LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Se protéger sur Internet et identifier les risques

Dans un monde numérique en constante évolution, comprendre les menaces et adopter les bonnes pratiques de cybersécurité est essentiel pour tous. Ce guide vous aidera à naviguer en toute sécurité sur Internet et à protéger vos informations personnelles contre les pirates informatiques.

Images : freepik

MAJ 18/08/2023

Aperçu de notre présentation

Les menaces

Comprendre les différentes menaces en ligne et les techniques utilisées par les pirates informatiques

Se protéger

Adopter les bonnes pratiques pour sécuriser vos appareils et naviguer en toute sécurité

Sauvegarde et mise à jour

Assurer la sécurité de vos données par des sauvegardes et mises à jour régulières

Ensemble, nous explorerons ces trois aspects essentiels de la cybersécurité pour vous permettre de profiter d'Internet en toute sécurité.

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Les idées reçues sur les dangers d'Internet

Mythe 1 : "Je n'ai rien à cacher, donc je n'ai rien à craindre"

Même des informations apparemment anodines peuvent être utilisées contre vous, notamment pour l'usurpation d'identité ou les arnaques ciblées.

Mythe 2 : "Seules les grandes entreprises sont ciblées"

Les particuliers sont souvent des cibles plus faciles car moins protégées que les grandes organisations.

Mythe 3 : "Mon antivirus me protège totalement"

Un antivirus est essentiel mais ne protège pas contre toutes les menaces, notamment l'ingénierie sociale et le phishing.

Être conscient de ces idées reçues est la première étape pour adopter une attitude plus vigilante en ligne et mieux protéger vos données personnelles.

Quels sont les objectifs des pirates informatiques ?

- Démontrer une faille dans un système informatique
- Espionner des individus ou des organisations
- Récupérer des données personnelles (bancaires, identité...)
- Faire des blagues (parfois malveillantes)
- S'enrichir par diverses techniques d'extorsion

Les motivations des pirates informatiques varient considérablement, allant de la simple démonstration technique à des objectifs financiers ou politiques plus graves.

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Le saviez-vous ?

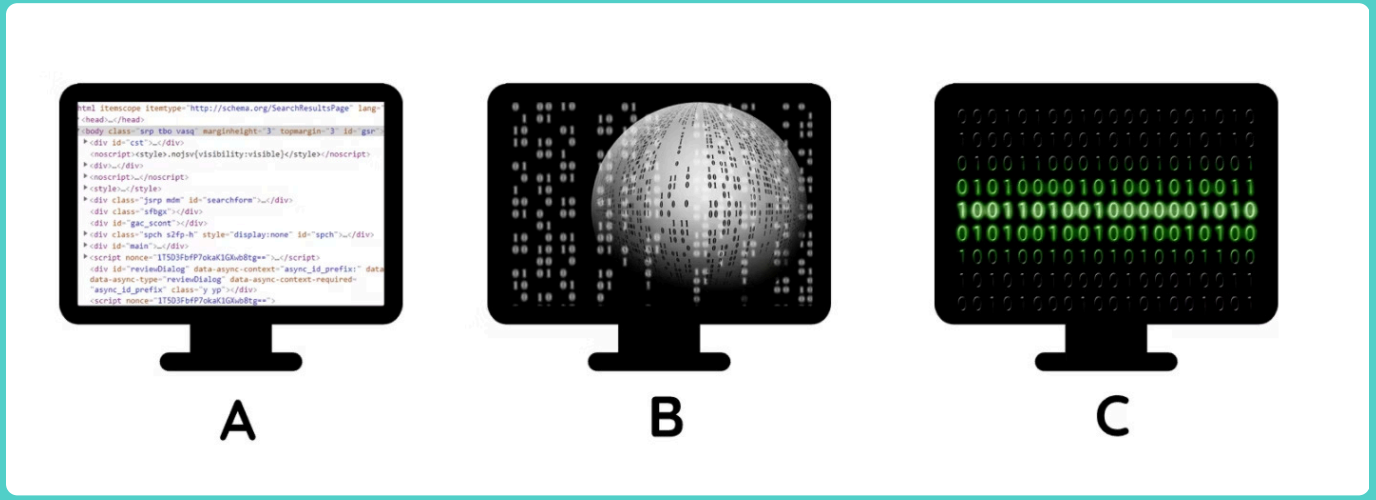
"30 milliards de données ont été volées en 2020, soit plus que le total cumulé des 15 dernières années"

Le contexte de la pandémie a intensifié nos interactions numériques ; avec la concentration des données, c'est une véritable aubaine pour les cybercriminels.

Parfois, les hackeurs piratent avec éthique. C'est à dire pour dénoncer les dérives de la surveillance numérique, défendre la liberté d'information, d'expression ou les atteintes aux libertés fondamentales.

Source : Courrier International n°1596 du 3 au 9 juin 2021

À votre avis, à quoi ressemble l'écran d'un pirate informatique ?



La plupart du temps, pour pirater un ordinateur, il faut utiliser des **lignes de code** qui ressemblent à l'image A.

Pour détourner le système, il ne suffit pas d'écrire des chiffres 0 et 1 comme on le voit souvent dans les films !

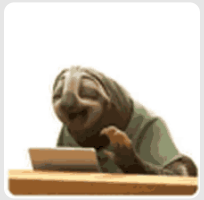
LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Quand vous vous faites pirater, que peut-il se passer sur votre ordinateur ?

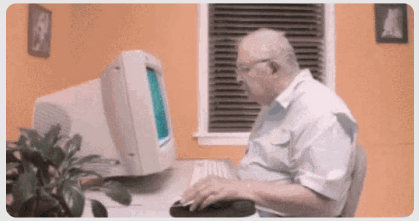
Ralentissement

Votre ordinateur peut devenir plus lent



Bugs fréquents

Il peut manifester des bugs et dysfonctionnements



Perte de données

Vous risquez de perdre des fichiers personnels importants

⚠ Contrairement aux idées reçues, votre ordinateur n'explosera pas et votre écran ne se fissurera pas lors d'un piratage. Les dommages sont généralement liés aux performances et aux données.

Quelles sont les techniques des pirates ?

Les pirates informatiques sont des individus qui utilisent divers moyens pour frauder les utilisateurs, endommager leur équipement informatique ou voler les informations confidentielles des entreprises et des particuliers en ligne. Pour parvenir à leurs fins, ils emploient diverses techniques sophistiquées.

Dans les prochaines diapositives, nous examinerons en détail ces techniques pour mieux les comprendre et savoir comment s'en protéger.

1- L'absence d'antivirus sur votre appareil

Un ordinateur ou un appareil mobile sans antivirus est comme une maison sans serrure - accessible à tous les intrus. Les logiciels malveillants peuvent :

- Voler vos données personnelles
- Espionner votre activité en ligne
- Prendre le contrôle de votre appareil
- Endommager vos fichiers importants

Il est **essentiel** d'installer un antivirus fiable et de le maintenir à jour régulièrement pour bénéficier des dernières protections.

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

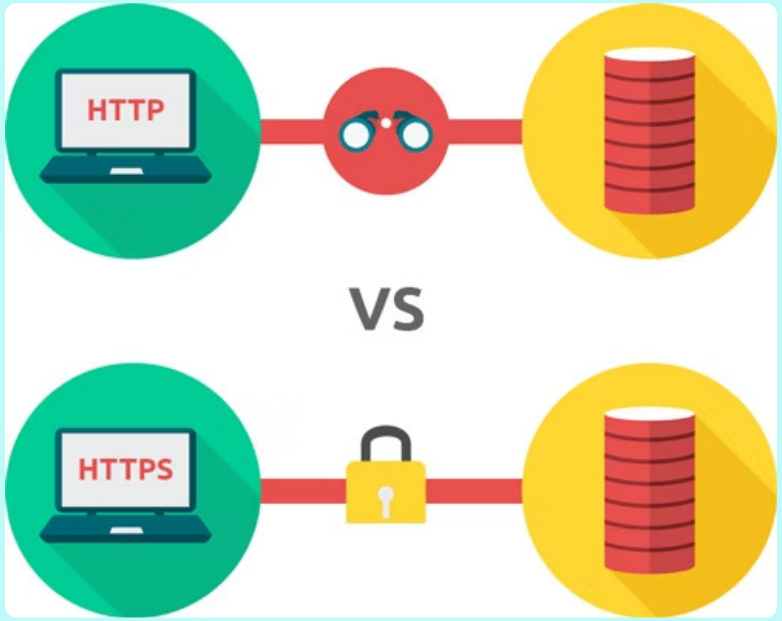
Loiret votre Département

2- Naviguer sur des sites internet non sécurisés

Visiter des sites non sécurisés expose gravement vos données personnelles :

- Vos informations de connexion peuvent être interceptées
- Des logiciels malveillants peuvent être téléchargés à votre insu
- Vos habitudes de navigation peuvent être suivies et exploitées
- Vos informations bancaires risquent d'être volées lors des paiements

Recherchez toujours le cadenas et "https://" dans l'adresse du site avant de partager des informations sensibles.



3- L'utilisation d'un réseau wifi public non sécurisé

Les réseaux wifi publics sont des terrains de jeu pour les pirates informatiques car :

- Vos données transitent sans être chiffrées
- N'importe qui peut se connecter et intercepter le trafic
- Les attaques "homme du milieu" sont faciles à réaliser
- Votre appareil peut être plus facilement infiltré

Évitez d'effectuer des transactions bancaires, des achats en ligne ou de vous connecter à des comptes sensibles lorsque vous utilisez un réseau wifi public.

Privilégiez l'utilisation d'un VPN (réseau privé virtuel) pour chiffrer vos données sur les réseaux publics.

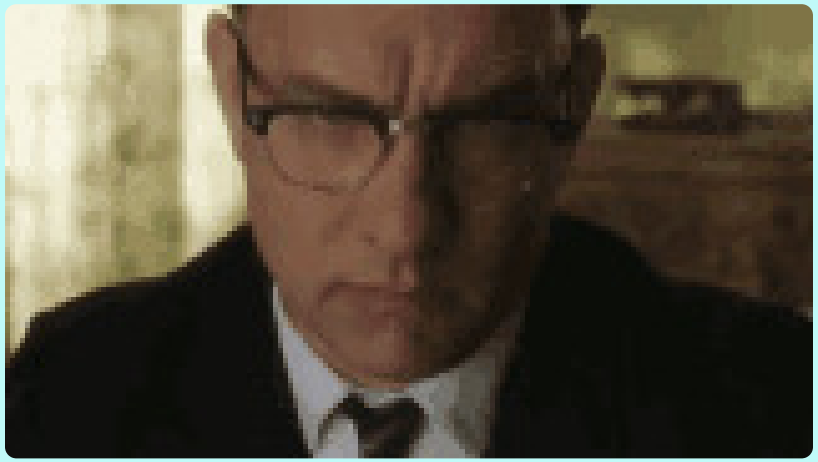
LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

5-Les fausses promesses

Les pirates utilisent souvent des offres alléchantes pour vous piéger :

- Gains d'argent importants pour un effort minimal
- Produits de luxe à prix dérisoires
- Voyages gratuits ou promotions exceptionnelles
- Héritages inattendus de personnes inconnues
- Remboursements importants d'organismes officiels



Si une offre semble trop belle pour être vraie, c'est qu'elle l'est probablement. Ces techniques visent à vous faire baisser votre vigilance et à partager vos informations personnelles.

⊗ Rappelez-vous : personne ne vous offre d'argent gratuitement sur internet. Méfiez-vous des offres qui semblent trop avantageuses.

6- Les sentiments

L'ingénierie sociale exploite vos émotions pour vous manipuler :

- **Urgence** : Messages qui créent un sentiment de panique ou d'urgence
- **Empathie** : Demandes d'aide de personnes prétendant être en difficulté
- **Curiosité** : Informations intrigantes qui vous poussent à en savoir plus
- **Peur** : Menaces ou alertes concernant vos comptes ou appareils

Ces techniques visent à court-circuiter votre réflexion rationnelle et à vous faire agir impulsivement, sans vérifier la légitimité de la demande.

⚠ Prenez toujours le temps de vérifier l'authenticité des messages urgents ou émotionnels, même s'ils semblent provenir d'un ami ou d'un proche.

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Réaction appropriée face à un piratage

Pensez-vous que la réaction des deux personnes piratées dans la vidéo ci-dessous, extraite d'une série télévisée américaine, est appropriée ?

https://www.youtube.com/watch?v=u8qgehH3kEQ&t=50s

Cette scène humoristique montre une réaction inefficace face à un piratage : taper à deux sur un clavier n'aide pas à contrer une attaque informatique ! Dans la réalité, il faut déconnecter l'appareil du réseau, contacter un professionnel et suivre un protocole de sécurité précis.

Voici quelques mesures pour assurer la sécurité de vos données et de vos appareils

- [ ] **Installer un antivirus**

  Protégez votre ordinateur ou vos appareils mobiles avec un logiciel antivirus fiable et à jour

- [ ] **Éviter les sites suspects**

  Ne naviguez que sur des sites de confiance, reconnaissables par le "https://" et l'icône du cadenas

- [ ] **Utiliser des réseaux sécurisés**

  Privilégiez les réseaux wifi privés et sécurisés plutôt que les réseaux publics

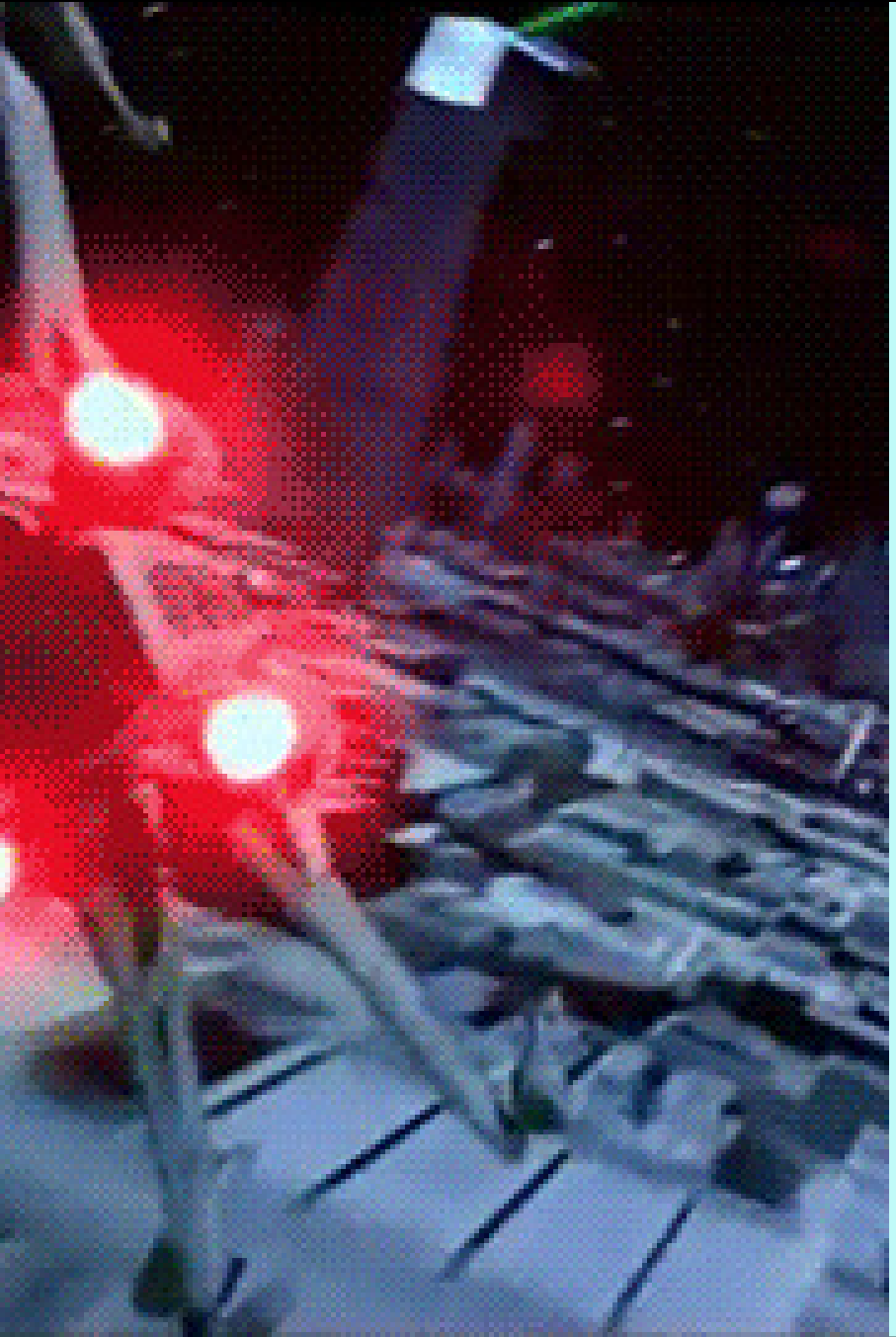
- [ ] **Être vigilant avec les emails**

  Ne répondez pas aux mails suspects et ne cliquez pas sur leurs liens ou pièces jointes

Protégez vos données personnelles en évitant de les partager inutilement et faites des sauvegardes régulières de vos fichiers importants sur un support externe ou un service cloud fiable.

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département



Comment protéger ses appareils des attaques ?

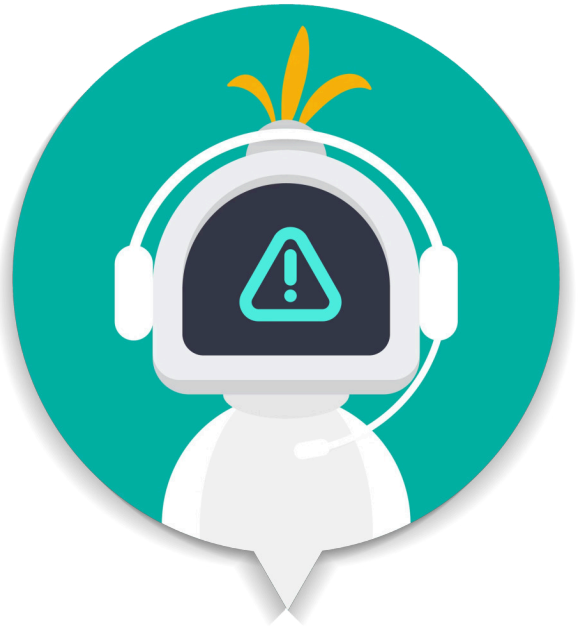
La protection de vos appareils numériques nécessite une approche globale combinant des outils de sécurité, des comportements prudents et une maintenance régulière.

Dans les prochaines diapositives, nous examinerons en détail les principales mesures de protection à adopter, à commencer par l'utilisation d'un antivirus et les mises à jour régulières de vos systèmes.

L'antivirus, pourquoi faire?

L'antivirus est comparable à une ceinture de sécurité pour votre appareil numérique :

- Il détecte et neutralise les programmes malveillants avant qu'ils ne causent des dommages
- Il analyse en permanence les fichiers et programmes que vous utilisez
- Il vérifie les sites web que vous visitez pour identifier les menaces potentielles
- Il vous alerte en cas d'activités suspectes sur votre appareil



Bon à savoir : Windows 10 et 11 incluent un antivirus gratuit appelé Windows Defender, qui est automatiquement intégré dans tous les ordinateurs équipés de ces systèmes d'exploitation.

Important : N'installez qu'un seul antivirus à la fois. L'utilisation simultanée de plusieurs antivirus peut ralentir votre système et créer des conflits.

Les mises à jour

Pourquoi les mises à jour sont essentielles

Les mises à jour ne sont pas qu'une simple formalité, elles sont cruciales pour votre sécurité :

- Elles corrigent les failles de sécurité découvertes par les développeurs
- Elles améliorent la protection contre les nouvelles menaces
- Elles optimisent les performances de vos appareils

Types de mises à jour

- **Mises à jour critiques** : Corrigent les failles de sécurité (gratuites)
- **Mises à jour de version** : Ajoutent des fonctionnalités (parfois payantes)

Configurez vos appareils pour installer automatiquement les mises à jour de sécurité et vérifiez régulièrement les mises à jour disponibles pour tous vos logiciels.

Quels sont les réflexes à adopter sur internet ?

Vérifier l'authenticité des sites

Avant de saisir vos informations personnelles, assurez-vous que le site est légitime (https://, cadenas, absence de fautes d'orthographe)

Utiliser des mots de passe robustes

Créez des mots de passe uniques et complexes pour chaque compte, et changez-les régulièrement

Limiter le partage d'informations

Ne partagez que les informations strictement nécessaires et vérifiez régulièrement les paramètres de confidentialité de vos comptes

Se déconnecter après chaque session

Particulièrement sur les ordinateurs partagés ou publics, déconnectez-vous toujours de vos comptes

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

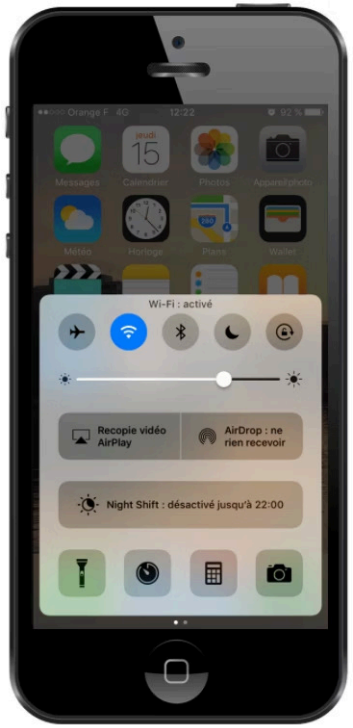
L'achat sur internet

Dans cet exercice, vous êtes chargé(e) d'analyser le comportement en ligne de Thibault lors de son achat d'un article sur Amazon, afin de déterminer s'il présente des risques pour sa sécurité ou s'il est sécurisé.

Nous allons suivre pas à pas les actions de Thibault pour identifier les potentiels risques de sécurité qu'il prend durant son processus d'achat en ligne.

L'achat sur internet

La connexion au réseau wifi public

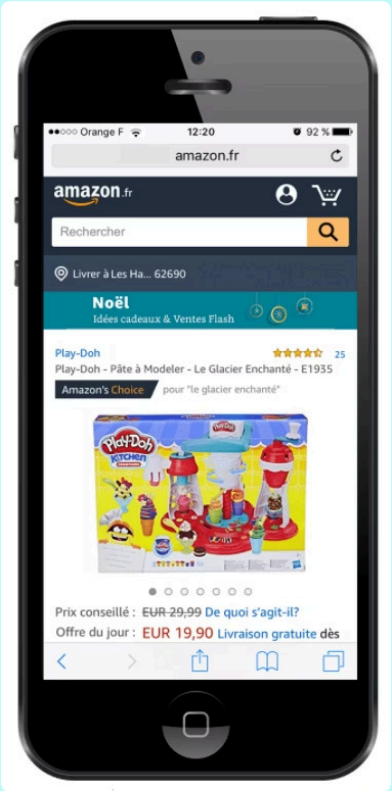


Thibault se trouve à l'aéroport d'Orly. Il connecte son téléphone sur le réseau wifi public de l'aéroport.

⚠ **Premier risque identifié :** Se connecter à un réseau wifi public dans un lieu très fréquenté comme un aéroport présente un risque élevé. Ces réseaux sont souvent non sécurisés et peuvent être facilement exploités par des pirates pour intercepter les données qui y transitent.

L'achat sur internet

La navigation sur le site Amazon

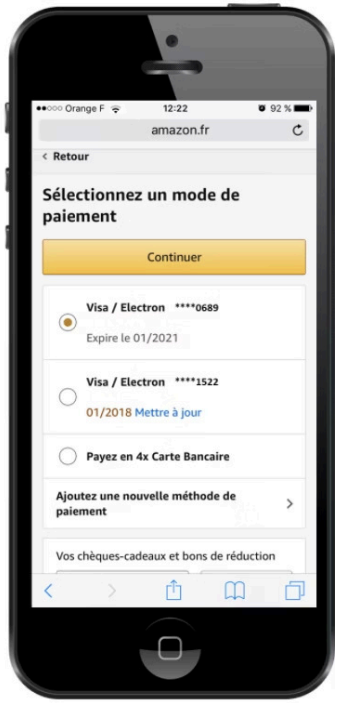


Thibault veut acheter un jeu pour son fils. Il se rend sur le site Amazon et sélectionne l'article de son choix car il se sent coupable de partir dans un hôtel de luxe aux Caraïbes pour donner un atelier numérique.

Deuxième risque identifié : Il ne vérifie pas si le site est sécurisé. En observant l'adresse du site, on ne voit pas le "https://" ni l'icône du cadenas, ce qui indique que la connexion n'est pas chiffrée. Cela signifie que toutes les informations échangées entre son navigateur et le site peuvent être interceptées.

L'achat sur internet

Le paiement en ligne



Thibault achète l'article et renseigne ses coordonnées bancaires...

Cette étape est particulièrement risquée car :

- Il est toujours connecté à un réseau wifi public non sécurisé
- Le site n'utilise pas de connexion chiffrée (pas de https)
- Il entre des données bancaires sensibles dans ces conditions

⚠ **Troisième risque identifié :** Thibault entre ses coordonnées bancaires sur un site non sécurisé tout en étant connecté à un réseau public. C'est une combinaison extrêmement risquée qui pourrait entraîner un vol de ses données bancaires.

L'achat sur internet

La confirmation de l'achat

Thibault a bien commandé son article, il vient de recevoir un mail de confirmation. Il est vraiment content car cet achat va atténuer la peine du petit garçon qui rêvait de soleil.

L'achat est terminé, mais Thibault a pris plusieurs risques importants durant ce processus. Voyons à la diapositive suivante quels étaient ces risques et comment il aurait pu les éviter.

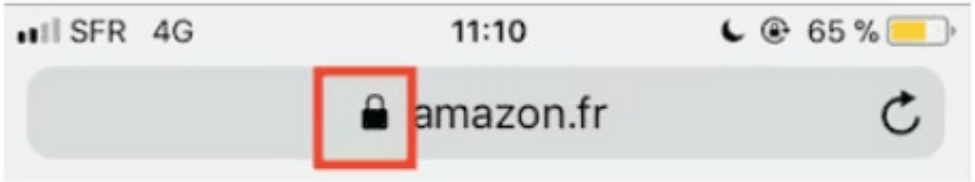
L'achat sur internet

D'après-vous, Thibault a-t-il pris des risques durant son achat en ligne ? Si oui, pourquoi ?

Thibault prend le risque que ses coordonnées bancaires soient interceptées par un pirate, et ce pour deux raisons principales :

1. **Utilisation d'un réseau wifi public** : Il a effectué une transaction bancaire en utilisant un réseau wifi public, qui est plus vulnérable aux attaques. Il aurait dû utiliser sa connexion mobile (4G/5G) ou attendre d'être sur un réseau privé et sécurisé.
2. **Site non sécurisé** : Il n'a pas vérifié la fiabilité du site, comme l'indique l'absence de cadenas et de "https" dans l'adresse URL. Les données transmises peuvent être facilement interceptées.

De plus, il aurait dû désactiver la connexion automatique au wifi et la géolocalisation lorsqu'il était à l'extérieur, pour préserver sa sécurité et économiser la batterie.



LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS
Loiret votre Département

Bonjour

Aprés les dernieres calculs de vos impots sur le revenus nous avons déterminé que vous étes admissible

a recevoir un rembouresement d'impots de 150 euro.

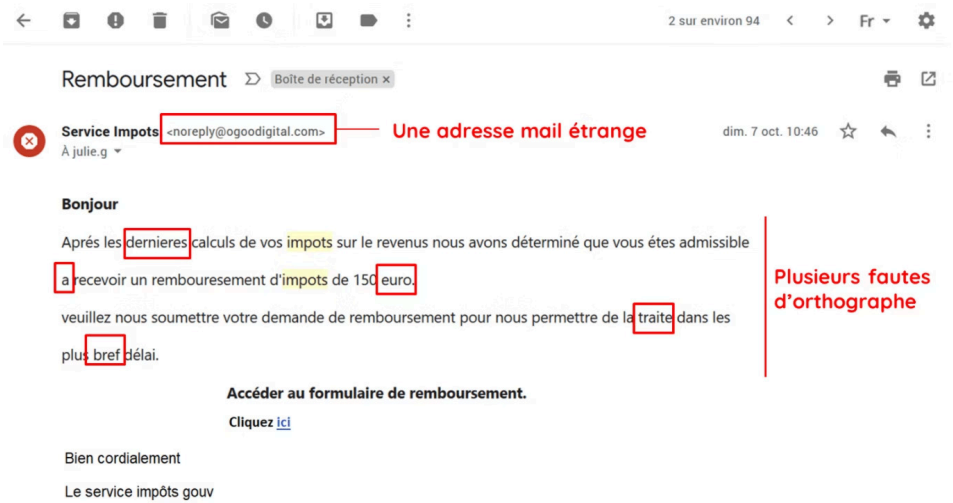
veuillez nous soumettre votre demande de remboursement pour nous permettre de la traite dans les

Comment reconnaître les mails et SMS malveillants ?

Ce mail est-il fiable ?

Analysons ensemble ce message pour déterminer s'il présente des signes de tentative d'hameçonnage (phishing).

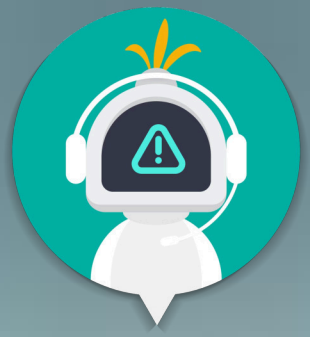
Comment reconnaître les mails et SMS malveillants ?



Ce mail n'est **pas sécurisé** et plusieurs indices le prouvent :

- L'offre proposée est **trop belle pour être vraie** : un iPhone gratuit sans condition est hautement improbable
- L'**adresse mail de l'expéditeur** est inconnue et ne correspond pas à une organisation officielle
- Il y a des **fautes d'orthographe** dans le contenu du mail, signe typique de phishing
- Le mail vous demande de **cliquer sur un lien** pour renseigner des informations personnelles

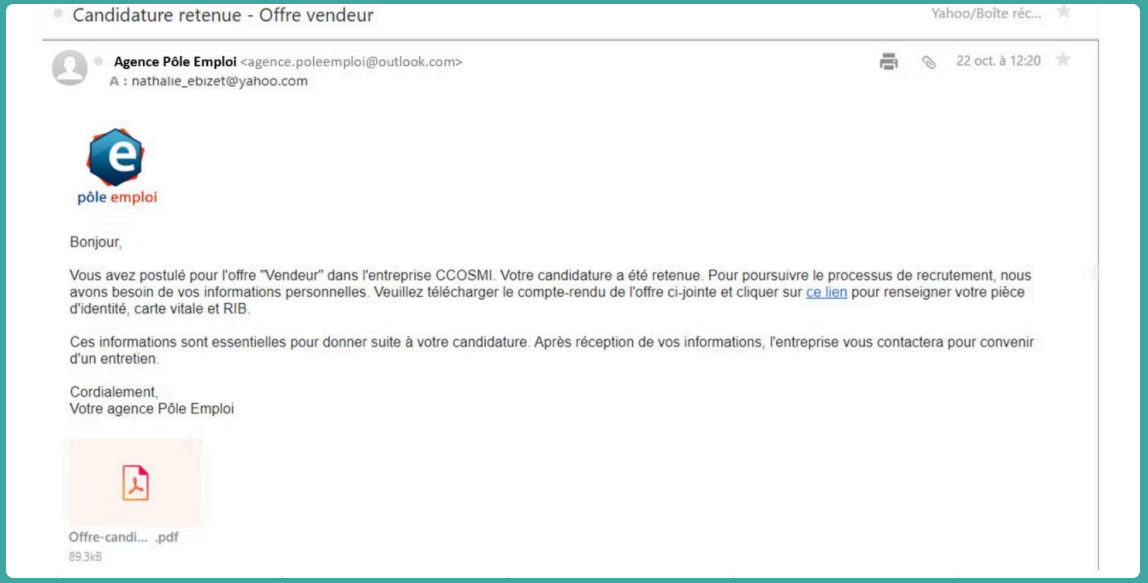
Une astuce pour vérifier si un lien est fiable : passez la souris dessus sans cliquer. L'adresse réelle du site apparaîtra, vous permettant de vérifier si elle correspond à un site légitime.



Comment reconnaître les mails et SMS malveillants ?

Ce nouveau mail est-il fiable ?

Examinons ce mail qui semble provenir de Pôle Emploi pour déterminer s'il présente des signes de tentative d'hameçonnage.



Candidature retenue - Offre vendeur

Yahoo/Boîte réc...

Agence Pôle Emploi <agence.poleemploi@outlook.com>
A : nathalie_ebizet@yahoo.com

22 oct. à 12:20

pôle emploi

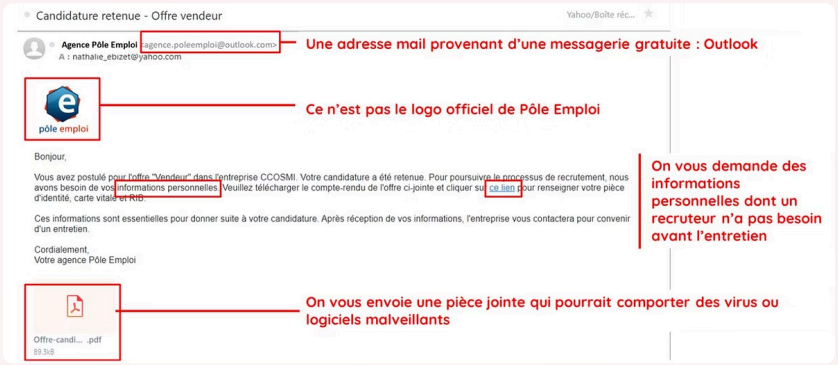
Bonjour,

Vous avez postulé pour l'offre "Vendeur" dans l'entreprise CCOSMI. Votre candidature a été retenue. Pour poursuivre le processus de recrutement, nous avons besoin de vos informations personnelles. Veuillez télécharger le compte-rendu de l'offre ci-jointe et cliquer sur ce lien pour renseigner votre pièce d'identité, carte vitale et RIB.

Ces informations sont essentielles pour donner suite à votre candidature. Après réception de vos informations, l'entreprise vous contactera pour convenir d'un entretien.

Cordialement,
Votre agence Pôle Emploi

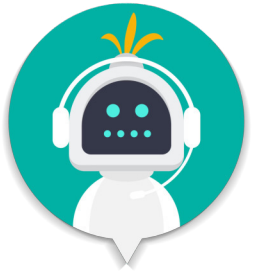
Offre-candi... .pdf
89.3kB



Comment reconnaître les mails et SMS malveillants ?

Ce mail n'est **pas sécurisé** et plusieurs indices le prouvent :

1. L'adresse mail de l'expéditeur provient d'une messagerie gratuite (Outlook), ce qui est inhabituel pour une organisation officielle comme Pôle Emploi
2. Le logo présent n'est pas le logo officiel de Pôle Emploi
1. Les informations personnelles demandées dans le mail ne sont pas nécessaires pour qu'un recrutement soit validé
2. Le lien et la pièce jointe contenus dans le mail sont probablement dangereux et pourraient contenir des logiciels malveillants



Les institutions officielles comme Pôle Emploi utilisent leurs propres domaines email (@pole-emploi.fr) et ne vous demanderont jamais de communiquer des informations sensibles par email.

Comment reconnaître les mails et SMS malveillants ?

Le "Phishing" ou "Hameçonnage"

Les deux exemples précédents concernent des tentatives de "Phishing" qui est une technique couramment utilisée par les pirates.

Cette méthode consiste à se faire passer pour une entreprise ou une organisation fiable dans le but de duper l'utilisateur pour obtenir des informations personnelles, notamment des données bancaires.

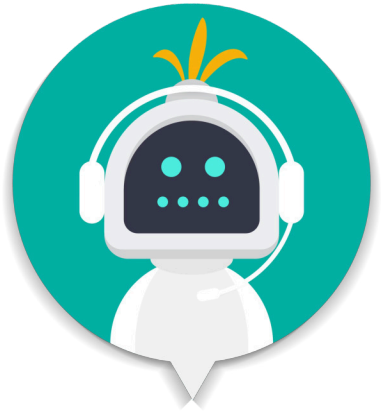
Comment s'en protéger :

- Vérifiez toujours l'adresse email de l'expéditeur (méfiez-vous des domaines @gmail, @outlook, etc.)
- Soyez méfiant si on vous demande des informations personnelles sans raison valable
- N'ouvrez jamais les pièces jointes de source douteuse
- Ne cliquez pas sur les liens suspects dans les emails

Comment reconnaître les mails et SMS malveillants ?

Ce nouveau mail est-il fiable ?

Ce mail semble provenir d'un ami. Est-ce pour autant fiable ? Analysons-le ensemble.



LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

URGENT

Sabrina Adebis <sabedis@gmail.com> 13:55 (Il y a 0 minute)

À nathalie_ebizet

Bonjour Nathalie

Je t'écris parce que j'ai vraiment besoin de ton aide, c'est urgent. Mon entreprise est en faillite, je n'ai plus de travail et j'ai vraiment besoin d'argent pour nourrir les enfants... C'est horrible, je ne vais pas m'en sortir sans ton aide. Bientôt je vais devoir quitter notre logement et dormir dehors. Réponds-moi s'il te plaît.

Merci
Sabrina

Comment reconnaître les mails et SMS malveillants ?

Il est important de ne pas considérer qu'un mail est sécurisé uniquement parce que l'adresse de l'expéditeur vous est familière.

Pourquoi ce mail est suspect :

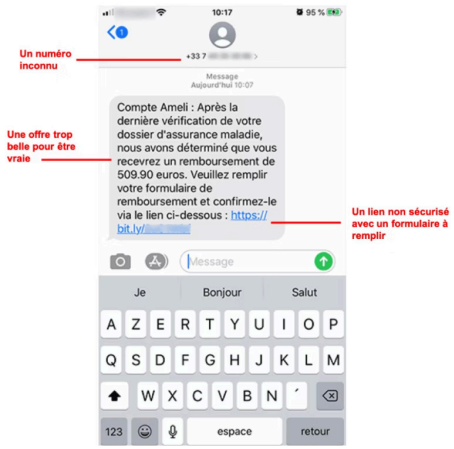
- Votre ami peut être victime d'un piratage de compte
- Le message demande de l'argent en urgence, un scénario classique d'arnaque
- L'histoire semble dramatisée pour provoquer une réaction émotionnelle
- La demande d'un virement urgent est particulièrement suspecte

Comment réagir :

Contactez votre ami par un autre moyen (téléphone, autre messagerie) pour vérifier la légitimité de la demande avant d'envoyer de l'argent.

Comment reconnaître les mails et SMS malveillants ?

Ce nouveau SMS est-il fiable ?



Il est important d'être vigilant face aux SMS frauduleux. Plusieurs indices indiquent que ce SMS n'est pas sécurisé :

Le message propose un remboursement important sans aucune raison valable

Le message vous incite à cliquer sur un lien inconnu et à remplir un formulaire avec vos informations personnelles

Le numéro de l'expéditeur est inconnu et ne correspond pas à un service officiel

Le message utilise des prétextes d'urgence pour vous inciter à réagir rapidement sans réfléchir

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

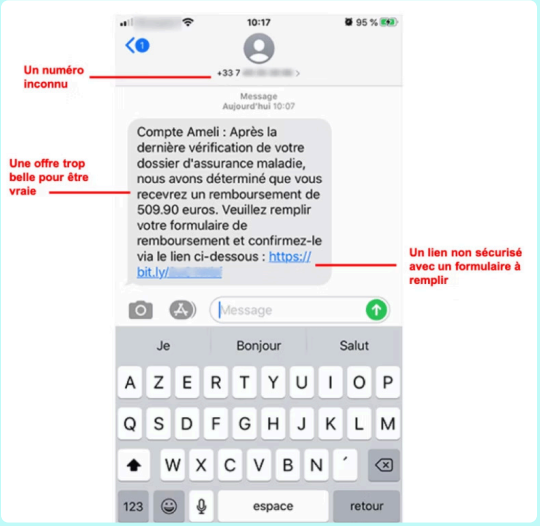
Comment reconnaître les mails et SMS malveillants ?

Les SMS frauduleux (smishing) utilisent souvent des prétextes courants :

- **Remboursements** : Impôts, Sécurité Sociale, banques...
- **Gains** : Loteries, concours que vous n'avez jamais joué
- **Urgences** : Messages alarmants nécessitant une action immédiate
- **Colis** : Livraisons en attente, frais supplémentaires à payer
- **Comptes bloqués** : Banques, réseaux sociaux, services en ligne

Ces messages exploitent souvent :

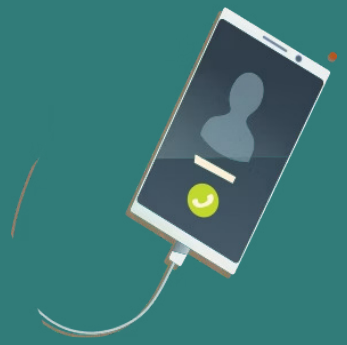
- L'urgence : "Dernière chance", "Sous 24h"
- L'appât du gain : "Remboursement", "Vous avez gagné"
- La peur : "Compte bloqué", "Fraude détectée"



⚠ Ne cliquez **jamais** sur les liens contenus dans ces SMS suspects et ne répondez pas à ces messages. Si vous avez un doute sur un message qui semble provenir d'un service officiel, contactez directement l'organisation par ses canaux officiels.

C'est l'heure du Quizz

Testons vos connaissances sur la sécurité en ligne avec ce quiz interactif. Chaque question porte sur un aspect important de la cybersécurité que nous avons abordé dans cette présentation.



Images : freepik

Comment un virus ou un logiciel malveillant peut-il infiltrer votre ordinateur ?

Par mail, si je télécharge une pièce jointe malveillante

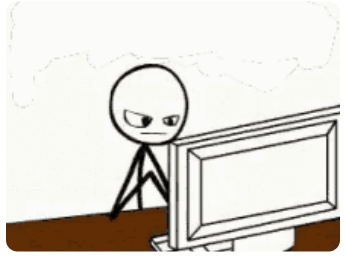
Si je télécharge un logiciel ou un fichier sur un site internet non sécurisé

Si je publie une photo sur Facebook

Si je consulte une publicité sur Youtube

Réponse :

Un virus ou logiciel malveillant peut pénétrer votre ordinateur via le téléchargement d'un fichier ou logiciel, sur un site ou par mail. Publier une photo ou consulter une publicité n'entraînera pas de virus, par contre ces données de navigation peuvent être utilisées par les entreprises à des fins commerciales.



LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Si un virus pénètre mon ordinateur, que peut-il se passer ?

- Mon ordinateur peut exploser
- Mon ordinateur peut devenir plus lent
- Mon ordinateur peut devenir moins performant
- Je risque de perdre des fichiers personnels enregistrés dans mon ordinateur (photos, vidéos...)

Réponse :

Votre système informatique va se détériorer progressivement : il deviendra plus lent, moins performant... Certaines fonctions et fichiers peuvent être supprimés : veillez donc à enregistrer vos données personnelles sur une clé USB, un disque dur externe, ou un espace de stockage en ligne.

Un ordinateur n'explosera pas physiquement à cause d'un virus - c'est un mythe souvent véhiculé dans les films !

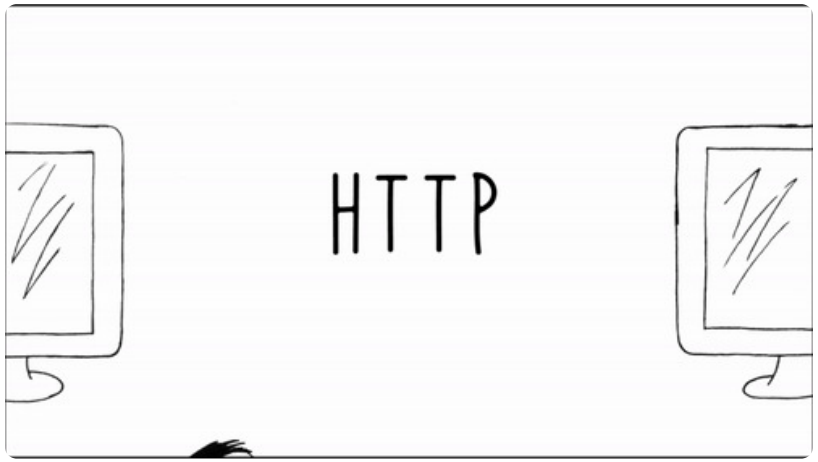
À quoi reconnait-on que les données d'un site sont cryptées ?

Son adresse commence par **http**	Son adresse commence par **https**	Son adresse commence par **www**

Réponse :

On reconnaît qu'un site internet est sécurisé quand son adresse - aussi appelée URL - commence par **https**. Le **S** signifie **sécurisé** !

Le préfixe "http" indique une connexion non chiffrée, tandis que "www" est simplement une convention de nommage qui ne garantit pas la sécurité. Recherchez toujours le cadenas dans la barre d'adresse en plus du "https".



LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

L'adresse web http://impogouv.fr est-elle sécurisée ?

Oui

Non

Réponse :

Non, cette adresse n'est pas sécurisée. On le remarque grâce à deux indices importants :

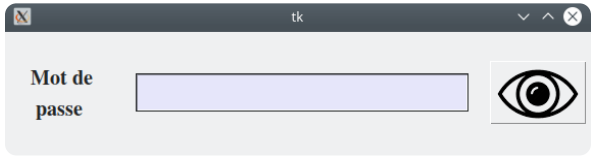
1. Il manque le "S" après http, ce qui indique que la connexion n'est pas chiffrée
2. Il y a une faute d'orthographe dans l'adresse : "impogouv" au lieu de "impots.gouv"

Cette combinaison d'indices révèle une tentative de phishing visant à imiter le site officiel des impôts. Le véritable site des impôts est **https://www.impots.gouv.fr**

De quoi un mot de passe sécurisé est-il nécessairement composé ?

- Chiffres
- Lettres
- Caractères spéciaux
- Un arobase @

Réponse :



Un mot de passe sécurisé doit être composé de **chiffres**, **lettres**, et **caractères spéciaux**. Il n'est pas obligatoire d'utiliser spécifiquement l'arobase (@) - n'importe quel caractère spécial (!, #, $, %, &, *, etc.) peut contribuer à la sécurité du mot de passe.

Pour une sécurité optimale, votre mot de passe devrait également :

- Comporter au moins 12 caractères
- Mélanger majuscules et minuscules
- Être unique pour chaque service
- Être régulièrement changé

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

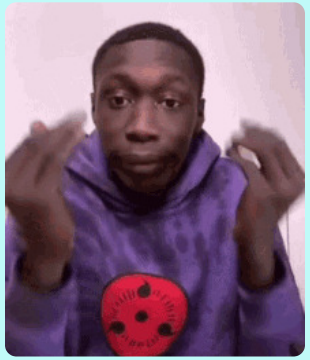
Lesquelles de ces affirmations sont vraies ?

Il faut toujours se déconnecter de ses comptes en ligne avant de quitter un ordinateur public ou partagé avec d'autres.

Il ne faut pas utiliser le réseau wifi public pour faire des achats en ligne.

Il faut utiliser des mots de passe courts et faciles à retenir.

Réponse :



Les deux premières affirmations sont vraies :

- Il est essentiel de se déconnecter de ses comptes en ligne sur un ordinateur partagé pour éviter que d'autres personnes n'accèdent à vos informations
- Il faut éviter d'utiliser des réseaux wifi publics pour les transactions sensibles, car vos informations pourraient être interceptées

La troisième affirmation est fausse : les mots de passe courts et faciles à retenir sont également faciles à pirater. Pour être sécurisé, un mot de passe doit être long et complexe.

Que pensez-vous de l'affirmation suivante : "Quand je reçois un mail provenant de l'adresse mail d'un ami, alors c'est forcément mon ami qui l'a écrit"

C'est faux : mon ami peut s'être fait pirater

C'est vrai : si l'adresse mail est exactement celle de mon ami, c'est forcément lui qui a écrit

Réponse :

C'est **faux**. Sur internet, méfiez-vous même des messages qui semblent provenir de vos amis :

- Le compte email de votre ami peut avoir été piraté
- L'adresse email peut être usurpée pour ressembler à celle de votre ami
- Un pirate peut avoir créé une adresse très similaire avec une légère modification

Si vous recevez un message inhabituel de la part d'un ami (demande d'argent, liens suspects), contactez-le par un autre moyen pour vérifier qu'il en est bien l'auteur.

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département

Imaginez que vous receviez un mail suspect : on vous demande de renseigner vos données bancaires pour bénéficier d'une offre exceptionnelle. Que pouvez-vous faire ?

Cliquer sur le lien proposé dans le mail pour vérifier que l'offre est réelle	Passer ma souris sur le lien pour découvrir l'adresse web qui s'y cache	Répondre au mail en posant des questions plus précises sur l'offre

Réponse :

La bonne réponse est de **passer votre souris sur le lien sans cliquer** pour voir l'adresse réelle qui s'y cache. Cela vous permettra de vérifier si le lien mène vers un site légitime ou une tentative de phishing.

Si le mail est suspect, vous ne devez **jamais** :

- Cliquer sur les liens ou télécharger les pièces jointes - ils pourraient contenir des logiciels malveillants
- Répondre au message - cela confirme que votre adresse email est active
- Fournir des informations personnelles ou bancaires

La meilleure action reste de supprimer immédiatement ce type de message suspect.

Merci d'avoir suivi cet atelier et de votre attention

Nous espérons que cette présentation vous a permis de mieux comprendre les risques liés à l'utilisation d'Internet et d'acquérir les compétences nécessaires pour vous protéger efficacement en ligne.

Protégez vos appareils

Utilisez un antivirus à jour et effectuez régulièrement des mises à jour de sécurité

Sécurisez vos comptes

Créez des mots de passe robustes et uniques pour chacun de vos comptes en ligne

Restez vigilant

Méfiez-vous des messages suspects et vérifiez toujours la légitimité des demandes d'information

LE NUMÉRIQUE POUR TOUS LES LOIRÉTAINS

Loiret votre Département