Par les animateurs de la médiathèque

Sécurité Numérique pour les nuls



Conférence
Le 10 juin 2025

14h00 – 16h00

Inscription obligatoire

Protéger ses données, protéger ses appareils et se protéger soi-même vis-à-vis des risques du numérique.

Ce document est la copie des diapositives présentées en conférence. Vous pouvez contrôler le défilement des diapositives, en cliquant sur les symboles, ci-dessous, pour aller vers des explications détaillées, des illustrations complémentaires.
Ce principe est particulièrement utile dans la section Réagir, pour aller directement sur le traitement des risques qui vous importent.

Pour aller

Pour revenir

Sommaire, qu'allons nous voir ?



La sécurité et le numérique

Page suivante



Comment identifier les vulnérabilités, les menaces, les risques du numérique



Réagir en fonction de risques avérés



Comment se protéger avec une bonne hygiène numérique

Cliquez sur ces symboles pour aller au chapitre choisi ou faites défiler les diapos dans l'ordre

La sécurité numérique ?



Elle concerne nos biens personnels:

Matériels, monétaires, données…

Mais aussi ce que nous sommes:

Identité, sensibilité, réputation…

Elle concerne nos biens collectifs:

Fonctionnement de nos associations, entreprises, services de l'état,

Et aussi l'utilisation de notre personne à notre insu, notre instrumentalisation pour servir des causes partisanes.

Principes généraux de la sécurité

Au-delà de la sécurité de nos personnes,

Nous avons des biens (matériels, immatériels)

Les accès à nos biens peuvent avoir des vulnérabilités

Susceptibles d'être exploitées(menaces)

Par des attaquants

➔ Nous encourons des risques

➔Quand ils sont avérés, ce sont des dommages / sinistres

Sans oublier les causes accidentelles et les pannes !

Nos biens informatiques à sécuriser

Environnement informatique local

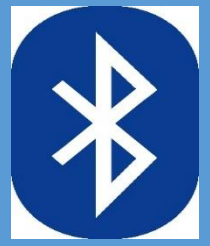


Connexions physiques









Ressources matérielles:
Ecran, clavier, souris, mémoire, disque dur, …

Logiciels:
Système d'exploitation,
Navigateur internet, autres ….

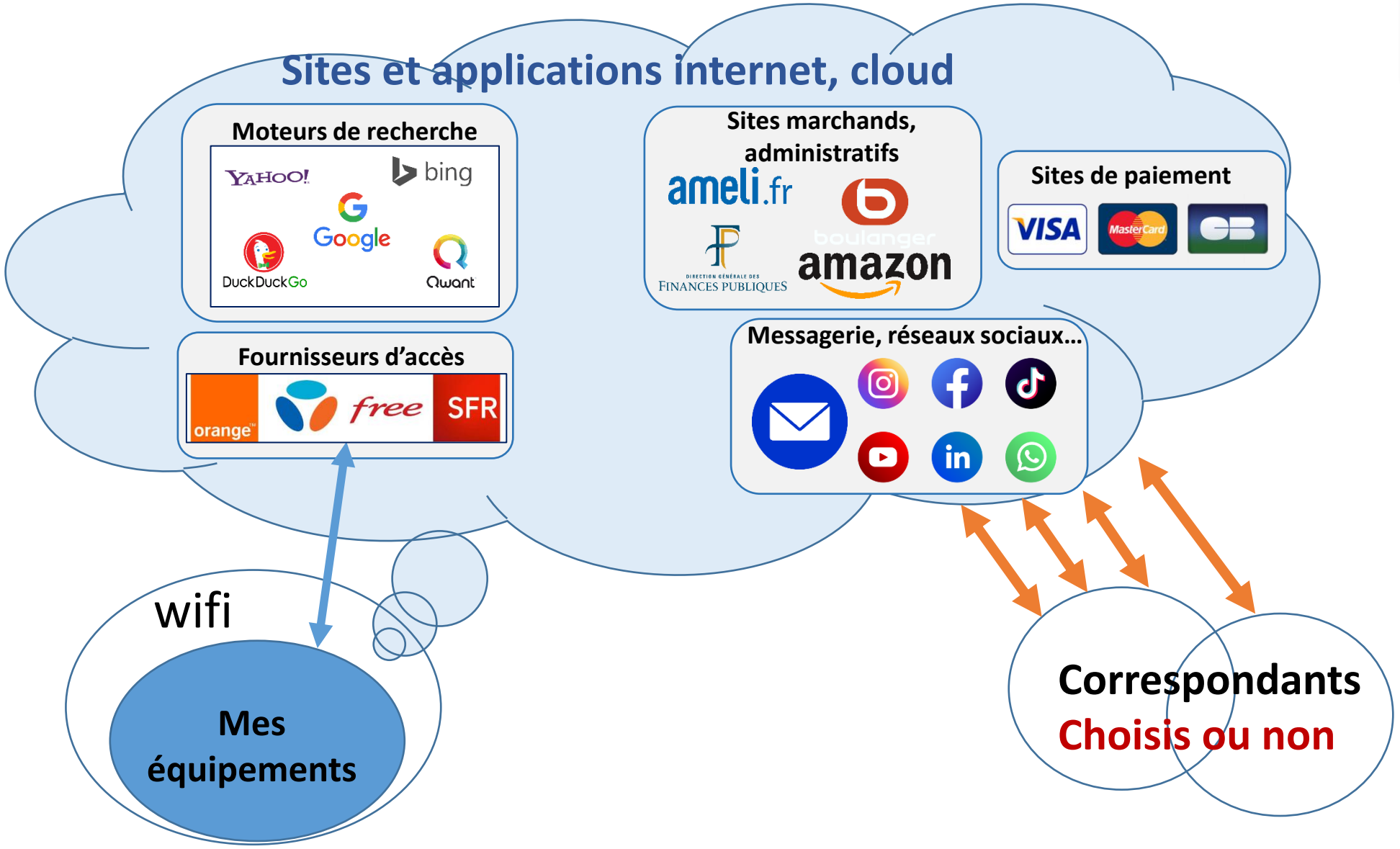
Fichiers,
Images, vidéo, audio, …
Données personnelles

Notre équipement informatique principal





Environnement informatique avec internet



Les données personnelles

- **Constitutives d'une identité**
  - Nom, prénoms, date et lieu de naissance, parents, adresse
  - Identifiants: N° sécurité sociale, Impôts, comptes, …
  - Mots de passe, codes secrets
- **Caractérisant une personne:**
  - Photos,
  - Religion, appartenance politique, préférences sexuelles ou autres, …
  - Gouts, opinions, correspondances, …
  - Navigations internet
- **Localisation**
- **Données relatives à d'autres personnes**
  - Émetteurs, destinataires de mes courriers, contacts, …
  - Amis, « followers » de réseaux sociaux





diplômes,
données RH
email pro, fonction



salaires
impôts, charges
transactions commerciales



Les données personnelles dites « sensibles »

ce qui prouve notre identité

Etat-civil, adresses

qui on fréquente

Contacts / Réseaux



où on se trouve

Coordonnées géographiques

les traces qu'on laisse

Traces numériques

ce qui se dit de nous

Réputation

ce qu'on est et ce qu'on aime

Idées, opinions, préférences, et centres d'intérêts

Où laisse-t-on des informations ?



- De manière plus ou moins protégée dans ses matériels
- Chez son fournisseur d'accès internet,
- Dans un moteur de recherche
- Sur les sites internet visités
- Sur les réseaux sociaux et messageries
  - **Et les copies qui peuvent en être faites, on ne sait où !!!**

Quelles informations laisse-t-on sur Internet?

- **Volontairement:**
  - Comptes, en remplissant des formulaires
  - Mots clés de recherche
  - Messagerie
- **A notre insu, ou presque:**
  - Géolocalisation
  - Préférences, clics, « likes », …





- **Accès autorisés ou non à nos ressources locales**
  - Webcam, photos,
  - Prise de contrôle de notre équipement

Internet introduit des informations dans notre informatique

- A notre demande, téléchargements:
  - Logiciels gratuits ou payants
  - Images, vidéos, musique,
  - Documents, …
- A notre insu:
  - Les cookies
  - Logiciels malveillants



Légaux ou pas !!!



Fin de la section
Cliquer pour revenir au sommaire, si souhaité

Vulnérabilités, menaces, risques



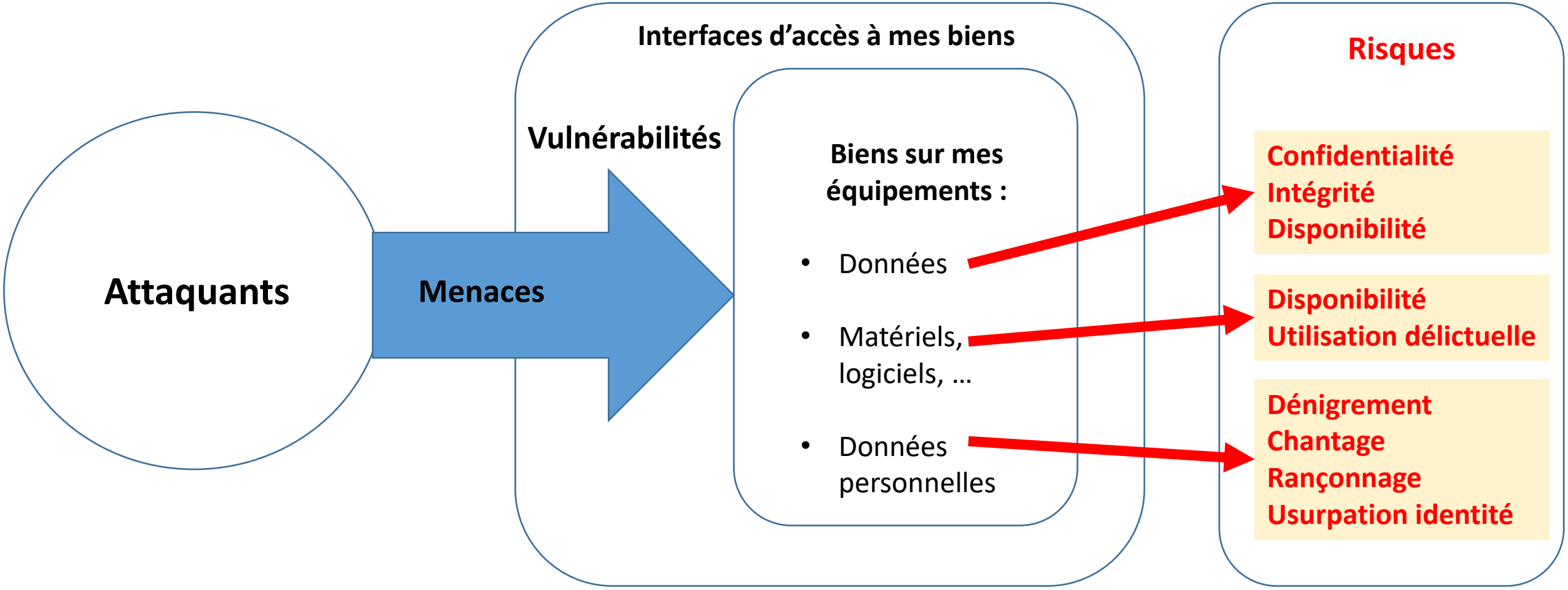
La plus grande des vulnérabilités



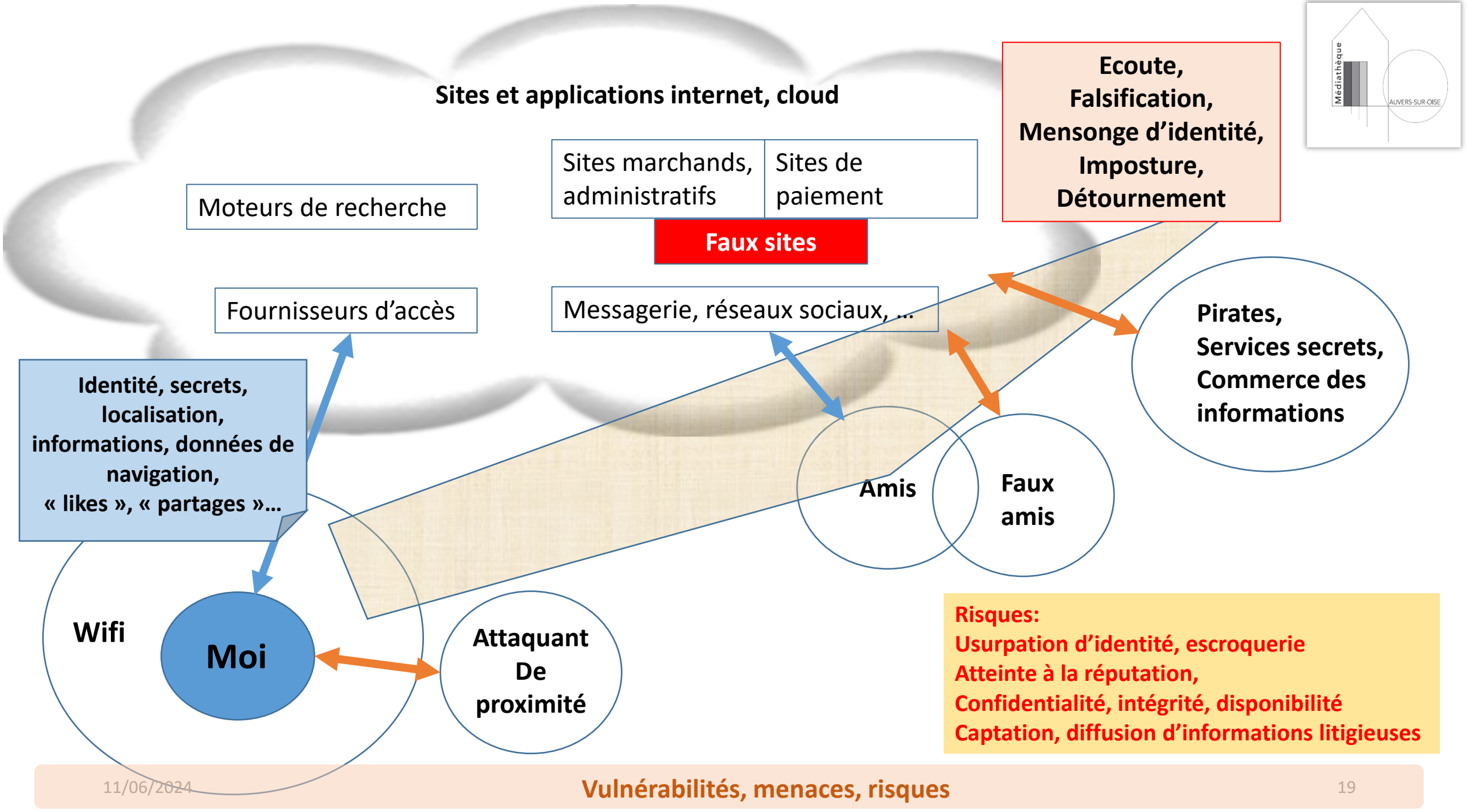
La fragilité humaine !

- **De personnes vulnérables,**
- **Mais aussi de tout un chacun à un moment ou à un autre !**

Risques de sécurité pour nos biens informatiques



Les solutions résident dans la réduction des vulnérabilités : précautions comportementales, protections informatiques


Sites et applications internet, cloud
Ecoute,
Falsification,
Mensonge d'identité,
Imposture,
Détournement
Sites marchands, administratifs
Sites de paiement
Moteurs de recherche
Faux sites
Fournisseurs d'accès
Messagerie, réseaux sociaux, …
Identité, secrets, localisation, informations, données de navigation, « likes », « partages »…
Pirates,
Services secrets,
Commerce des informations
Amis
Faux amis
Wifi
Moi
Attaquant De proximité
Risques:
Usurpation d'identité, escroquerie
Atteinte à la réputation,
Confidentialité, intégrité, disponibilité
Captation, diffusion d'informations litigieuses

Les vulnérabilités techniques

- Les pannes matérielles
- Les défauts logiciels (bugs)
- Les « failles sécuritaires » des logiciels
- Des supports USB contaminés
- La sécurité insuffisante de réseaux
  - **Notamment les Wifi publics.**



Les vulnérabilités d'exploitation

- Mots de passe faibles ou mal protégés
- Les erreurs d'utilisation
- Le paramétrage trop confiant/permissif des logiciels
- Les mises à jour des logiciels non effectuées







Les modes d’attaque 1/2

- Logiciels malveillants:
  - Virus
  - Cheval de Troie (Trojan horse)
  - Logiciel espion (Spyware)
  - Rançongiciel (Ransomware)









Les modes d’attaque 2/2

- Falsification des données



- Mensonge d’identité:
  - Imposture (spoofing)
  - Hameçonnage (phishing)



- Détournement



Le respect de la loi et de l'éthique

- Pas de consultation, création, mise en ligne de:
  - Sites, messages, contenu faisant l'apologie de la violence, de discriminations, de pornographie ou de pratiques illégales…



- Ne pas transférer, ou « liker »



  - Des messages aux contenus susceptibles par leur nature de porter atteinte au respect de la personne humaine et de sa dignité ou d'inciter à la violence politique, raciste ou xénophobe…

Fin de la section
Cliquer pour revenir au sommaire, si souhaité



Réagir

Le tableau de la diapositive suivante liste les risques connus

Les liens vous permettent d'aller vers les diapositives qui exposent :

- **Comment Identifier le danger,**
- **Comment réagir.**

- **Pour revenir au tableau, cliquer sur**

Téléphone et SPAM
SPAM téléphonique
Wangiri
Usurpation de n° de téléphone mobile
SPAM électronique

Harcèlement chantage
Cyberharcèlement
Chantage ordinateur ou webcam piraté
Rançongiciels
Sextorsion

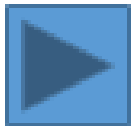
Fraudes escroqueries
Fraude Carte Bancaire
FOVI Faux Ordres de Virement
Faux conseiller bancaire
faux support technique
Escroqueries diverses
Escroqueries plateformes

Hameçonnage - Identité- Données
L'hameçonnage
Fuite, violation de données
Usurpation d'identité
Suppression de données
Propagande Fake News

Piratages
Piratage de compte
Piratage de système
Virus

Les liens vous permettent d'aller vers les diapositives qui exposent :

- **Comment Identifier le danger,**
- **Comment réagir.**
- **Cliquer sur**  **vous fera revenir sur cette diapositive.**

Vers la section « Se protéger » 

LE SPAM TÉLÉPHONIQUE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique



EXTORSION D'ARGENT

Vous recevez des messages ou des appels non sollicités à caractère publicitaire, commercial ou malveillant sur votre téléphone ?
Vous êtes victime de spam téléphonique !

BUT
Vendre des produits ou des services, diffuser une publicité virale, ou une propagande, voler des données personnelles et/ou professionnelles, escroquer financièrement, etc.

TECHNIQUE
Prospection commerciale ou tentative d'escroquerie par messages SMS ou MMS, ou par appel téléphonique.

LE SPAM TÉLÉPHONIQUE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



COMMENT RÉAGIR ?

- En cas d'appels non sollicités, demandez que vos coordonnées soient retirées des fichiers de coordonnées de l'appelant
- En cas de spam téléphonique, signalez-le sur la plateforme 33 700
- Bloquez les SMS indésirables en leur renvoyant le mot « STOP »
- En cas de sollicitation répétée ou abusive, si vous êtes inscrit sur la liste d'opposition Bloctel, adressez-lui une réclamation
- Si vous avez demandé à ne plus être sollicité mais que les appels téléphoniques continuent, déposez plainte auprès de la CNIL
- Si les sollicitations s'apparentent à du harcèlement, déposez plainte

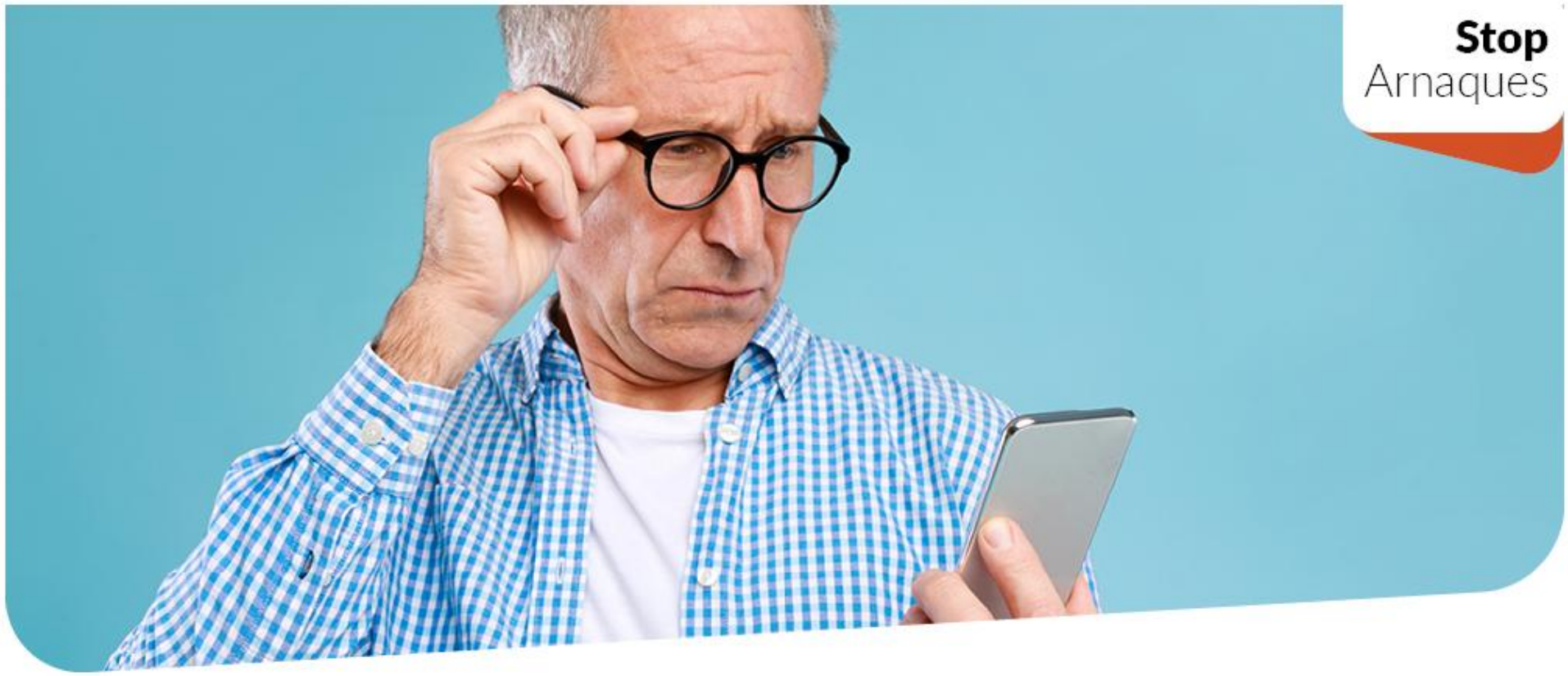
LIENS UTILES

www.33700.fr
ou par SMS 33700

Bloctel
www.bloctel.gouv.fr

CNIL
www.cnil.fr

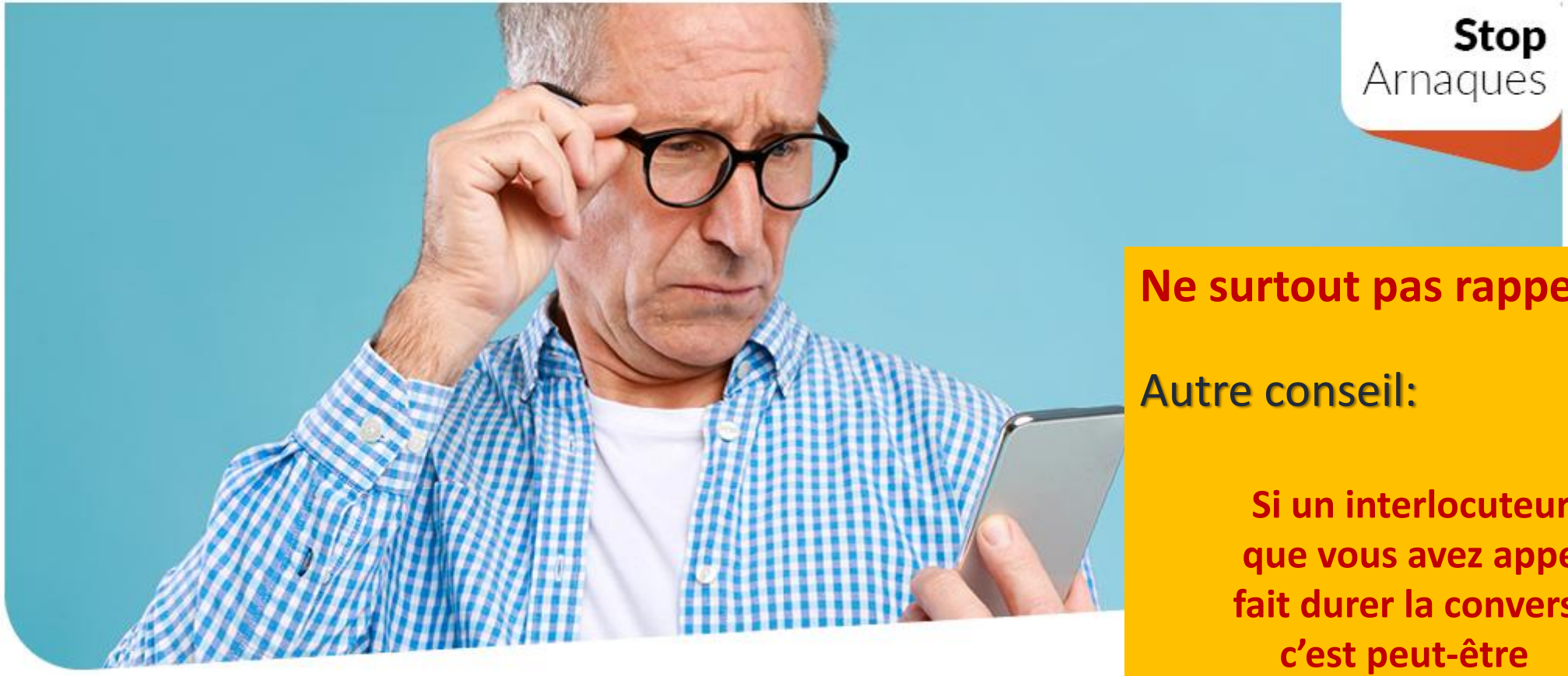
Un numéro étranger vous appelle très brièvement sans laisser de message (fraude Wangiri)



On veut vous faire rappeler un numéro surtaxé en France ou à l'étranger.

Variantes: un message vocal ou SMS vous invite à rappeler le numéro

Un numéro étranger vous appelle très brièvement sans laisser de message (fraude Wangiri)

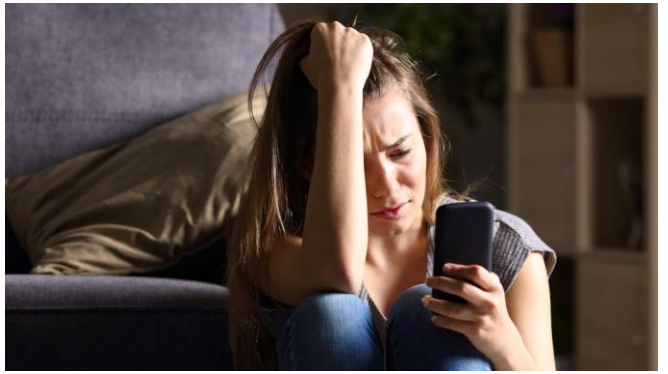


Ne surtout pas rappeler

Autre conseil:

Si un interlocuteur
que vous avez appelé
fait durer la conversation,
c'est peut-être
un numéro surtaxé !

Usurpation de N° de téléphone mobile



L’escroc utilise le numéro usurpé pour masquer son identité.

But recherché

Afficher ce N° comme émetteur de nombreux SMS d'hameçonnage (*smishing*), concernant essentiellement de fausses livraisons de colis.

Réaliser des appels de démarchage commercial illégal, concernant bien souvent des travaux de rénovation énergétique.

- La victime reçoit en retour des actions de l’escroc des réponses, parfois très violentes, de personnes agacées par le message qu'elles ont reçu. Cette nuisance peut être très stressante pour les victimes et durer quelques jours consécutifs.

Depuis le 1er octobre 2024, la loi impose aux opérateurs téléphoniques un mécanisme d'authentification des numéros (MAN) de téléphone fixe. L'extension du mécanisme d'authentification des numéros aux téléphones mobiles est en cours de déploiement début 2025

LE SPAM ÉLECTRONIQUE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



EXTORSION D'ARGENT

Vous recevez des messages électroniques douteux et/ou pour lesquels vous n'avez pas demandé à être sollicité ? Vous êtes victime de spam électronique !

BUT
Vendre des produits ou des services, diffuser une publicité virale, ou une propagande, voler des données personnelles et/ou professionnelles, escroquer financièrement, etc.

TECHNIQUE
Envois de messages en masse sur les boîtes mails, les messageries instantanées ou les réseaux sociaux.

LE SPAM ÉLECTRONIQUE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT RÉAGIR ?



- Si l'émetteur vous semble légitime, cliquez sur le lien de désabonnement ou de désinscription
- Au moindre doute, ne répondez pas, n'ouvrez pas les pièces jointes, ne cliquez pas sur les liens
- Signalez le message douteux sur les sites spécialisés (voir liens utiles)
- Marquez les spams comme « indésirables » ou bloquez les expéditeurs de spams
- Si vous avez demandé à ne plus être sollicité mais que vous continuez à recevoir des spams, déposez plainte auprès de la CNIL

LIENS UTILES

Signal-spam.fr

Info Escroqueries
0 805 805 817 (gratuit)

L'HAMEÇONNAGE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT

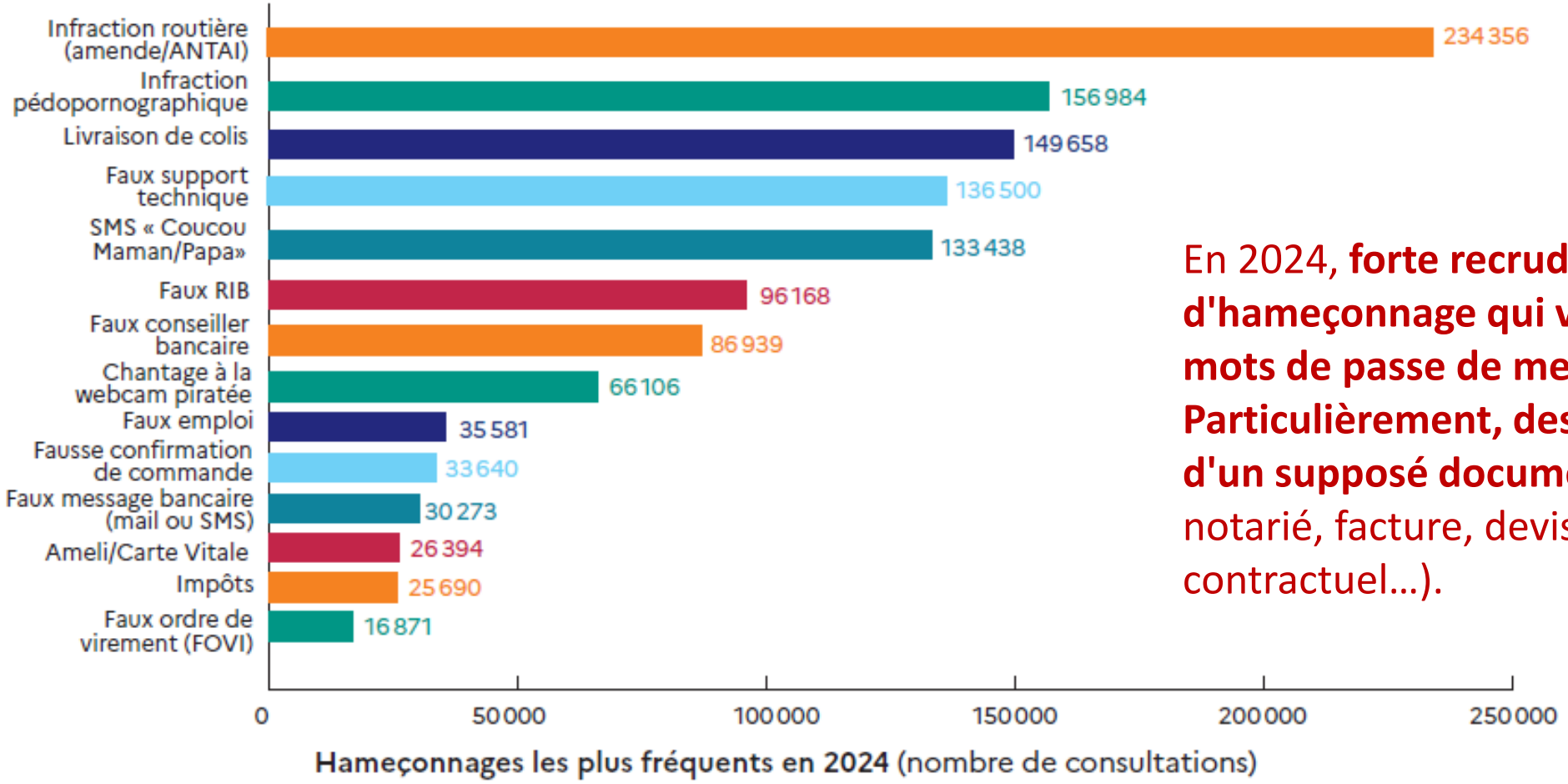
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

SMS, mails, messages privés ou publications sur les réseaux sociaux, messages instantanés, liens sponsorisés et publicités en ligne, appels téléphoniques….

L'hameçonnage est à l'origine de nombreuses autres cybermalveillances



Hameçonnages les plus fréquents en 2024 (nombre de consultations)

En 2024, **forte recrudescence des messages d'hameçonnage qui visent à récupérer des mots de passe de messagerie mail. Particulièrement, des mails qui informent d'un supposé document à télécharger** (acte notarié, facture, devis ou autre document contractuel…).

Réagir

L'HAMEÇONNAGE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir ci-dessous)

LIENS UTILES

Signal-spam.fr

Phishing-initiative.fr

Info Escroqueries
0 805 805 817 (gratuit)

L'HAMEÇONNAGE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

VICTIME



COMMENT RÉAGIR ?

- Ne communiquez jamais d'inf… suite à un message ou un appel téléphoniq…
- Au moindre dout… …tement l'organisme concerné pour confir…
- Faite… …diatement (en cas d'arnaque bancaire)
  …ts de passe divulgués/compromis
  …plainte
  …nalez-le sur les sites spécialisés (voir ci-dessous)

Vérifier l'adresse d'envoi de tout message internet ou autre nous paraissant potentiellement frauduleux , voir à le comparer au site connu qui est sensé le générer

LI… …TILES

Signal-spam.fr

Phishing-initiative.fr

Info Escroqueries
0 805 805 817 (gratuit)

Fuite ou violation de données personnelles

Divulgation non autorisée d'informations personnelles détenues par un tiers (sites Internet, services en ligne, entreprises, associations, collectivités, administrations)

But recherché
en faire un usage frauduleux ou pour les revendre à d'autres cybercriminels qui les utiliseront.

Récupérées par des cybercriminels, les données personnelles peuvent servir:

- À l'hameçonnage ciblé
- Aux tentatives d'escroquerie, de fraude, d'extorsion,
- A l'atteinte à l'image ou la réputation,
- A l'usurpation d'identité,
- Au cyberharcèlement,
- ou encore tentatives de piratage des comptes en ligne lui appartenant.

Fuite ou violation de données personnelles, que faire?

- Contacter le service ou l'organisme concerné pour la confirmer et savoir quelles informations ont pu être compromises.
- Changer au plus vite le mot de passe sur les sites ou services concernés.
- Si les coordonnées bancaires figurent dans la fuite de données, prévenir immédiatement la banque.
- Signaler les pages, les comptes, les messages divulguant les informations personnelles auprès des plateformes sur lesquelles elles sont diffusées et demander leur suppression.
- Demander à ce que les données personnelles divulguées ne soient plus référencées par les moteurs de recherche lorsqu'elles y apparaissent.
- Si, un mois après la demande de suppression, les données personnelles sont toujours accessibles sur la plateforme concernée, adresser une réclamation (plainte) à la CNIL par le biais de son téléservice de plainte en ligne (https://www.cnil.fr/fr/plaintes/internet).
- En cas d'utilisation frauduleuse des données personnelles divulguées, conserver toutes les preuves (messages, adresse du site web, captures d'écran…) et déposer plainte.
- Engager au besoin une action de groupe ou un recours collectif.

Usurpation d'identité

Usurpation d'identité : Délit qui désigne l'utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses.

But recherché
Utilisation d'informations personnelles et/ou bancaires pour en faire un usage frauduleux.

En fonction des informations recueillies, les escrocs peuvent commettre diverses infractions au nom de la victime :

- Ouverture de ligne téléphonique ou de compte bancaire,
- Création de comptes sur les réseaux sociaux,
- Souscription d'un crédit, location de voiture, escroquerie des proches,
- Fausses petites annonces, diffamation, cyberharcèlement, chantage, extorsion…

Au-delà du préjudice moral, l'usurpation d'identité peut avoir des conséquences très importantes pour les victimes qui peuvent se voir poursuivies pour des infractions dont elles devront prouver qu'elles n'en seraient pas les auteurs.

Usurpation d'identité, que faire ? 1/2

1.Conserver toutes les preuves (captures d'écran, messages, adresses des pages Internet concernées, documents…) qui pourront servir pour prouver l'infraction.

2.Signaler directement l'usurpation d'identité auprès des plateformes sur laquelle elle a lieu.

3.Déposez plainte

4.Prévenir immédiatement tous les établissements bancaires ou financiers de l'usurpation d'identité. Si les informations bancaires ont été dérobées, faire opposition immédiatement.

5.Faire annuler et renouveler les pièces d'identité utilisées par les escrocs.

6.Préparer une attestation sur l'honneur à l'attention de tous les organismes pour justifier qu'on ,n'est pas l'auteur des faits reprochés en joignant une copie de la plainte déposée.

Usurpation d'identité, que faire ? 2/2

- **Contacter la Banque de France** pour signaler les faits et vérifier si des crédits ont été souscrits ou si un compte bancaire a été ouvert à votre insu. Consulter également le fichier central des chèques (FCC), celui des incidents de remboursement des crédits aux particuliers (FICP) et le fichier national des comptes bancaires et assimilés (FICOBA) pour vérifier si des opérations frauduleuses n'ont pas été commises en votre nom.

- Pour être conseillé dans les démarches, ***contactez la plateforme** Info Escroqueries* du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits).

Supprimer une donnée enregistrée dans les moteurs de recherche

➢ **Pour supprimer une donnée d'un moteur, il faut :**

- demander sa suppression du site internet sur lequel elle a été publiée initialement,
- puis demander une réindexation du site par le moteur de recherche.
- le délai peut prendre plusieurs jours !
- Si cela n'avance pas, faire appel à CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

➢ **Moralité : il vaut mieux éviter de mettre une information sur Internet plutôt que d'essayer de la supprimer après coup.**

Propagande, désinformation et fausses nouvelles



- **Mésinformation** : information fausse partagée sans l'intention de nuire
- **Désinformation** : information fausse qui est délibérément partagée pour porter préjudice
- **Information malveillante** : information fondée sur des faits réels, utilisée pour porter préjudice.

Diverses formes de partage d'information intentionnelles ou non,

pour causer un préjudice en lien avec la défense d'une cause

ou d'une vision morale ou politique particulière.

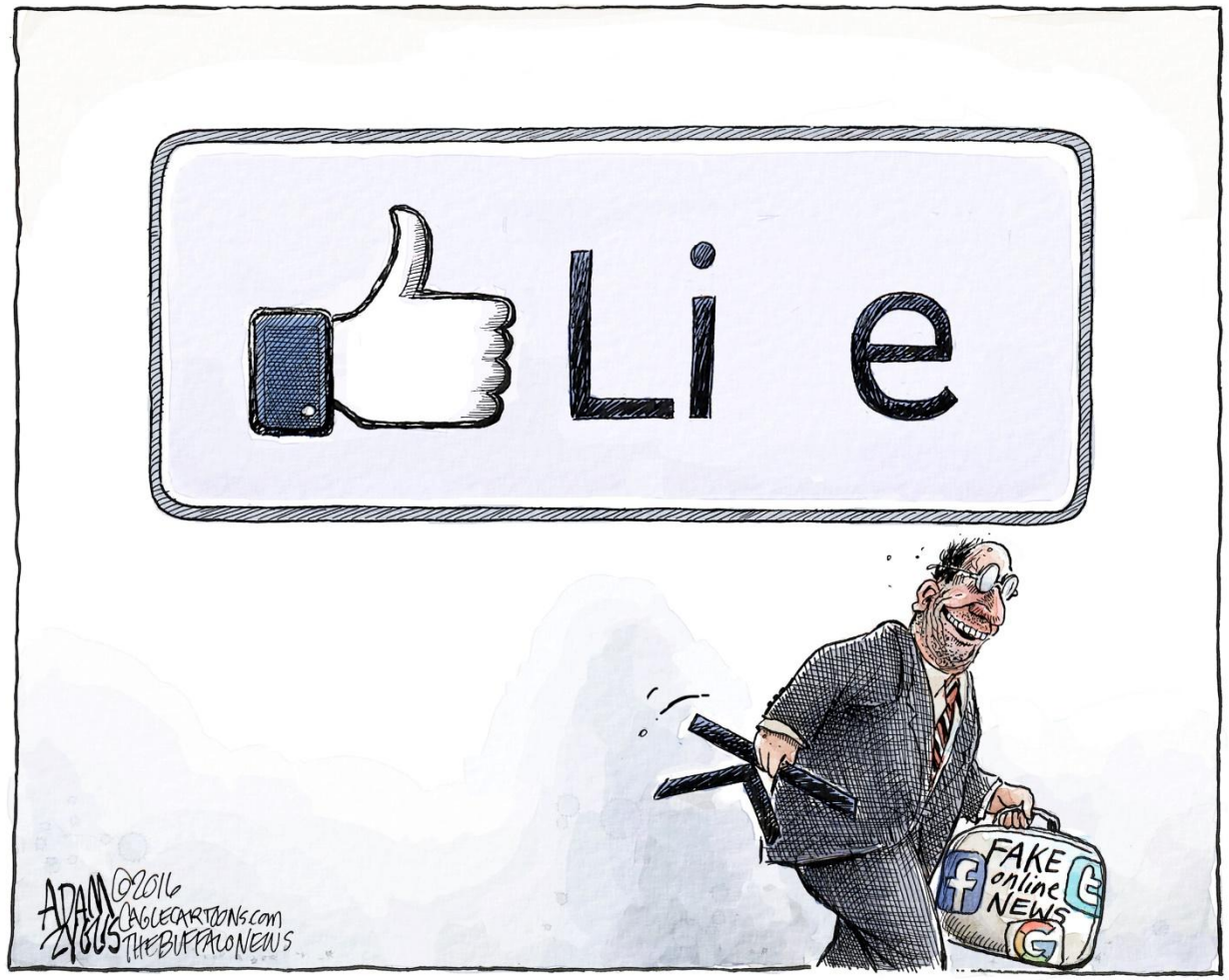
Propagande, désinformation et fausses nouvelles



1. Se méfier

- Le sujet me touche particulièrement, personnellement ?
- Suis-je capable d'identifier la source de l'information ? D'où elle émane, de quel contexte ?
- Cette information me parait elle plausible telle quelle ?
- Qui pourrait avoir un intérêt à répandre cette information ?
- Y a-t-il des indices qui discréditent la source de cette info ? Comme des fautes d'orthographe par exemple ? Des titres très accrocheurs ?

Propagande, désinformation et fausses nouvelles



2. Ne pas tout transférer à ses contacts!

Ne transférez à vos contacts que des informations et messages dont vous êtes sûr de l'authenticité.

- Ne vous laissez pas submerger par l'émotion.
- Lorsque vous débusquez de fausses nouvelles, signalez-les sur les sites qui s'occupent de dévoiler les fake news, pour interrompre la chaîne de leur propagation.



L'INTELLIGENCE ARTIFICIELLE (IA) : des risques croissants, mais pas de bouleversement en 2024

L'IA , outil privilégié de la désinformation en ligne

- Elle est un « outil » qui renforce l'arsenal déjà très fourni des cybercriminels et de leur montée en compétence.

- **Mais l'IA va augmenter la productivité des attaquants, améliorer la sophistication et l'efficacité de leurs attaques, ainsi que la crédibilité de leurs escroqueries voire de les réaliser dans des langues qu'ils ne maîtrisent pas.**

Cyberharcèlement ou harcèlement en ligne

Agissements **malveillants répétés**, dans un cadre public ou restreint:

> Le cyberharcèlement a pour objectif l'**atteinte** et la **dégradation des conditions de vie de la personne qui en est victime**.



- Sous **diverses formes** : intimidations, insultes, menaces, rumeurs, publication de photos ou vidéos compromettantes,
- Ciblant **une seule personne ou de plusieurs individus**
- Sur les réseaux sociaux, messageries, forums, blogs, etc.
- Les **conséquences du cyberharcèlement peuvent être dramatiques** pour les victimes : dépression, décrochage scolaire ou professionnel, troubles psychologiques ou émotionnels, violence, suicide, etc.

Le cyberharcèlement est puni par la loi
qui prévoit de lourdes sanctions à l'encontre de ses auteurs.

Cyberharcèlement ou harcèlement en ligne : Que faire?

- Ne pas répondre
- En parler à un tiers de confiance.
- Conserver les preuves
- Verrouiller au plus vite les comptes de réseaux sociaux.
- Signaler les contenus ou les comportements illicites auprès des plateformes sur lesquelles ils sont présents afin de les faire supprimer.
  Demander à ce que les contenus harcelants ne soient plus référencés par les moteurs de recherche.
- *Signaler les faits sur la plateforme dédiée du ministère de l'intérieur à* : Internet-signalement.gouv.fr.
- ***Déposer plainte***

CHANTAGE À L'ORDINATEUR OU À LA WEBCAM PRÉTENDUMENT PIRATÉS

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CYBERCRIMINEL



EXTORSION D'ARGENT

Un inconnu vous écrit pour vous annoncer qu'il possède des vidéos compromettantes réalisées avec votre webcam et réclame une rançon pour ne pas les rendre publiques ? Vous êtes victime du chantage à l'ordinateur ou à la webcam prétendus piratés !

BUT
Soutirer de l'argent contre la menace de divulguer des vidéos compromettantes de la victime à ses contacts.

TECHNIQUE
Envoi d'un message, par courriel (mail) avec parfois pour émetteur l'adresse de la victime ou même un de ses mots de passe.

CHANTAGE À L'ORDINATEUR OU À LA WEBCAM PRÉTENDUMENT PIRATÉS

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



COMMENT RÉAGIR ?

- Ne paniquez pas : vous n'avez sans doute rien de compromettant à vous reprocher
- Ne répondez pas
- Ne payez pas
- Conservez les preuves
- Changez votre mot de passe partout où vous l'utilisez s'il a été divulgué ou au moindre doute
- Déposez plainte

LES RANÇONGICIELS

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CYBERCRIMINEL



EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT
Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE
Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

LES **RANÇONGICIELS**

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

VICTIME



COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

LIEN UTILE www.nomoreransom.org/fr/index.4html



Sextorsion

Près de 1 000% d'augmentation en 2024

L'escroc, sous une fausse identité, cherche à obtenir de la victime des échanges en vidéo ou des photos à caractère sexuel.

But recherché

- Faire chanter ensuite en menaçant de les divulguer.
- Soutirer de l'argent ou d'autres contenus intimes,
- Ou encore d' alimenter des sites pornographiques, voire la sphère pédocriminelle

- Contact via site de rencontre, réseau social ou messagerie instantanée,
- Contenus intimes parfois obtenus par piratage d'un compte ou par montage de contenu,
- **Les plus jeunes en sont de plus en plus victimes.**

LE PIRATAGE DE COMPTE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

En forte hausse en 2024



VOL DE DONNÉES

Vous constatez une activité anormale ou inquiétante sur vos comptes ou applications (messagerie, réseaux sociaux, sites administratifs, banques, sites e-commerce...) ? Vous êtes peut-être victime d'un piratage de compte !

BUT
Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.)

TECHNIQUE
Prise de contrôle d'un ou plusieurs comptes en ligne, suite à 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.

LE PIRATAGE DE COMPTE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

En forte hausse en 2024



Les comptes de réseaux sociaux piratés font l'objet de divers types d'escroqueries. Parmi les plus constatées en 2024,

- **l'identité de la victime est usurpée auprès de ses contacts :**

pour demander de l'aide afin de résoudre un problème supposé, en général lié à son téléphone. Le but est de pirater le compte du contact sollicité, d'effectuer des achats débités sur la facture de son abonnement téléphonique, …

- la victime fait l'objet de **chantage pour pouvoir récupérer son compte ou éviter la diffusion de contenus compromettants** que l'escroc aura récupérés dans les messages privés du compte piraté.

Il est souvent très difficile pour la victime du piratage de son compte de réseau social de le récupérer malgré ses démarches auprès de la plateforme.

LE PIRATAGE DE COMPTE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

VICTIME



COMMENT RÉAGIR ?

- Changez votre mot de passe piraté sur tous les sites ou comptes sur lesquels vous pouviez l'utiliser
- Vérifiez que les coordonnées de récupération de votre compte (e-mail, téléphone) n'ont pas été modifiées
- Prévenez votre banque
- Prévenez tous vos contacts de ce piratage
- Sauvegardez les preuves
- Déposez plainte si le préjudice le justifie

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

Piratage d'un système informatique

But recherché
Prendre le contrôle de l'appareil, dérober des informations personnelles ou confidentielles, pour en faire un usage frauduleux (usurpation d'identité, espionnage, fraude bancaire, etc.).



- En utilisant une faille de sécurité ou un défaut de configuration de l'appareil l'infectant ainsi avec un logiciel malveillant;
- Via le vol d'identifiants de connexion suite à un appel ou un message frauduleux, en devinant un mot de passe trop simple ou un mot de passe par défaut qui n'aurait pas été changé, etc.

Une fois introduit, le cybercriminel peut chercher à se propager dans les autres appareils du système..

Piratage d’un système informatique : Que faire ?

1. **Déconnecter l’appareil**
2. **Identifier la source de l’intrusion** et prendre les mesures nécessaires pour qu’elle ne puisse pas se reproduire
3. **Identifier toute activité inhabituelle** : création de nouveaux comptes utilisateurs ou administrateurs, lancement de programmes ou processus inconnus, perte de données, etc.
4. **Évaluer l’étendue de l’intrusion** à d’autres appareils de votre système informatique.
5. **Essayer de récupérer ou de faire récupérer par un professionnel les preuves**.
6. ***Déposez plainte***

Etapes suivantes avec l’aide d’un professionnel si nécessaire

LES VIRUS INFORMATIQUES

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



VOL DE DONNÉES

Vous constatez un ralentissement ou un blocage anormal de votre appareil, des messages ou des fenêtres d'erreur s'affichent sans raison apparente ? Vous avez une alerte de votre antivirus ? Vous êtes peut-être victime d'un virus informatique !

BUT

Prendre le contrôle d'un système informatique pour en faire un usage frauduleux, comme espionner l'utilisateur, dérober des données personnelles et/ou confidentielles, attaquer d'autres appareils, chiffrer les fichiers et demander une rançon, etc.

TECHNIQUE

Infection d'un équipement suite à l'ouverture d'une pièce jointe piégée, d'un clic sur un lien frauduleux, de la navigation sur un site malveillant, de l'installation d'une application piratée, le branchement d'un support (clé USB...) contaminé, etc.

LES VIRUS INFORMATIQUES

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT RÉAGIR ?



- Débranchez la machine d'Internet ou du réseau local
- Identifiez et corrigez l'origine de l'infection
- Récupérez les preuves disponibles
- Déposez plainte
- Supprimez l'infection avec votre antivirus et en cas d'échec réinstallez votre système
- Changez tous vos mots de passe
- Au besoin, faites-vous assister par des professionnels

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr



La fraude à la carte bancaire

C’est l’utilisation frauduleuse des coordonnées de la carte bancaire d’une personne à son insu alors que celle-ci est pourtant toujours en possession de sa carte.

But recherché
Dérober les coordonnées bancaires de la victime pour en faire un usage frauduleux (achats en ligne, etc.).

Trouver l’origine précise d’une telle fraude est souvent difficile.

Pour obtenir les coordonnées de la carte bancaire de la victime, le fraudeur peut utiliser tous les moyens déjà explicités, mais aussi :

- Le piégeage d’un distributeur de billets,
- Lors d’un paiement, un individu malhonnête qui photographie la carte.

Victime d'une arnaque à la carte bancaire, que faire ?

1. **Faire immédiatement opposition à la carte bancaire** Le numéro d'opposition figure sur le site Internet de la banque, sur les distributeurs de billets. On peut aussi contacter par téléphone le serveur interbancaire d'opposition à la carte bancaire au 0 892 705 705. Ce service est ouvert 7 jours sur 7, 24h sur 24.

2. Dès l'identification d'un débit frauduleux sur votre compte bancaire, **alerter la banque au plus vite pour en demander le remboursement**.

3. **Signalez la fraude bancaire auprès de la plateforme *Perceval*** du ministère de l'intérieur.

4. ***Déposer plainte***

5. **Mettre à jour ses équipements**

6. **Réaliser une analyse antivirale complète**

7. **S'assurer qu'aucun compte en ligne ne soit piraté.**

FOVI ou arnaque au faux ordre de virement bancaire

C'est un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié.

But recherché

Escroquerie financière en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé visant à faire verser de l'argent sur un compte bancaire détenu par les cybercriminels. Dans certains cas, cette fraude fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée.



Variantes connues:

- Demande d'un dirigeant avec un caractère « urgent et confidentiel »,
- Usurpation d'identité pour demander un changement de RIB et capter un virement

Le compte bancaire de l'escroc est souvent situé à l'étranger.

Escroquerie réalisée par téléphone et/ou par messages électroniques, voire les deux, et concerne les particuliers et tous les types d'organisation.

FOVI ou arnaque au faux ordre de virement bancaire, que faire ?

1. **Identifier les virements frauduleux**

2. **Alerter immédiatement votre banque en cas de transaction frauduleuse et demandez le retour des fonds**

3. **Demander la suspension du virement**

4. Conserver les preuves,

5. Si la fraude a pu être permise par le piratage d'un compte de messagerie, changer immédiatement son mot de passe :

6. *Dépose plainte et contacter info-escroquerie*



Fraude au faux conseiller bancaire

Escroquerie consistant à tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes bancaires.

But recherché
Tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes bancaires.

- L'escroc dispose de nombreuses informations pour crédibiliser son arnaque :
- Il peut usurper un numéro de téléphone de la banque
- Il prétend avoir identifié des actions suspectes en cours sur le compte bancaire
- Il demande de communiquer des codes ou fait confirmer des actions via l'application bancaire

Variante de la fraude au faux conseiller bancaire

Une déclinaison de ce mode opératoire observée en 2023 s'est intensifiée en 2024 :
l'hameçonnage aux fausses confirmations de commande, par mail mais aussi par SMS.
Demandant une validation d'achat en ligne et invitant à appeler un numéro
de téléphone donné si elle n'est pas à l'origine du paiement.

Le but recherché est le même

Tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes bancaires.



DARTY

Nous vous informons que votre commande **DARTY** pour un **iphone 13** d'une valeur de 960.00 € est en cours de traitement, et sera livré dans les prochains jours. Si vous n'êtes pas à l'origine de ce paiement veuillez contacter :

NUMERO VERT : 0 9[redacted]308

Cordialement,
client Darty,

SAS au capital de 23 470 382 Euros Siège social : ZAC Port d'Ivry - 9 rue des Bateaux Lavoirs – 94200 IVRY-SUR-SEINE.

Fraude au faux conseiller bancaire: Que faire?

- Vérifier l'information par vous-même.
- Ne jamais communiquer identifiants, codes, mots de passe.
- Ne valider aucune opération dont on n'est pas à l'origine.
- Faire opposition à la carte bancaire. sans délai
- Changer code confidentiel/mot de passe d'accès au compte en ligne au plus vite ou demander à la banque de le réinitialiser.
- Identifier les opérations frauduleuses, alerter la banque.
- Conserver les preuves pour signaler l'escroquerie aux autorités et à la banque
- Fraude à la carte bancaire, signaler ***sur la plateforme Perceval***
- ***Déposer plainte***
- Mettre à jour les équipements (ordinateurs, téléphones, tablettes…) pour corriger des failles de sécurité.
- Réaliser une analyse (scan) antivirale complète de vos appareils.

Fraude au faux conseiller bancaire: Que faire?

- Vérifier l'information par vous-même.
- Ne jamais communiquer identifiants, codes, mots de passe.
- Ne valider aucune opération dont on n'est pas à l'origine.
- Faire opposition à la carte bancaire. sans délai
- Changer code confidentiel/mot de passe d'accès au com… …mander à la banque de le réinitialiser.
- Identifier les opérations fra…
- Conserver l… …querie aux autorités et à la banque
- …signaler ***sur la plateforme Perceval***
- Mettre à jour les équipements (ordinateurs, téléphones, tablettes…) pour corriger des failles de sécurité.
- Réaliser une analyse (scan) antivirale complète de vos appareils.

En cas de communication téléphonique ou internet bancaire douteuse , rappelez immédiatement son contact commercial bancaire avant toute action demandée

LES FAUX SUPPORTS TECHNIQUES

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique



ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT
Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants.

TECHNIQUE
Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

LES FAUX SUPPORTS TECHNIQUES

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT RÉAGIR ?



- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

En 2024, la plupart des déclenchements d'arnaque de faux support ont eu lieu suite à un clic sur un contenu sponsorisé (premiers résultats de moteurs de recherche, publicités et titres d'articles racoleurs sur des sites Internet ou les réseaux sociaux).



Son imagination n’a pas de limites !!!

Pour vous soutirer de l’argent

Fausse annonce immobilière, escroquerie sentimentale, fausse annonce d’emploi…



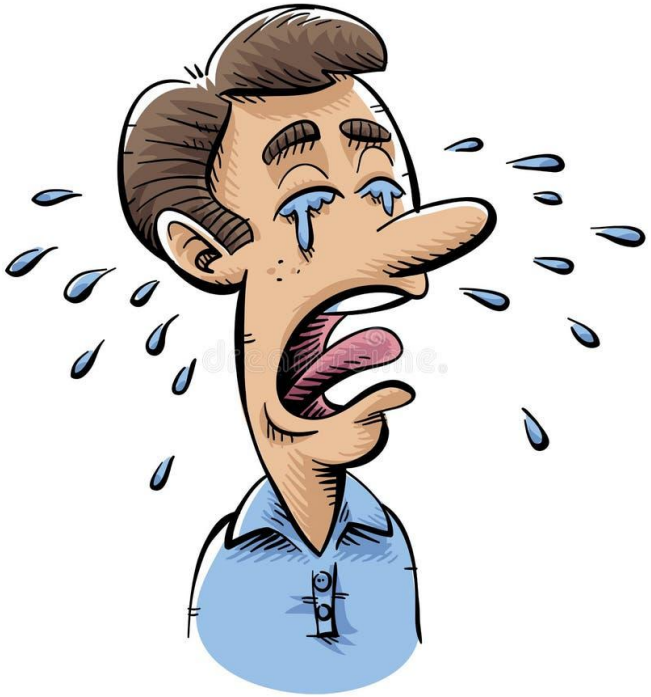






Son imagination n’a pas de limites !!!

Pour vous soutirer de l’argent



Le bon escroc sait:

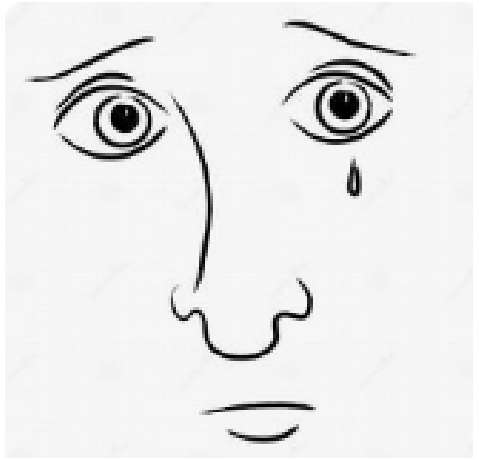
Se montrer très sympathique, empathique…
Faire des offres très attirantes,
Créer l’urgence à profiter de l’offre très attirante,
Vous isoler de votre entourage habituel,
Faire monter la pression, progressivement,

Pour vous soutirer de l’argent, une fois et plus si possible.



Son imagination n’a pas de limites !!!

Pour vous soutirer de l’argent



REAGIR

Se méfier des annonces trop attractives,
S’assurer de l’entité de la personne ou de la société,
Garder les traces et les documents transmis.

Interrompre la relation, alerter la banque,
Porter plainte



Son imagination n’a pas de limites !!!

Pour vous soutirer de l’argent

REAGIR

Se méfier des annon… …ves,

S’assurer … personne ou de la société,

… et les documents transmis.

…nterrompre la relation, alerter la banque,

Porter plainte

Vérifier l’adresse d’envoi de tout message internet ou autre nous paraissant potentiellement frauduleux , voir à le comparer au site connu qui est sensé le générer

Sites de vente entre particuliers : 20 conseils pour éviter les arnaques

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Médiathèque AUVERS-SUR-OISE

1. Vérifiez les conditions générales d'utilisation
2. Renseignez-vous sur les modalités de transaction,
3. Attention aux offres ou annonces de trop « bonnes affaires »,
4. Vérifiez si le vendeur dispose d'un historique de ventes,
5. Méfiez-vous des invitations à poursuivre les échanges en dehors de la plateforme,
6. Demandez à l'interlocuteur une adresse mail et un numéro de téléphone,
7. Recherchez dans un moteur de recherche des indications d'escroquerie,
8. Marquez les copies de vos documents/justificatifs d'identité,
9. Vérifiez la légitimité des messages, liens vers des sites Internet ou appels reçus,
10. Privilégiez les transactions qui assurent une remise du produit et des fonds en main propre.

Sites de vente entre particuliers : 20 conseils pour éviter les arnaques

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Médiathèque AUVERS-SUR-OISE

11. Procédez à l'échange dans un lieu public fréquenté,
12. Méfiez-vous des interlocuteurs qui insistent pour imposer une société de livraison précise.
13. Utilisez de préférence le système de paiement de la plateforme
14. Méfiez-vous des interlocuteurs qui insistent pour utiliser un autre moyen de paiement en ligne.
15. Refusez l'utilisation de moyens de paiement « *alternatifs* »
16. Refusez les propositions de payer la transaction à une entreprise de livraison.
17. Si un acheteur a payé plus que le prix prévu, refusez de rembourser le trop payé
18. Si l'interlocuteur demande le règlement de la transaction au travers d'un service de paiement en ligne (PayPal, Paylib…), vérifiez l'authenticité des messages
19. Assurez-vous de l'authenticité des preuves de paiement ou d'expédition
20. Sécurisez l'accès à votre compte



Se protéger

Avant tout, avec une bonne hygiène numérique !

Deux sites de référence officiels recommandés



https://www.cybermalveillance.gouv.fr

https://www.cnil.fr



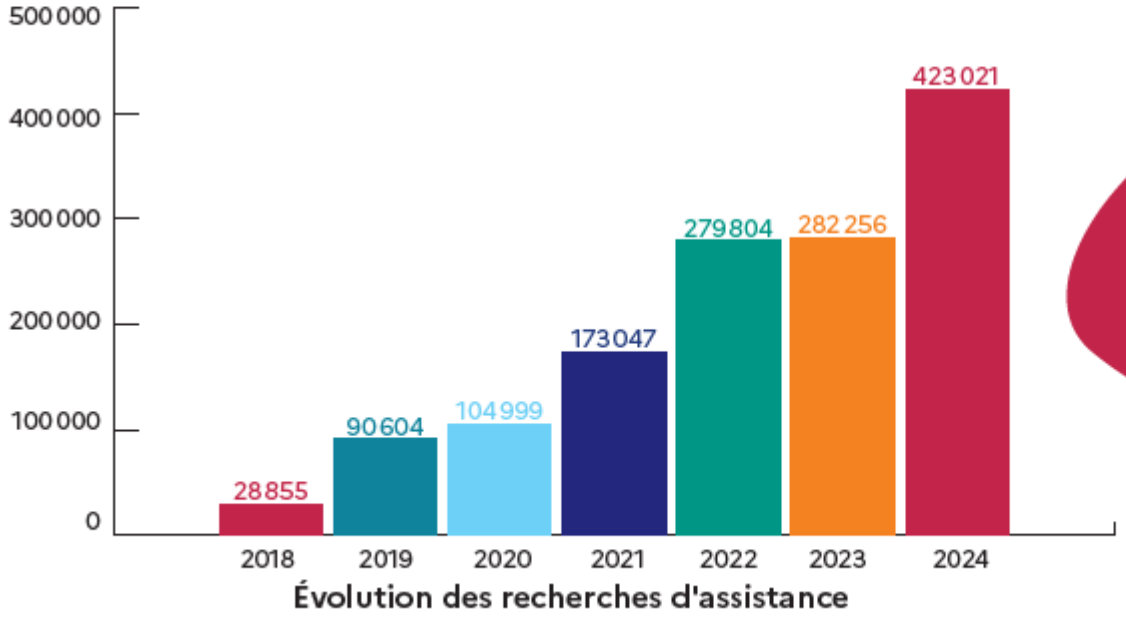
Statistiques 2024

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

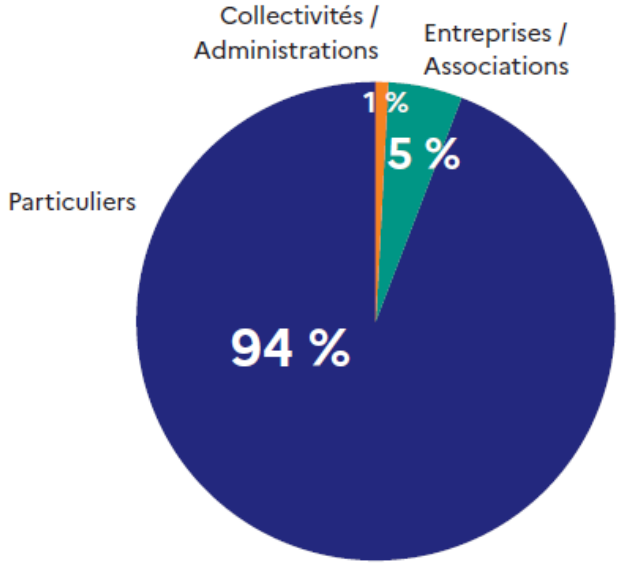
LES DEMANDES D'ASSISTANCE 2024

En 2024, la plateforme Cybermalveillance.gouv.fr a enregistré plus de 420 000 demandes d'assistance. Leur analyse offre une vision des différentes formes de menaces auxquelles les publics du dispositif sont confrontés.



Évolution des recherches d'assistance

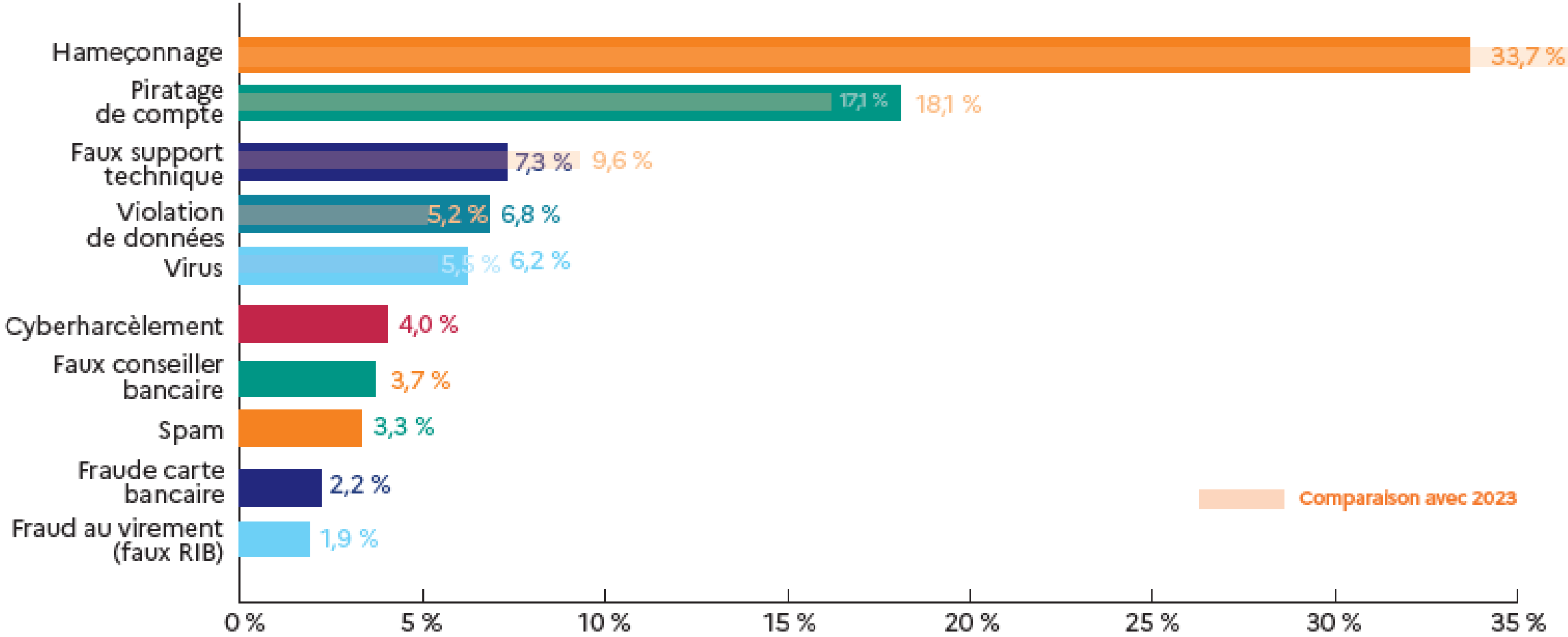
420 000
demandes d'assistance en ligne en 2024



Répartition des demandes d'assistance par catégories de public

Le taux de satisfaction des publics pour ce service d'assistance en ligne reste élevé (87,4 %).

Statistiques 2024



Hygiène numérique comportementale

	Principes valables quelle que soit l'utilisation
1	Maîtriser ses cercles de connaissances
2	Être vigilant en communiquant des informations personnelles, intimes ou sensibles.
3	Maîtriser ses publications: Messagerie et réseaux sociaux
4	Ne pas communiquer de documents d'identité de manière inconsidérée
5	Faire preuve de discernement avec certaines informations relayées et les vérifier
6	Être vigilant lorsqu'on communique numéro de téléphone, ou adresse électronique
7	Être vigilant lorsqu'on répond à des formulaires d'inscription, des bons de commande, ou à des jeux concours
8	Lire avec attention tous les documents sur lesquels on doit apposer sa signature ou son consentement
9	Se méfier des offres trop attractives, des réponses urgentes à donner
10	Éviter les sites non sûrs ou illicites

Cliquez pour voir :

- **Les conseils de la CNIL,**
- **L'identité France Connect,**
- **La gestion des cookies**

Hygiène numérique dans l’utilisation

	Principes valables quelle que soit l'utilisation
1	Utiliser des mots de passe différents et complexes pour chaque site et application
2	Effectuer régulièrement des sauvegardes
3	Appliquer de manière régulière et systématique les mises à jour de sécurité
4	Utiliser un antivirus et éventuellement un pare-feu
5	N’installer des applications ou logiciels que depuis les sites ou magasins officiels
6	Ne pas se connecter à des réseaux Wifi ou des supports amovibles non sécurisés
7	Ne pas utiliser le compte "Administrateur" quand ce n'est pas nécessaire
8	Masquer la Webcam, neutraliser le micro si l'utilisation n'est pas nécessaire
9	Faire régulièrement une analyse antivirale complète (scan)
10	Ne pas laisser son ordinateur allumé, utilisable sans contrôle

Cliquez pour voir les conseils sur :

- **Les mots de passe**
- **Les sauvegardes,**
- **Les mises à jour des logiciels**

Hygiène de communication numérique

	Principes valables quelle que soit l'utilisation
1	Se méfier des messages (mail ou SMS) qui amènent à communiquer des informations personnelles et/ou bancaires.
2	Être vigilant à la réception d'un message (mail ou SMS) incitant à cliquer sur un lien Internet ou un QR code
3	Ne pas répondre aux messages dont on ne connait ni l'expéditeur ni l'intérêt de répondre
4	Créer différentes adresses de messagerie ou des « alias » en fonction de ses besoins
5	Ne pas céder au caractère urgent et pressant d'une demande
6	Ne pas valider une action (opération ou annulation, validation, blocage…) dont on n'est pas l'initiateur
7	Refuser toute demande de prise de contrôle à distance de l'ordinateur, la tablette ou le téléphone
8	Si un appel provenant d'une banque ou organisme administratif ou commercial paraît suspect, raccrocher et contacter les numéros et contacts officiels
9	Vérifier les sites sur lesquels on va faire des achats
10	séparer usages personnels et usages professionnels

Cliquez pour voir les conseils sur :

- **Les SPAM,**
- **La navigation internet,**
- **Le paiement sécurisé**
- **La surveillance de sa e-réputation**

Hygiène de communication numérique

	Principes valables quelle que soit l'utilisation
1	Se méfier des messages (mail ou SMS) qui amènent à communiquer des infor… personnelles et/ou bancaires.
2	Être vigilant à la réception d'un message (mail ou SMS) incitan… Internet
3	Ne pas répondre aux messages dont on ne co… répondre
4	Créer différentes adresses de … …tion de ses besoins
5	Ne pas céder au… …e demande
6	Ne pas … …mulation, validation, blocage…) dont on n'est …
	… prise de contrôle à distance de l'ordinateur, la tablette ou le
	… provenant d'une banque ou organisme administratif ou commercial paraît … pect, raccrocher et contacter les numéros et contacts officiels
	Vérifier les sites sur lesquels on va faire des achats
10	séparer usages personnels et usages professionnels

Vérifier l'adresse d'envoi de tout message internet ou autre nous paraissant potentiellement frauduleux , voir à le comparer au site connu qui est sensé le générer.
Ne cliquer ni sur un lien, ni sur un QR Code.

Fin de la section
Se Protéger



Maintenant je sais l’essentiel,
Je me protège et je sais réagir si nécessaire

Fin de la présentation

Les pages suivantes sont les explications complémentaires ou des illustrations appelées par le symbole



CNIL.

Conseils pour protéger votre vie privée

1. Réfléchissez avant de publier



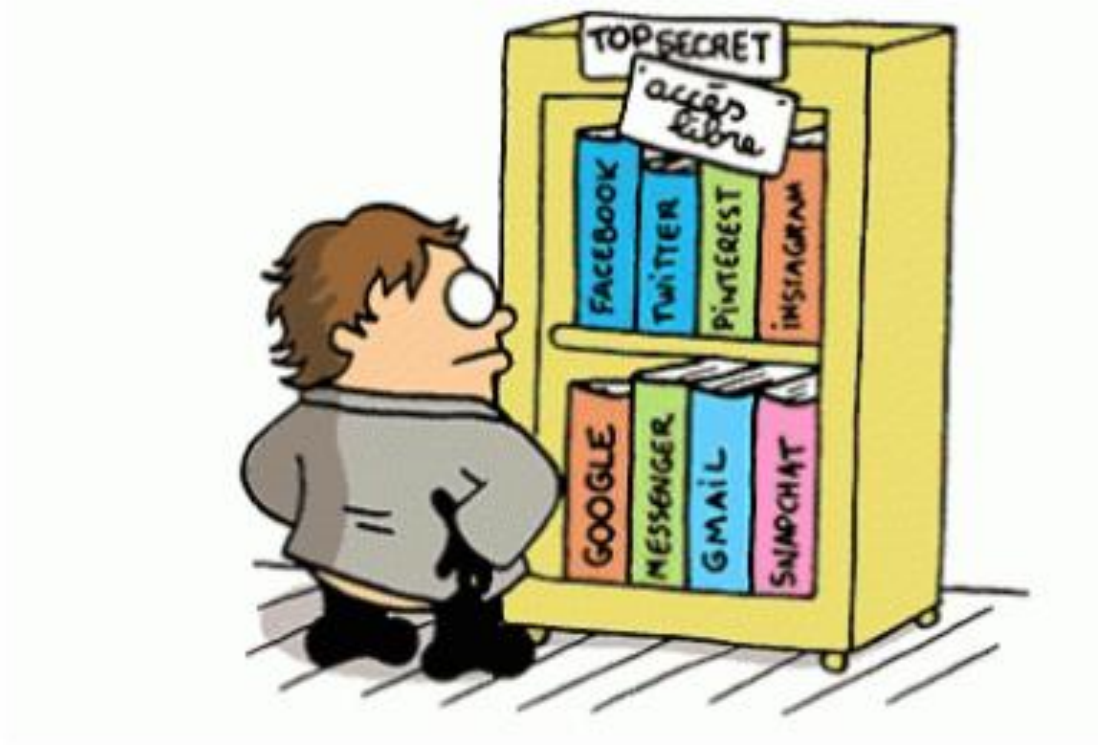
2. Respectez les autres



CNIL.

Conseils pour protéger votre vie privée

3. Ne dites pas tout



4. Sécurisez vos comptes



5. Créez plusieurs adresses e-mail

PAUL.SMITH@MAIL.COM



Pour les services de confiance et le réseau profesionnel...

POLAROID34@AUTREMAIL.ORG



Sous pseudo pour s'inscrire sur les réseaux sociaux, forums ou sites de rencontres...

PS523@POUBELLE.FR



Une adresse pourriel pour les jeux concours, les cartes de fidélité...

CNIL.

Conseils pour protéger votre vie privée

6. Attention aux photos et aux vidéos



7. Utilisez un pseudonyme



https://filigrane.beta.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FiligraneFacile BÊTA

Si vous devez communiquer un document contenant des données personnelles sensibles

Ajoutez un filigrane à n'importe quel document

L'ajout d'un filigrane sur vos documents est une bonne pratique mais certains organismes peuvent avoir besoin d'un document vierge (banques, services publics, etc.)

Le fichier filigrané sera au format PDF.
Les fichiers originaux seront **effacés de nos serveurs après la génération** du fichier filigrané.
Le fichier filigrané sera **effacé de nos serveurs après le premier téléchargement** (ou au bout d'un jour s'il n'y a pas eu de téléchargement).

Sélectionner des fichiers :

Formats supportés : jpg, png, heic, pdf.

Choisir des fichiers Aucun fichier n'a été sélectionné

Indiquez le filigrane à insérer :

Ex : Document exclusivement destiné à la location immobilière

Ajouter le filigrane

Utiliser une identité numérique de confiance

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

France Connect

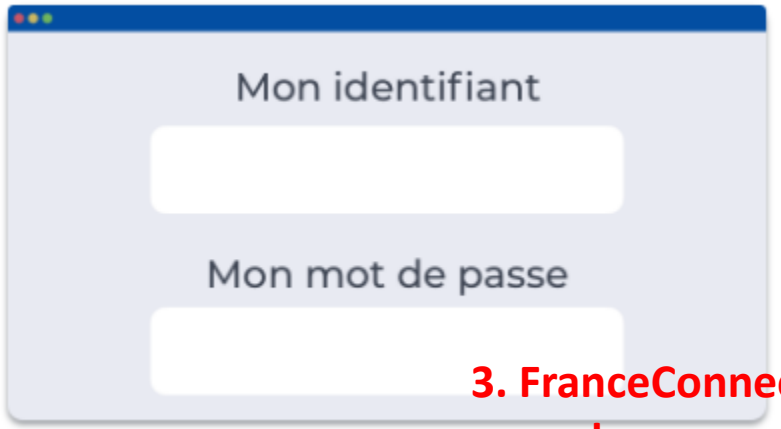


1. Pour accéder au service, je clique sur le bouton France Connect



2. Je choisis un des comptes que je connais déjà

Utiliser une identité numérique de confiance



3. FranceConnect me redirige vers la page de connexion pour rentrer mes identifiants



4. FranceConnect me confirme que la connexion est établie !

Eviter les cookies



- Refuser / paramétrer les cookies
- Effacer les cookies en fin de navigation
- Utiliser une fenêtre de navigation privée
- Choisir un moteur de recherche comme Qwant ou Lilo
- Lire les conditions avant de s'engager
- Paramétrer son compte

Qwant
Le moteur de recherche qui respecte votre vie privée

lilo

8. Attention aux mots de passe

UN MOT DE PASSE EN BÉTON



IL NE DIT RIEN SUR VOUS



UN COMPTE, UN MOT DE PASSE



Bien choisir ses mots de passe

Impératif
8 caractères minimum
Mélange de chiffres et de lettres
Mélange de majuscules et minuscules
Au moins un caractère spécial
Pas de nom commun, ou propre, pas de date

Vos animateurs ont réalisé un tutoriel sur les mots de passe, enregistré au fonds documentaire numérique de la médiathèque

10 CONSEILS POUR FAIRE VOS SAUVEGARDES

mémo

1. Effectuez des sauvegardes régulières de vos données
2. Identifiez les appareils et supports qui contiennent des données
3. Déterminez quelles données doivent être sauvegardées
4. Choisissez une solution de sauvegarde adaptée à vos besoins
5. Planifiez vos sauvegardes
6. Déconnectez votre support de sauvegarde après utilisation
7. Protégez vos sauvegardes (perte, vol, casse...)
8. Testez vos sauvegardes
9. Vérifiez le support de sauvegarde
10 Pro. Sauvegardez les logiciels indispensables à l'exploitation de vos données

Faire des sauvegardes

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

mémo

10 CONSEILS POUR GÉRER VOS MISES À JOUR

1. Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels
2. Téléchargez les mises à jour uniquement depuis les sites officiels
3. Identifiez l'ensemble des appareils et logiciels utilisés
4. Activez l'option de téléchargement et d'installation automatique des mises à jour
5. Pro — Définissez les règles de réalisation des mises à jour
6. Planifiez les mises à jour lors de périodes d'inactivité
7. Méfiez-vous des fausses mises à jour sur Internet
8. Pro — Informez-vous sur la publication régulière des mises à jour de l'éditeur
9. Pro — Testez les mises à jour lorsque cela est possible et faites des sauvegardes
10. Pro — Protégez autrement les appareils qui ne peuvent pas être mis à jour

Effectuer les mises à jour des logiciels

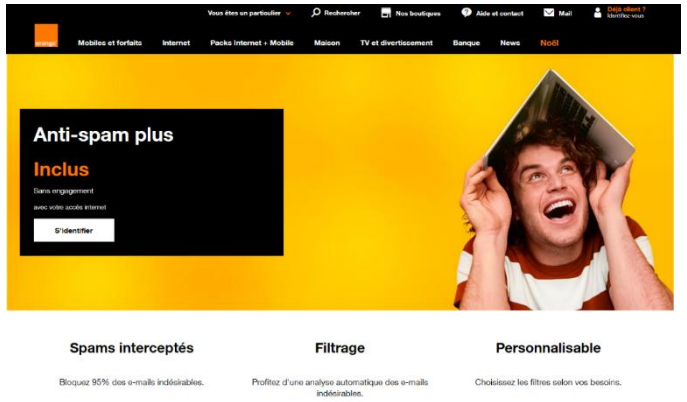
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Se protéger du SPAM





- Ne pas répondre à un spam
- Ne pas cliquer sur les liens ou QR Code intégrés
- Ne pas cliquer sur « se désabonner »
- Ne pas ouvrir les pièces jointes
- Etre prudent lors de la communication de son adresse électronique
- Utiliser un filtre de spam
- Signaler les spam https://www.signal-spam.fr



Repérer une arnaque reçue par courriel

- Est-ce que le message/courriel m’est réellement destiné ?
- Attention aux expéditeurs inconnus
- Être attentif au niveau de langage du courriel
- Vérifiez les liens dans le courriel
- Se méfier des demandes étranges et offres trop tentantes!
- L’adresse de messagerie source n’est pas un critère fiable

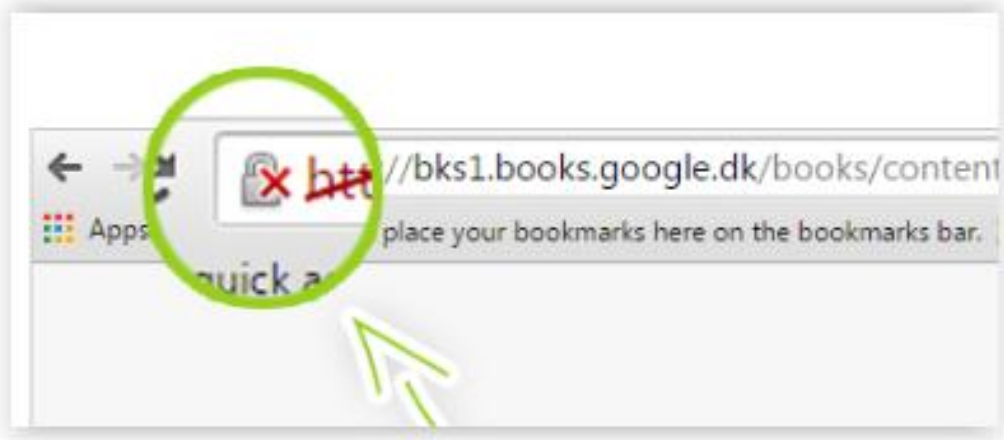


Reconnaitre les sites internet sécurisés

Sites sécurisés

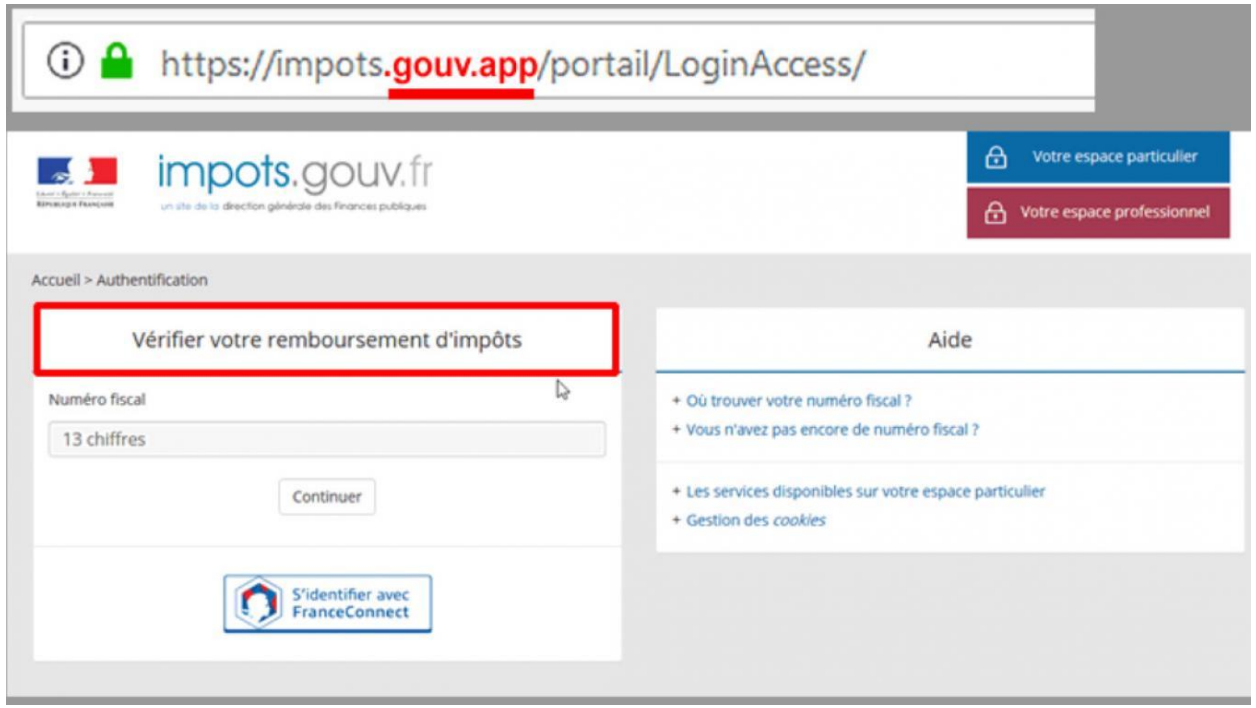


Sites non sécurisés



Se méfier des sites internet inconnus





CNIL.

9. Faites le ménage dans vos historiques



10. Vérifiez vos traces



https://www.cnil.fr/fr/effacer-des-informations-me-concernant-sur-un-moteur-de-recherche

Réaliser un paiement sécurisé sur internet 1/2

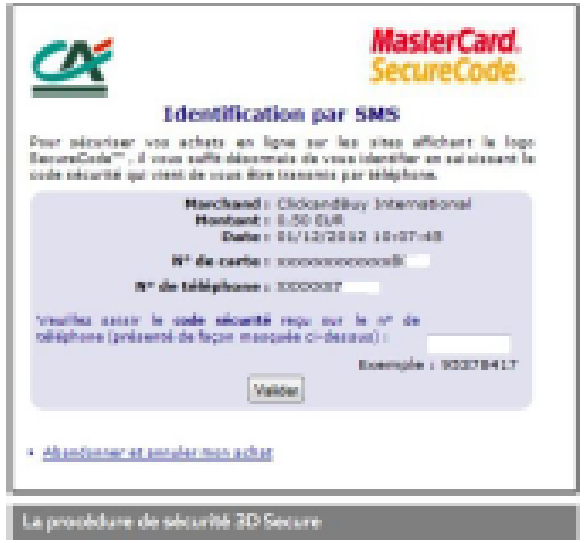
- Le site marchand doit être sécurisé
- Avant de commencer s'assurer d'avoir :



- Ne pas utiliser un réseau wifi public pour effectuer un paiement

Réaliser un paiement sécurisé sur internet 2/2

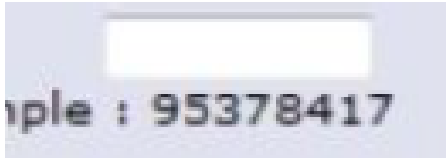
La procédure Active 3D Secure apparaît à l'écran



Code reçu par SMS sur votre téléphone.



Ecrivez le code à 8 chiffres reçu par SMS.



+ Réception du courriel de confirmation du paiement

Ou procédé équivalent via application bancaire sur le smartphone

Surveiller sa e-réputation

- Entrer ses nom et prénom dans un moteur de recherche
- Le résultat est un aperçu de ce qu'on publie sur nous

