus.