ATELIER NUMÉRIQUE TOUS NIVEAUX

Les arnaques en ligne, cours d'autodéfense

NOUS SOMMES #CYBERENGAGÉS
CYBER MOIS
01 OCT
31 OCT
ÉDITION 2025

02 96 92 51 18
CONSEILLER-NUMERIQUE@PLOUGRESCANT.FR

CYBER MOIS
Financé par
GOUVERNEMENT
Liberté
Égalité
Fraternité
FRANCE RELANCE
CONSEILLER NUMÉRIQUE France services
PRESQU'ÎLE DE PLOUGRESCANT CÔTES-D'ARMOR

OBJECTIFS DE L'ATELIER

- Découvrir les différents types d'arnaques
- S'exercer à reconnaître les types d'arnaques
- Les réflexes à adopter face aux cybercriminels
- Se sentir plus en confiance pour les achats en ligne

Nous allons apprendre à nous mettre en cybersécurité.

Cyber : préfixe généralement utilisé pour signifier une dimension informatique et réseau à la notion qu'il accompagne : cyberharcèlement, cyberguerre, etc.

Découvrir les différents types d’arnaques en ligne

L'expression « en ligne » signifie « connecté à un réseau », en l'occurrence le réseau informatique Internet. Cette expression n'est donc pas propre au web, mais à Internet dans sa globalité, on la retrouve également à propos des réseaux téléphoniques.

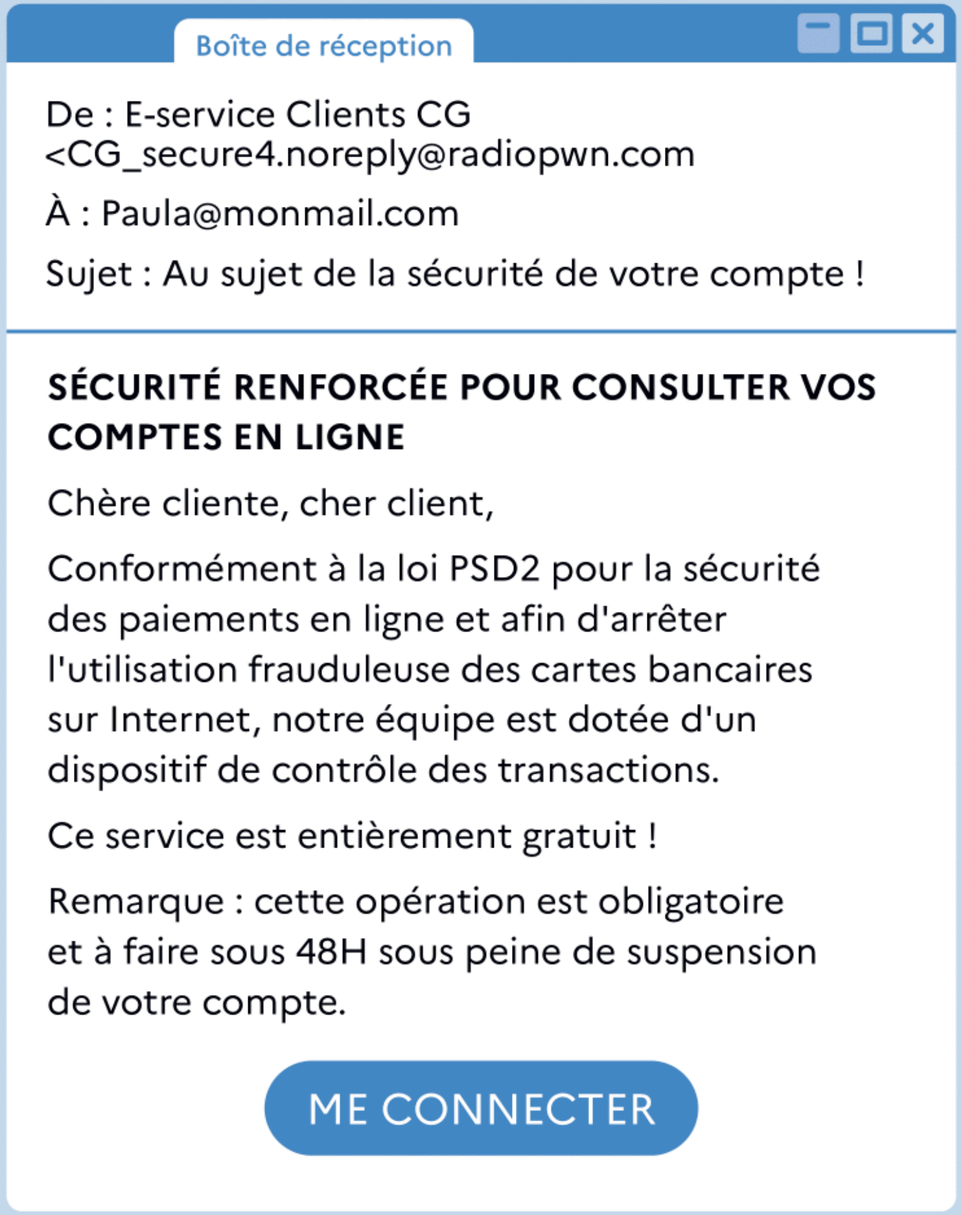
En ligne = via internet, au moyen de liens que vous retrouverez dans des :

- mails frauduleux
- SMS
- sites suspects
- etc.

cybermalveillance.gouv.fr

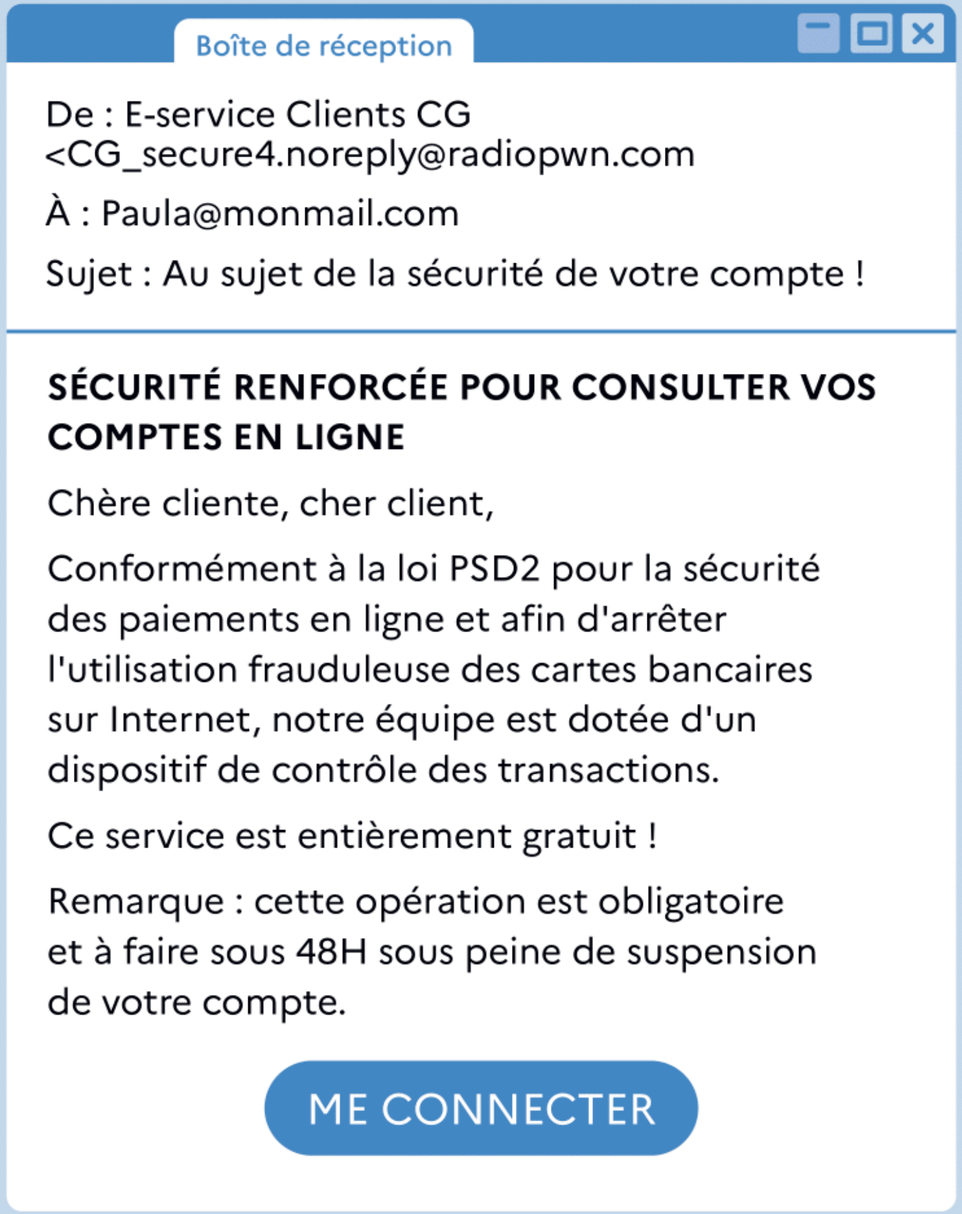
➡️ Assistance et prévention en cybersécurité pour les particuliers et les professionnels.

Paula reçoit un mail bancaire



Quel est le but recherché ?

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

Quel est le but recherché ?

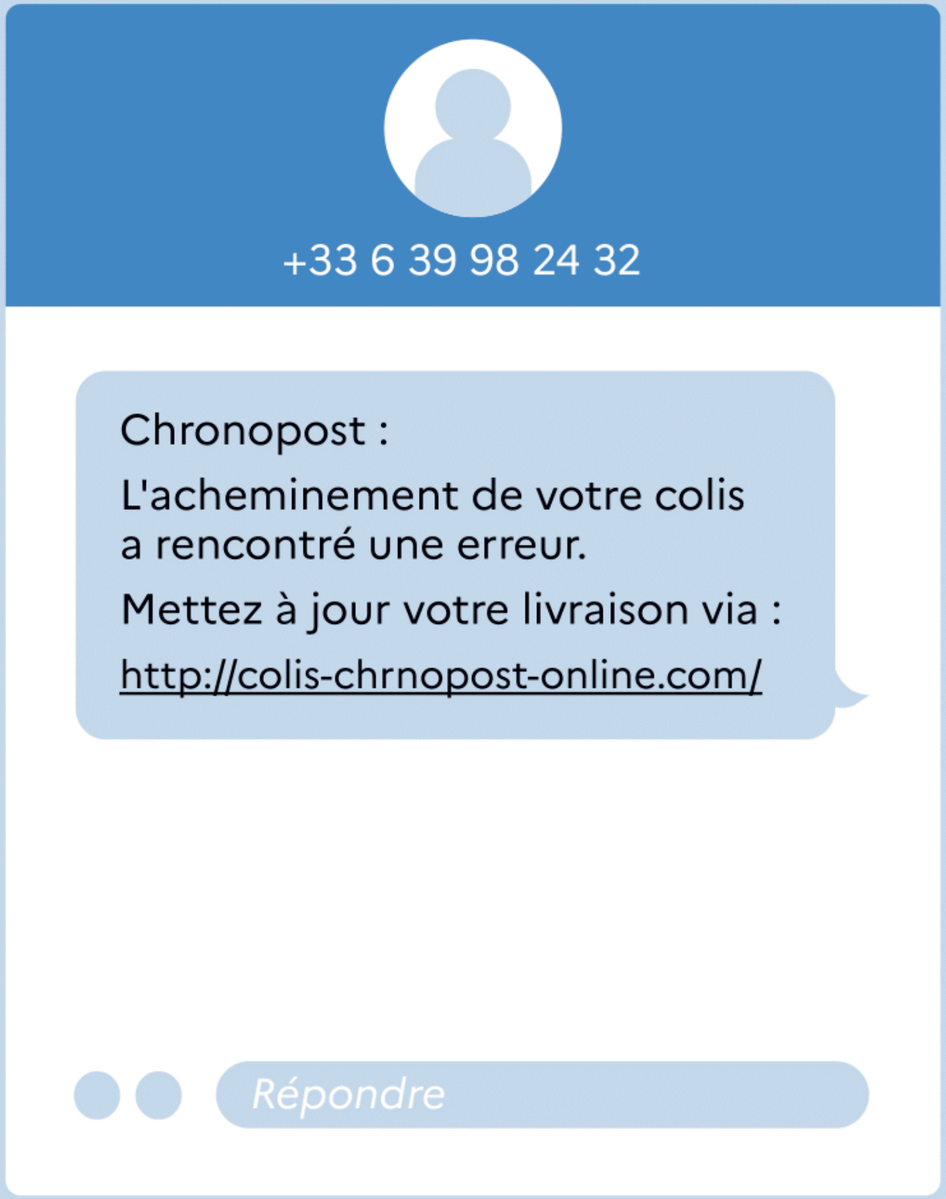
Voler des informations personnelles ou professionnelles pour en faire un usage frauduleux.

- Comptes
- Mots de passe
- Données bancaires

Bons réflexes à adopter :

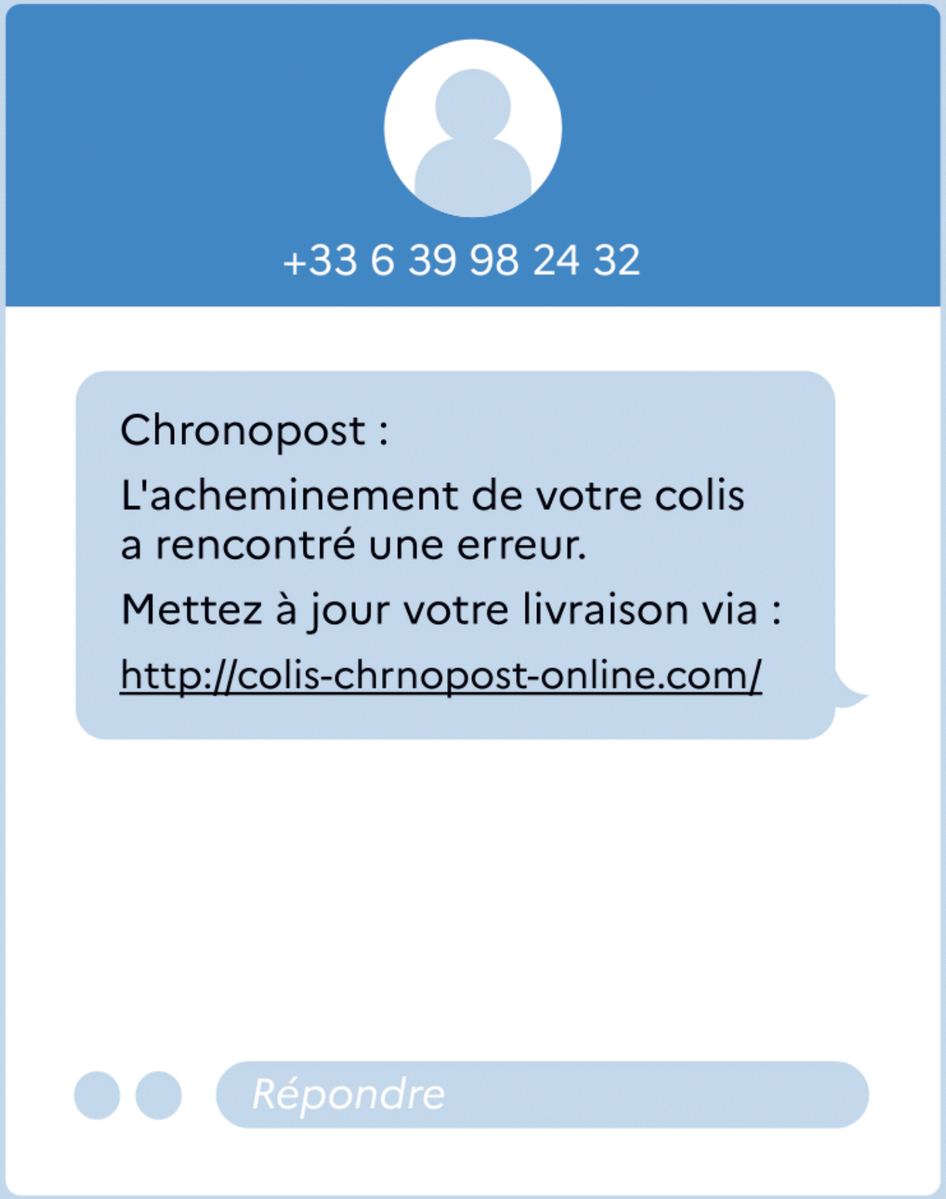
- Vérifier l'adresse mail
- Ne pas cliquer sur les liens dans les mails lorsqu'on est pas certain de l'émetteur
- Signaler le mail comme spam
- Supprimer le mail

Khadija reçoit un SMS



Quel est le but recherché ?

Khadija reçoit un SMS



Quel est le but recherché ?

Voler des informations personnelles ou professionnelles pour en faire un usage frauduleux.

- Comptes
- Mots de passe
- Données bancaires

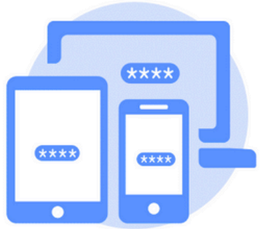
Bons réflexes à adopter :

- Vérifier le numéro de téléphone
- Ne pas cliquer sur les liens dans les sms lorsqu'on est pas certain de l'émetteur

Type d'arnaque : Hameçonnage (Phishing)

L'hameçonnage est une technique frauduleuse destinée à vous leurrer pour vous inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administration, etc.

Ne communiquez jamais d'information sensible suite à un message ou un appel



Utilisez des mots de passe différents et complexes pour chaque site et application

Au moindre doute, **contactez directement l'organisme concerné** pour confirmer ou infirmer l'information transmise

Activez la double authentification pour sécuriser vos accès si le site vous le permet

Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou sms.

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,

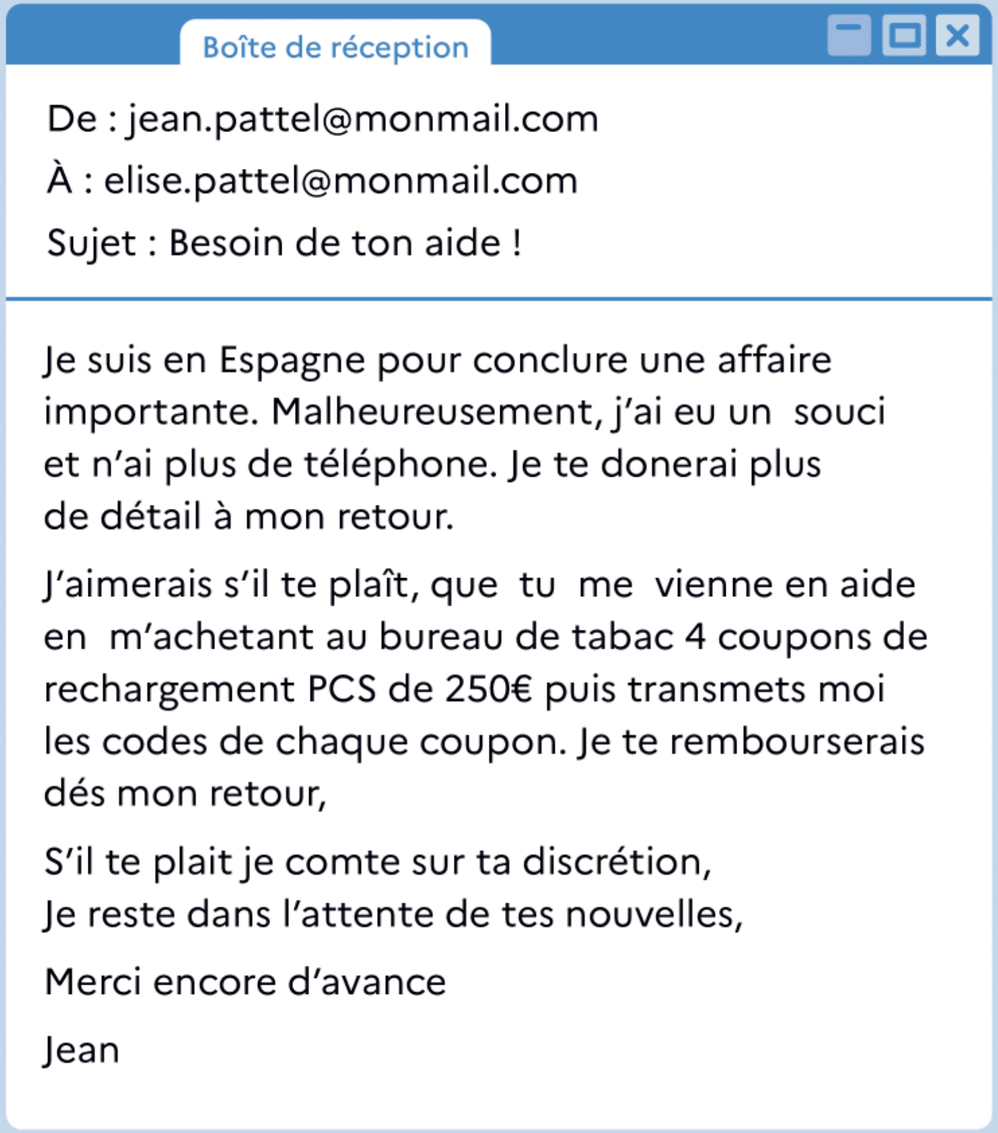
S'il te plait je comte sur ta discrétion,
Je reste dans l'attente de tes nouvelles,

Merci encore d'avance

Jean

Quel est le but recherché ?

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

Quel est le but recherché ?

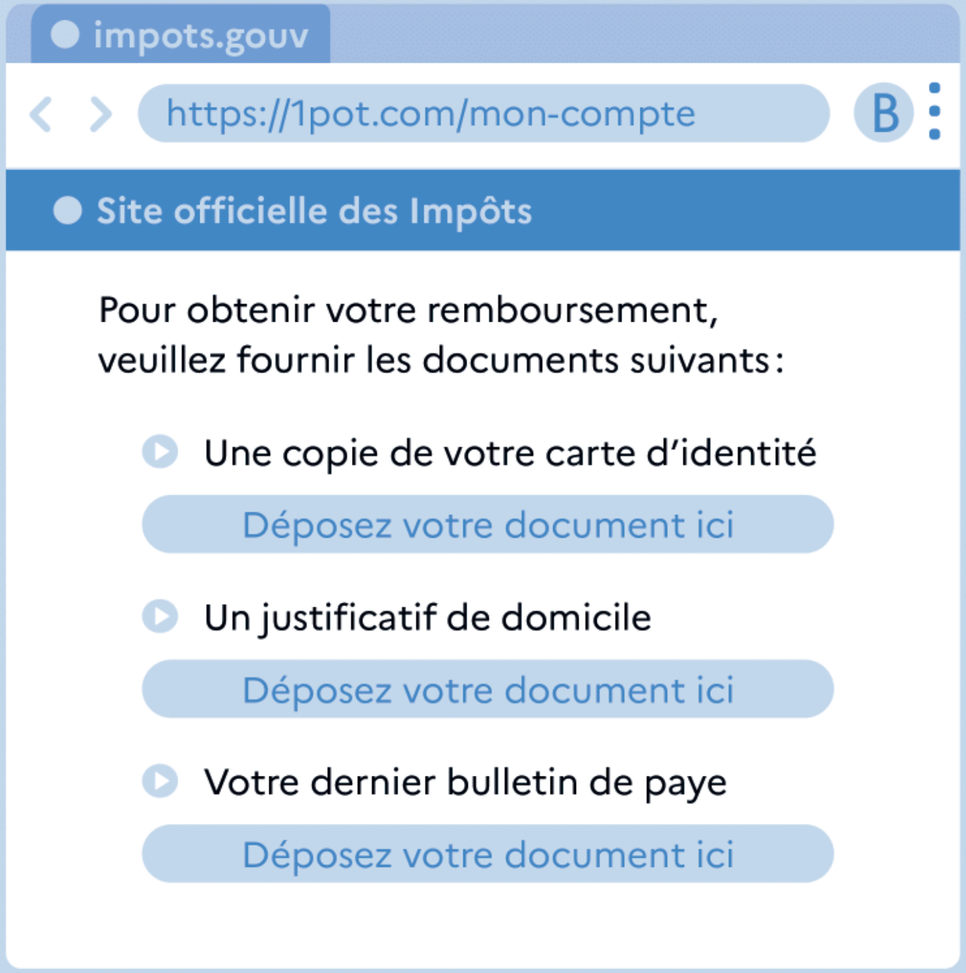
Voler des informations personnelles ou professionnelles pour en faire un usage frauduleux.

- Usurpation d'identité
- Transactions frauduleuses
- Spam

Bons réflexes à adopter :

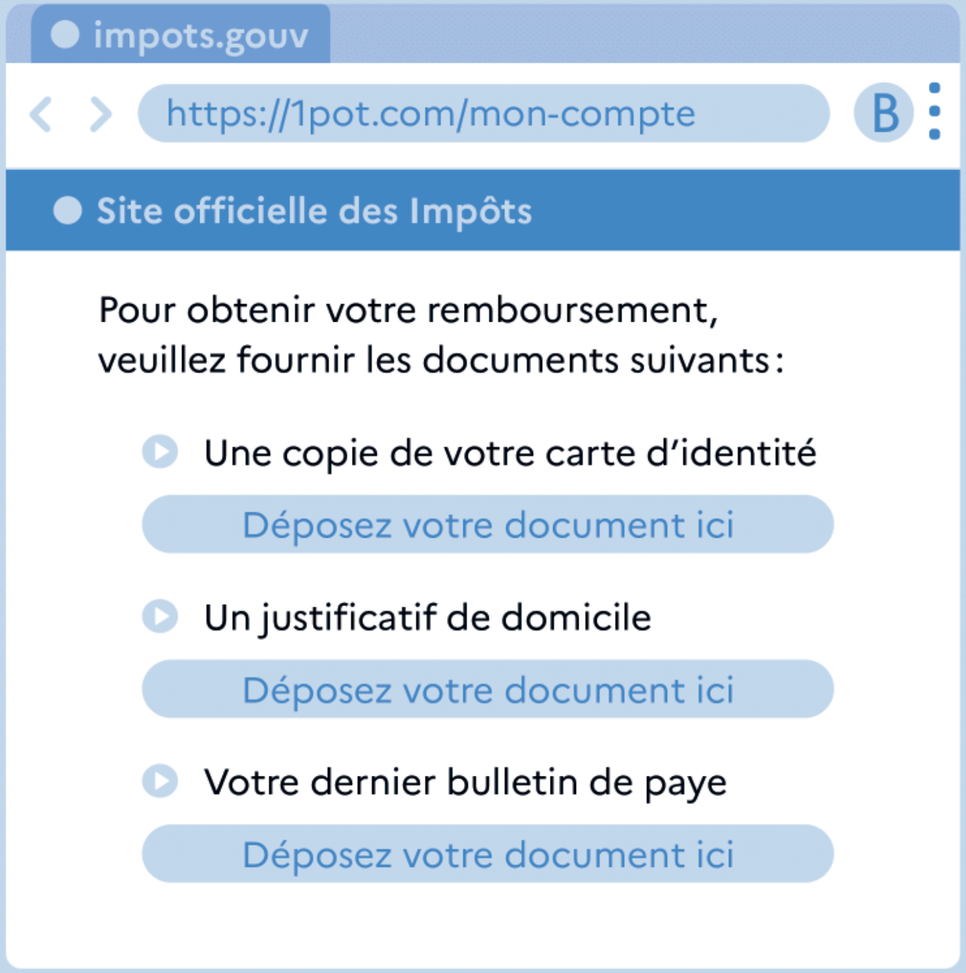
- Ne pas répondre au mail
- Appeler la personne concernée
- Supprimer le mail

Fatou croit envoyer des documents aux Impôts



Quel est le but recherché ?

Fatou croit envoyer des documents aux Impôts



Quel est le but recherché ?

Voler des informations personnelles ou professionnelles pour en faire un usage frauduleux.

- Usurpation d'identité
- Transactions frauduleuses
- Spam

Bons réflexes à adopter :

- Vérifier l'adresse du site qui s'affiche dans le navigateur
- Les sites officiels (dont les impôts) n'ont pas besoin de ces informations : ils les ont déjà

Type d'arnaque : Piratage

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerces en ligne. Les attaquants ont pu avoir accès à votre compte de plusieurs manières : mot de passe trop faible, mot de passe identique sur plusieurs sites, dont l'un a été piraté.

N'ouvrez pas les messages suspects, leurs pièces jointes et **ne cliquez pas sur les liens** provenant d'expéditeurs inconnus.

Évitez les sites internet non sûrs ou illicites qui hébergent des contrefaçons ou certains sites pornographiques qui peuvent infecter votre appareil avec un virus.

Sauvegardez régulièrement vos données pour vous protéger en cas de panne, de perte, de vol, de destruction de votre matériel ou de piratage informatique.

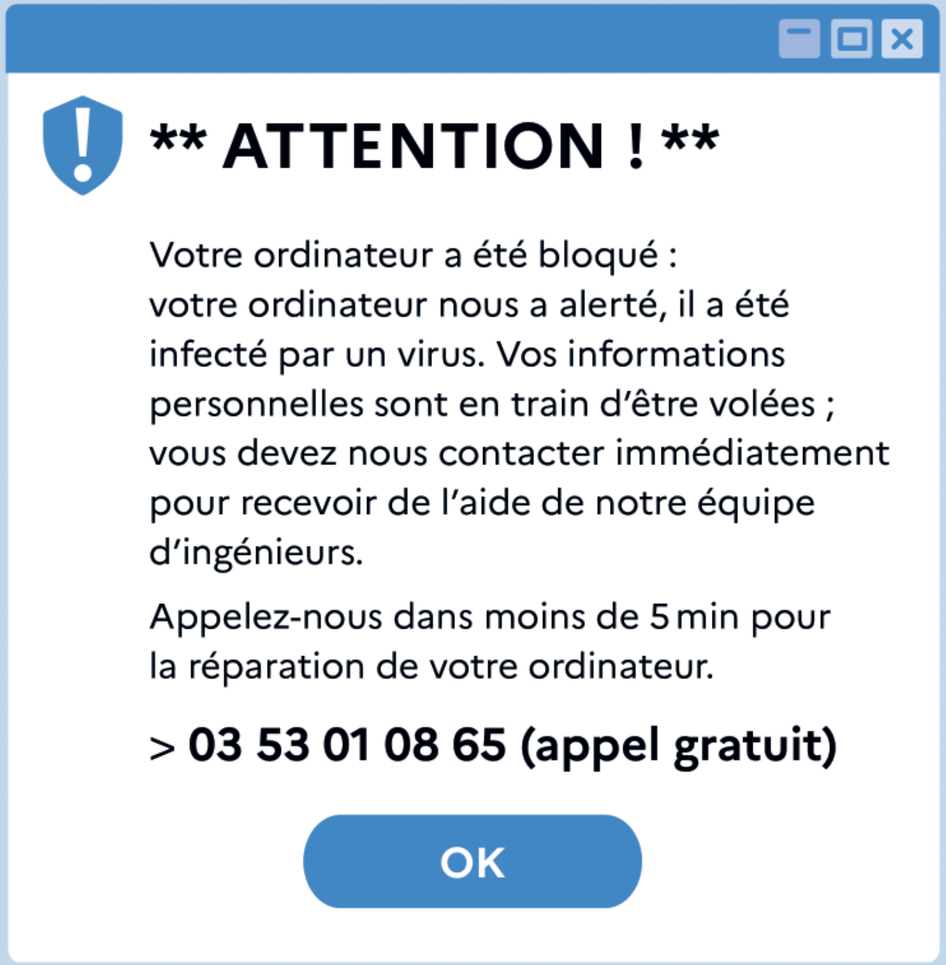
Utilisez des mots de passe différents et complexes pour chaque site et application.

Activez la double authentification lorsqu'elle est disponible.

Utilisez un antivirus et mettez-le à jour.

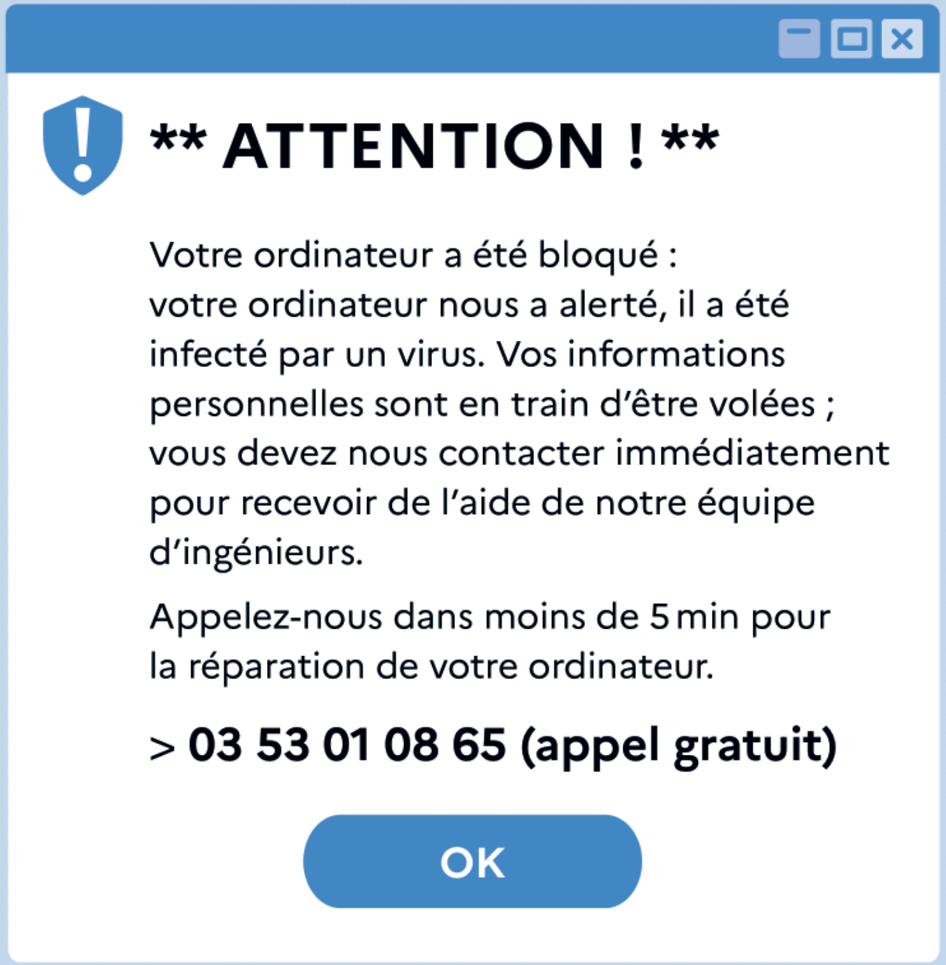
Mettez à jour régulièrement votre appareil, votre système d'exploitation et ses logiciels.

Bertrand navigue sur Internet.
Soudain, une fenêtre apparaît



Quel est le but recherché ?

Bertrand navigue sur Internet.
Soudain, une fenêtre apparaît



Quel est le but recherché ?

Soutirer de l'argent à la victime.

- Prise de contrôle de sa machine en faisant semblant de la lui dépanner
- Souscrire des abonnements pour des logiciels facturés par la suite

Bons réflexes à adopter :

- Ne pas répondre ni rappeler
- Si l'ordinateur semble bloqué, le redémarrez de manière forcée (bouton)
- En cas de doute et si vous n'arrivez pas à reprendre le contrôle de votre appareil :

www.cybermalveillance.gouv.fr/diagnostic/profil

Type d'arnaque : Faux support technique

Tech support scan en anglais, consiste à effrayer la victime par SMS, téléphone, chat, courriel ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google), pour ensuite la convaincre de payer un pseudo dépannage informatique.

Utilisez un antivirus sur vos matériels (ordinateur, téléphone mobile, tablette) et faites des analyses régulières (scan)

Évitez les sites internet non sûrs ou illicites qui hébergent des contrefaçons ou certains sites pornographiques qui peuvent infecter votre appareil avec un virus.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.

Appliquez de manière systématique les mises à jour de sécurité de vos appareils et leurs applications, en particulier vos navigateurs.

N'ouvrez pas les messages suspects, leurs pièces jointes et **ne cliquez pas sur les liens** provenant d'expéditeurs inconnus.

N'appelez jamais un numéro de support technique qui s'affiche à l'écran.

Type d'arnaque : Fuite de données personnelles

Une fuite ou violation de données personnelles est l'accès ou la divulgation non autorisés d'informations personnelles détenues par un tiers (site, entreprise, association, collectivité, administration, etc.).

Qu'est-ce qu'une donnée personnelle ?

Information susceptible de permettre d'identifier une personne : nom, adresse postale, adresse de messagerie, numéro de téléphone, numéro de sécurité sociale, etc.

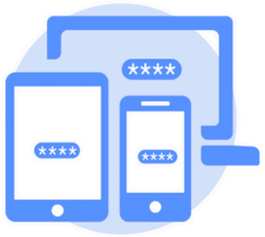
L'origine de la fuite peut être accidentelle ou malveillante. Selon la nature des informations concernées et si elles sont récupérées par des cybercriminels, une fuite de données personnelles peut avoir de multiples conséquences pour la victime : hameçonnage ciblé, escroquerie, usurpation d'identité, piratage de compte.

Type d'arnaque : Fuite de données personnelles

Ne communiquez pas de documents d'identité de manière inconsidérée (pièce d'identité, fiche de paie, avis d'imposition, RIB, etc.).

Ne communiquez que le minimum d'informations nécessaires sur les sites ou services en ligne.

Activez la double authentification lorsque les sites ou les services le permettent, pour augmenter le niveau de sécurité.



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

Désabonnez-vous ou supprimez les comptes en ligne que vous n'utilisez plus pour limiter les risques de fuite de vos données.

N'enregistrez pas vos coordonnées de carte bancaire pour des achats ponctuels sur un site Internet. Si vous les avez enregistrées, supprimez-les.

S’exercer à reconnaître les types d’arnaques

Rappel des arnaques vues :

- Phishing / Hameçonnage
- Piratage
- Faux support technique
- Fuite de données personnelles

➡️ Comment réagir face à ces arnaques ?

Je ne panique pas.

Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez un appel téléphonique du numéro suivant : 07 85 69 25 63

Vous décrochez, pensant que cela pourrait être un appel de l'un de vos proches.

"Bonjour, je suis Mélissa Dupont de [votre banque] et je remarque une activité suspecte sur votre compte depuis ce matin. Il y a eu plusieurs prélèvements de sommes importantes sur votre compte : 250€, 310€, 120€. J'aurais donc besoin de confirmer avec vous plusieurs informations concernant votre compte. Dans un premier temps, est-ce que vous pouvez me confirmer votre nom, prénom, date de naissance et numéro de compte ?"

Vous recevez un appel téléphonique du numéro suivant : 07 85 69 25 63

Vous décrochez, pensant que cela pourrait être un appel de l'un de vos proches.

"Bonjour, je suis Mélissa Dupont de [votre banque] et je remarque une activité suspecte sur votre compte depuis ce matin. Il y a eu plusieurs prélèvements de sommes importantes sur votre compte : 250€, 310€, 120€. J'aurais donc besoin de confirmer avec vous plusieurs informations concernant votre compte. Dans un premier temps, est-ce que vous pouvez me confirmer votre nom, prénom, date de naissance et numéro de compte ?"

Autodéfense contre les cybercriminels

Comment réagir ?

Réponse type :

"D'accord, je raccroche pour bloquer ma carte depuis mon application mobile et je rappelle ma conseillère à l'agence, merci. Au revoir."

Ne communiquez jamais d'information sensible suite à un message ou un appel

Au moindre doute, **contactez directement l'organisme concerné** pour confirmer ou infirmer l'information transmise

Hameçonnage

Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez le SMS suivant :

Indice : vous n’avez pas pris l’autoroute depuis le mois de mai.

Vous recevez le SMS suivant :

Indice : vous n'avez pas pris l'autoroute depuis le mois de mai.

Autodéfense contre les cybercriminels

Comment réagir ?

Ignorer et supprimer le SMS.

Si vous aviez pris l'autoroute, vérifier vos comptes et tickets bancaires, prendre contact avec l'entreprise de péage.

Ne communiquez jamais d'information sensible suite à un message ou un appel

Au moindre doute, **contactez directement l'organisme concerné** pour confirmer ou infirmer l'information transmise

Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou sms.

Hameçonnage

Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez le SMS suivant :

Indice : vous avez commandé un colis et reçu plusieurs mails du transporteur Fedex.

Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez le SMS suivant :

Indice : vous avez commandé un colis et reçu plusieurs mails du transporteur Fedex.

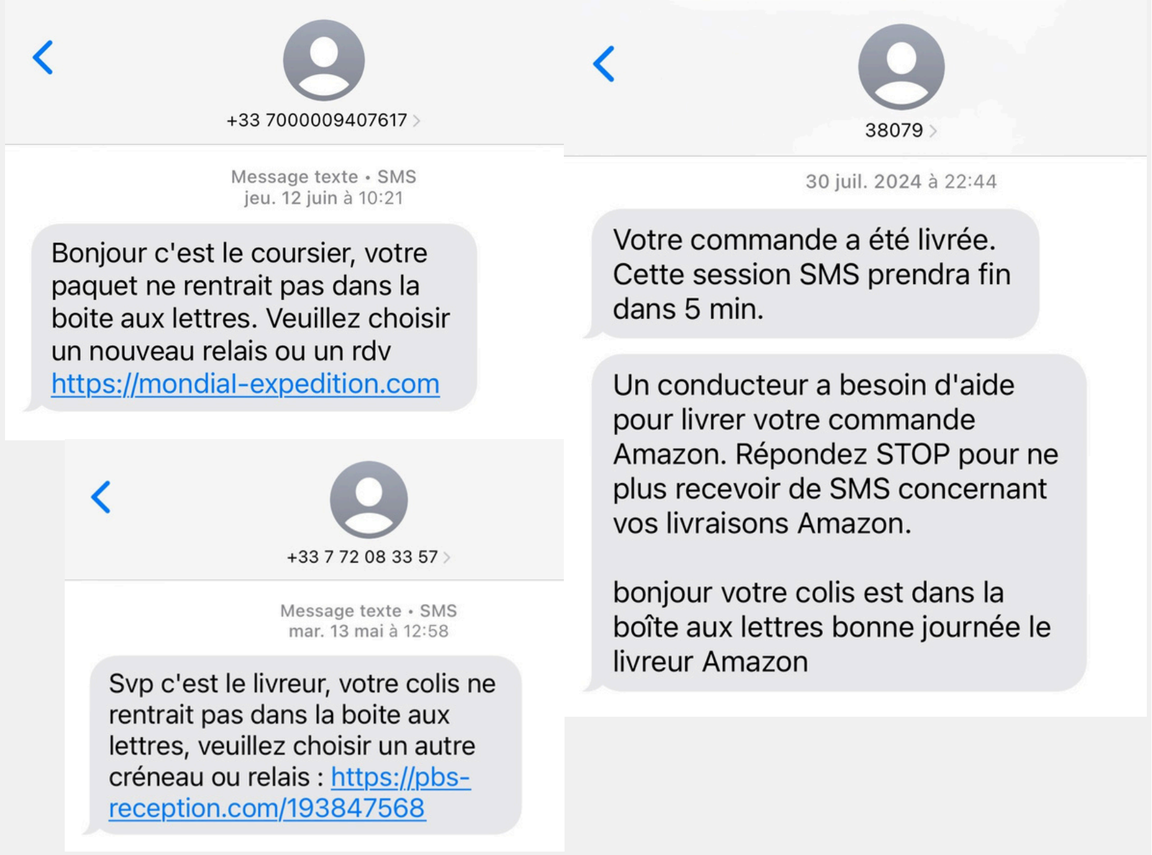
Exemple de SMS légitime.

Le lien renvoi bien vers le site officiel de Fedex.
En cas de doute, prendre contact avec Fedex.

Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez les SMS suivants :



Indice : vous avez commandé plusieurs colis ces derniers temps.

Autodéfense contre les cybercriminels

Vous recevez les SMS suivants :

+33 7000009407617

Message texte • SMS
jeu. 12 juin à 10:21

Bonjour c'est le coursier, votre paquet ne rentrait pas dans la boite aux lettres. Veuillez choisir un nouveau relais ou un rdv https://mondial-expedition.com

38079

30 juil. 2024 à 22:44

Votre commande a été livrée. Cette session SMS prendra fin dans 5 min.

Un conducteur a besoin d'aide pour livrer votre commande Amazon. Répondez STOP pour ne plus recevoir de SMS concernant vos livraisons Amazon.

bonjour votre colis est dans la boîte aux lettres bonne journée le livreur Amazon

+33 7 72 08 33 57

Message texte • SMS
mar. 13 mai à 12:58

Svp c'est le livreur, votre colis ne rentrait pas dans la boite aux lettres, veuillez choisir un autre créneau ou relais : https://pbs-reception.com/193847568

Indice : vous avez commandé plusieurs colis ces derniers temps.

Comment réagir ?

SMS légitime en vert : pas de lien, numéro officiel # SMS de cybercriminels en rouge : incitation à cliquer sur des liens, numéros non officiels.

Ne communiquez jamais d'information sensible suite à un message ou un appel

Au moindre doute, **contactez directement l'organisme concerné** pour confirmer ou infirmer l'information transmise

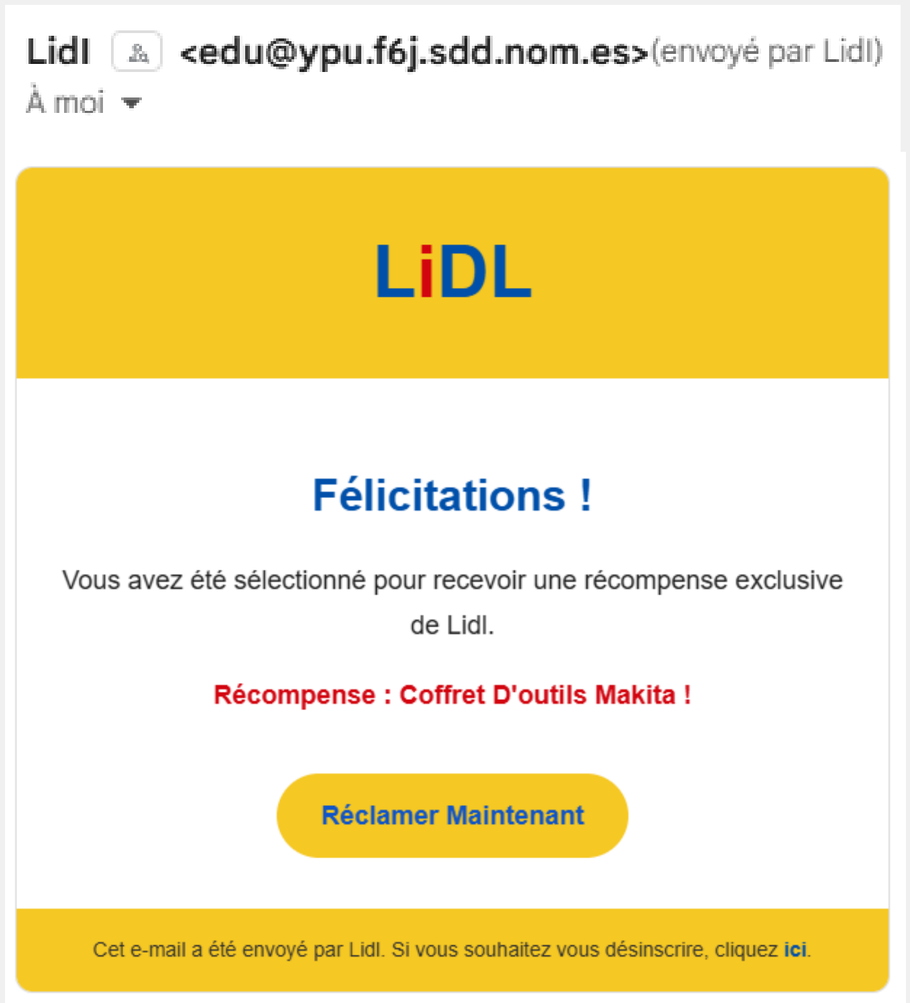
Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou sms.

Hameçonnage

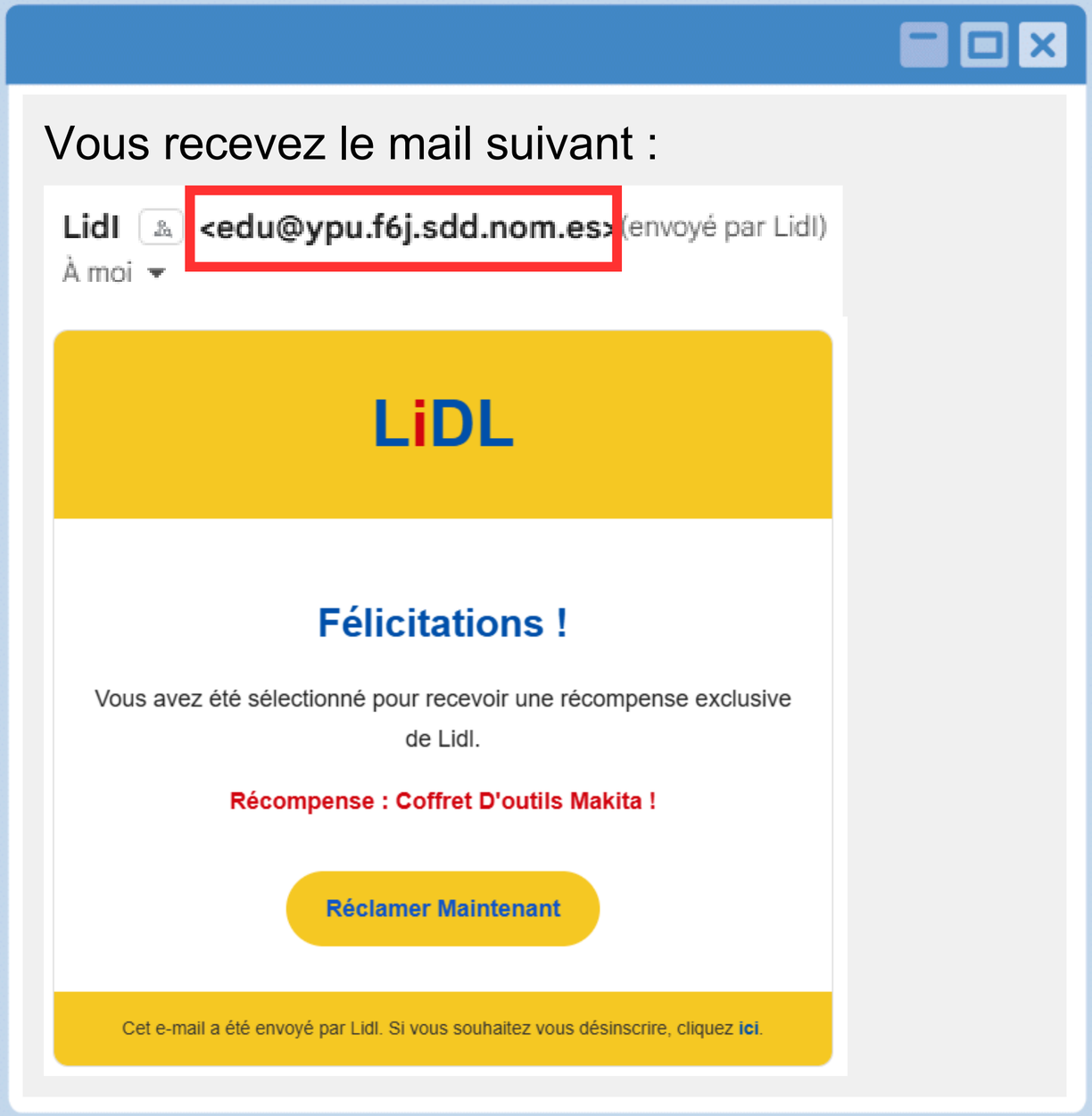
Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez le mail suivant :



Autodéfense contre les cybercriminels



Comment réagir ?

Ignorer et signaler le mail comme SPAM.

L'adresse mail n'est pas l'adresse mail officielle de Lidl. Le logo n'est pas le logo officiel de Lidl.

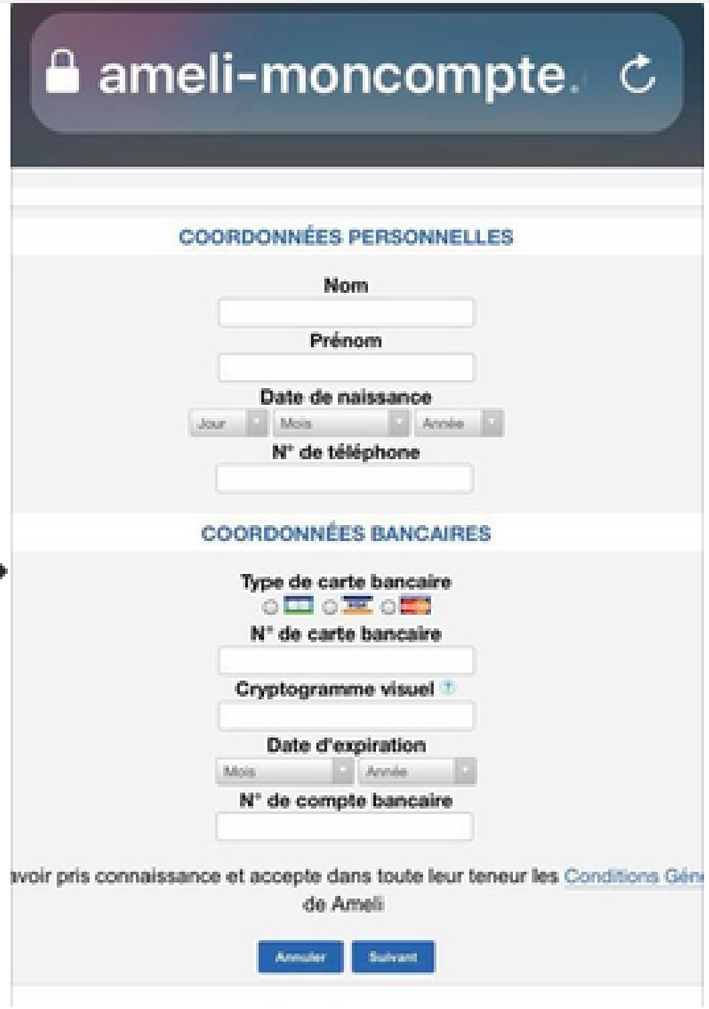
Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou sms.

Hameçonnage

Autodéfense contre les cybercriminels

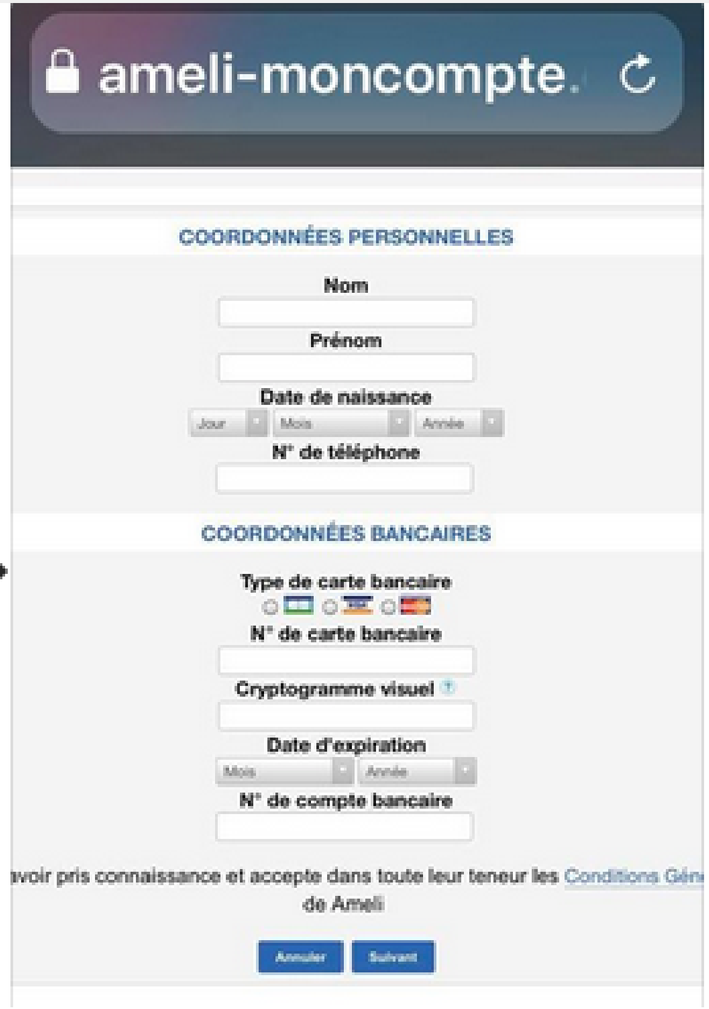
Comment réagir ?

Vous avez reçu un mail de l'Assurance Maladie pour obtenir un remboursement et vous vous retrouvez sur ce site :



Autodéfense contre les cybercriminels

Vous avez reçu un mail de l'Assurance Maladie pour obtenir un remboursement et vous vous retrouvez sur ce site :



Comment réagir ?

Quitter la page, signaler le mail comme SPAM.

- Vérifier l'adresse du site qui s'affiche dans le navigateur
- Les sites officiels (dont Ameli) n'ont pas besoin de ces informations : ils les ont déjà

N'ouvrez pas les messages suspects, leurs pièces jointes et **ne cliquez pas sur les liens** provenant d'expéditeurs inconnus.

Évitez les sites internet non sûrs ou illicites qui hébergent des contrefaçons ou certains sites pornographiques qui peuvent infecter votre appareil avec un virus.

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

Activez la double authentification lorsqu'elle est disponible.

Piratage

Autodéfense contre les cybercriminels

Comment réagir ?

Vous recevez un appel téléphonique du numéro suivant : 06 84 69 25 63

Vous décrochez, pensant que cela pourrait être un appel de l'un de vos proches.

"Bonjour, je suis Valentin Dupont de France Cybermalveillance et je remarque une activité suspecte sur votre ordinateur depuis ce matin. Il y a un virus qui se propage sur les ordinateurs toujours sous le système d'exploitation Windows 10, ce qui semble être votre cas. Dans un premier temps, est-ce que vous pouvez me confirmer votre adresse mail pour que je vous envoi un lien afin que je puisse installer un nouvel antivirus sur votre machine ?"

Vous recevez un appel téléphonique du numéro suivant : 06 84 69 25 63

Vous décrochez, pensant que cela pourrait être un appel de l'un de vos proches.

"Bonjour, je suis Valentin Dupont de France Cybermalveillance et je remarque une activité suspecte sur votre ordinateur depuis ce matin. Il y a un virus qui se propage sur les ordinateurs toujours sous le système d'exploitation Windows 10, ce qui semble être votre cas. Dans un premier temps, est-ce que vous pouvez me confirmer votre adresse mail pour que je vous envoi un lien afin que je puisse installer un nouvel antivirus sur votre machine ?"

Autodéfense contre les cybercriminels

Comment réagir ?

Réponse type :

"D'accord, je raccroche pour regarder cela de mon côté, je suis informaticien de métier, merci. Au revoir."

Utilisez un antivirus sur vos matériels (ordinateur, téléphone mobile, tablette) et faites des analyses régulières (scan)

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.

Appliquez de manière systématique les mises à jour de sécurité de vos appareils et leurs applications, en particulier vos navigateurs.

Faux support technique

Autodéfense contre les cybercriminels

Comment réagir ?

Vous regardez les informations à la télévision lorsque soudain est lancé un reportage sur une fuite de données massive chez Free (dont vous êtes client) suite à un piratage de leurs services.

En vérifiant votre boîte mail dans les prochains jours, vous recevez un mail de la part de Free vous avertissant que votre nom, prénom, date de naissance, numéro de client, numéro de téléphone et votre mot de passe ont été vendu sur le dark web...

Dark web : désigne la partie cachée et chiffrée d'internet qui est inaccessible via les navigateurs web traditionnels. Il fait partie du « deep web », qui englobe tout le contenu de l'internet non indexé par les moteurs de recherche et inaccessible par les requêtes de recherche standard.

Autodéfense contre les cybercriminels

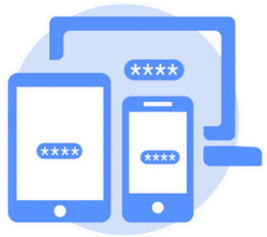
Vous regardez les informations à la télévision lorsque soudain est lancé un reportage sur une fuite de données massives chez Free (dont vous êtes client) suite à un piratage de leurs services.

En vérifiant votre boîte mail dans les prochains jours, vous recevez un mail de la part de Free vous avertissant que votre nom, prénom, date de naissance, numéro de client, numéro de téléphone et votre mot de passe ont été vendu sur le dark web...

Dark web : désigne la partie cachée et chiffrée d'internet qui est inaccessible via les navigateurs web traditionnels. Il fait partie du « deep web », qui englobe tout le contenu de l'internet non indexé par les moteurs de recherche et inaccessible par les requêtes de recherche standard.

Comment réagir ?

- Modifier votre mot de passe Free + mot de passe identique sur d'autres services
- Rester vigilant : SMS, mails, appels frauduleux



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

Activez la double authentification lorsque les sites ou les services le permettent, pour augmenter le niveau de sécurité.

Fuite de données

Achats en ligne

Comment se sentir plus en confiance ?

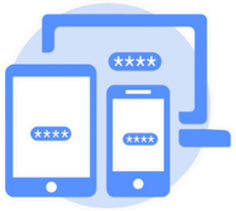
- Lancer une recherche Google du site par lequel vous allez acheter. Exemples :

  achat lookfantastic arnaque

  avis achat lookfantastic france

Ne communiquez que le minimum d'informations nécessaires sur les sites ou services en ligne.

N'enregistrez pas vos coordonnées de carte bancaire pour des achats ponctuels sur un site Internet. Si vous les avez enregistrées, supprimez-les.



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

- Prendre contact avec votre banque pour bénéficier d'une carte bancaire virtuelle

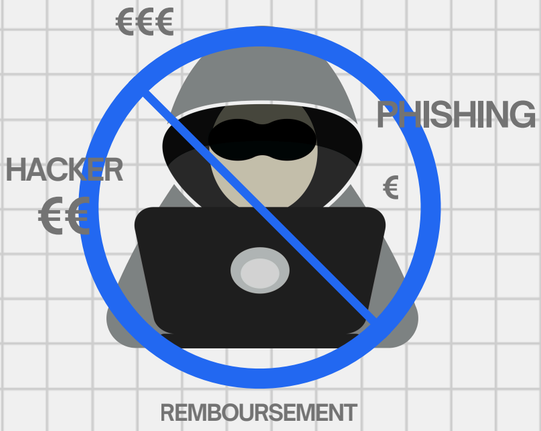
Une carte de crédit virtuelle est une forme numérisée de carte bancaire, conçue principalement pour les transactions en ligne.

Liée à un compte bancaire principal, elle peut générer des numéros uniques pour chaque achat. Cela permet de renforcer la sécurité contre la fraude et le vol de données.

L'inconvénient de la carte bancaire virtuelle est que vous avez besoin d'un smartphone pour que ce service puisse fonctionner…

DES QUESTIONS ?

Des commentaires ?



GIP ACYMA - Cybermalveillance.gouv.fr - contenus téléchargés sur https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/outils-acteurs-mediation mise à jour du 03 Avril 2025

02 96 92 51 18
CONSEILLER-NUMERIQUE@PLOUGRESCANT.FR

Financé par GOUVERNEMENT Liberté Égalité Fraternité