RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CONSEILLER NUMÉRIQUE
France services

FRANCE RELANCE

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Identifier et comprendre la malveillance sur Internet

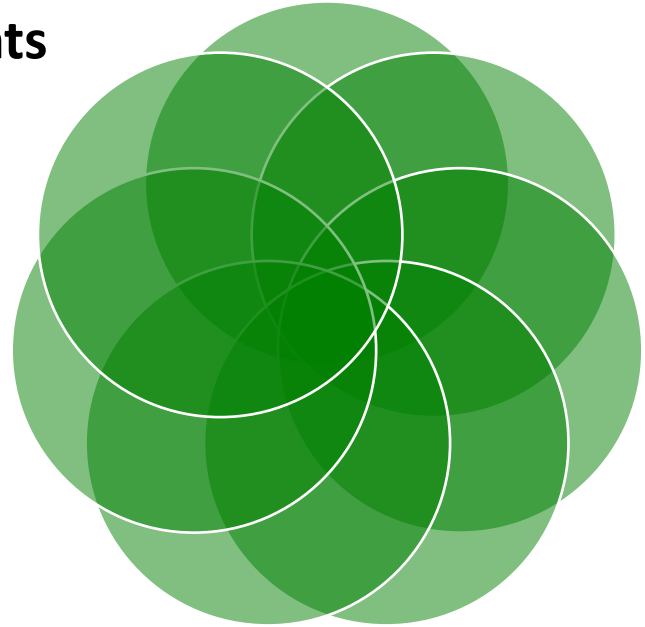
Connaitre le risque pour mieux le maîtriser.

Des dangers de formes variées

Ingénierie sociale

Logiciels malveillants

Hameçonnage (Phishing)



Arnaque au faux ordre de virement bancaire (FOVI)

Piratage de compte / Usurpation d'identité

Arnaque au faux support informatique

Arnaque à la romance

BONNE IDÉE OU PAS ?

Pensez-vous qu'un bon mot de passe puisse être utilisé pour plusieurs services (boîtes mail, réseaux sociaux, banque, sites de e-commerce, administrations…) ?

A Oui, quand les services n'ont rien à voir les uns avec les autres

B Oui, mais uniquement si le mot de passe contient des caractères spéciaux

C Non, chaque service doit avoir un mot de passe différent

Pensez-vous qu'un bon mot de passe puisse être utilisé pour plusieurs services (boîtes mail, réseaux sociaux, banque, sites de e-commerce, administrations…) ?

A Oui, quand les services n'ont rien à voir les uns avec les autres

B Oui, mais uniquement si le mot de passe contient des caractères spéciaux

C Non, chaque service doit avoir un mot de passe différent

Vous recevez un mail portant sur la fermeture de votre compte WhatsApp.
Ce mail contient le logo WhatsApp et comporte une pièce jointe.

Vous :

A Ouvrez la pièce jointe pour en savoir plus

B Hésitez à ouvrir la pièce jointe mais êtes rassuré par le logo Instagram

C N'ouvrez pas la pièce jointe et vous vous connectez directement sur votre compte

Vous recevez un mail portant sur la fermeture de votre compte WhatsApp. Ce mail contient le logo WhatsApp et comporte une pièce jointe.

Vous :

A Ouvrez la pièce jointe pour en savoir plus

B Hésitez à ouvrir la pièce jointe mais êtes rassuré par le logo Instagram

C N'ouvrez pas la pièce jointe et vous vous connectez directement sur votre compte

Vous recevez un SMS vous indiquant que votre colis arrive mais qu'il faut mettre à jour vos coordonnées de livraison.

Vous :

A Appuyez sur le lien contenu dans le SMS

B Ne faites rien

C Appelez le numéro de téléphone de l'expéditeur

Vous recevez un SMS vous indiquant que votre colis arrive mais qu'il faut mettre à jour vos coordonnées de livraison.

Vous :

A Appuyez sur le lien contenu dans le SMS

B Ne faites rien

C Appelez le numéro de téléphone de l'expéditeur

Vous recevez un mail vous informant que des photos où vous êtes tagué sont disponibles. Le site web vous demande de saisir votre identifiant et votre mot de passe Facebook.
Il semble que le site web possède un certificat légitime avec un cadenas à côté de la barre d'adresse.

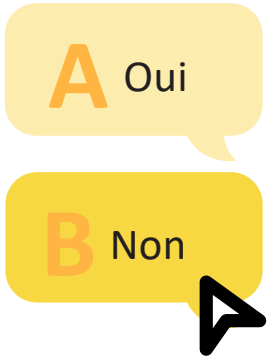
Vous saisissez votre identifiant et votre mot de passe sur le site web ?

A Oui

B Non

Vous recevez un mail vous informant que des photos où vous êtes tagué sont disponibles. Le site web vous demande de saisir votre identifiant et votre mot de passe Facebook.
Il semble que le site web possède un certificat légitime avec un cadenas à côté de la barre d'adresse.

Vous saisissez votre identifiant et votre mot de passe sur le site web ?



Que faire si un message bloquant votre ordinateur apparaît, signalant un problème technique grave, un risque de perte de vos données ou bien la présence de nombreux virus ?

A Ne rien faire

B Contacter le support technique au numéro indiqué sur le message d'erreur

C Tenter de redémarrer votre ordinateur et, si le problème persiste, demander de l'aide à un ami

Que faire si un message bloquant votre ordinateur apparaît, signalant un problème technique grave, un risque de perte de vos données ou bien la présence de nombreux virus ?

A Ne rien faire

B Contacter le support technique au numéro indiqué sur le message d'erreur

C Tenter de redémarrer votre ordinateur et, si le problème persiste, demander de l'aide à un ami

Que faire si un message bloquant votre ordinateur apparaît, signalant un problème technique grave, un risque de perte de vos données ou bien la présence de nombreux virus ?

Vous lancez un navigateur en mode privé, puis vous vous authentifiez
avec votre mot de passe pour accéder à votre profil.

Est-ce sans risque ?

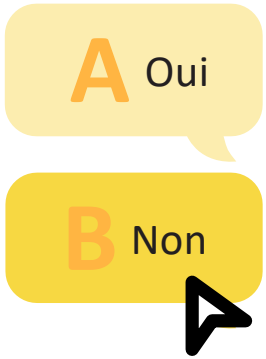
A Oui

B Non

Que faire si un message bloquant votre ordinateur apparaît, signalant un problème technique grave, un risque de perte de vos données ou bien la présence de nombreux virus ?

Vous lancez un navigateur en mode privé, puis vous vous authentifiez
avec votre mot de passe pour accéder à votre profil.

Est-ce sans risque ?



L’exemple de JEEP : prise de contrôle d’un véhicule connecté à partir d’un CD et un smartphone. Démo promotionnelle avec un journaliste au volant.

https://www.lemonde.fr/pixels/article/2015/07/22/deux-chercheurs-parviennent-a-pirater-une-voiture-a-distance_4694137_4408996.html

L’exemple de l’hydrolienne Sabella D10 : Cryptolocker Locky diffusé par mail à une employée et demande de rançon de 4000€. 15 jours d’arrêt.
https://www.sciencesetavenir.fr/high-tech/informatique/l-hydrolienne-sabella-bloquee-par-un-virus-chiffreur_11366

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

L’ingénierie sociale et les faux sites Internet

Dans le cadre de la sécurité de l'information, l'ingénierie sociale est une technique de manipulation utilisée par les (cyber)criminels pour inciter les gens à partager des informations confidentielles.

Elle mise sur l'instinct fondamental de l'être humain à faire confiance pour voler des informations personnelles et corporatives qui peuvent ensuite être utilisées pour commettre d'autres (cyber)crimes.

Plusieurs modes complexes

Phase d'appâtage (baiting)

Hameçonnage (phishing, smishing, vishing)

Utilisation de prétextes et faux-semblants

Quid pro quo (une chose pour une autre)

Harponnage (Spear phishing)

Les ressorts de l'Ingénierie sociale

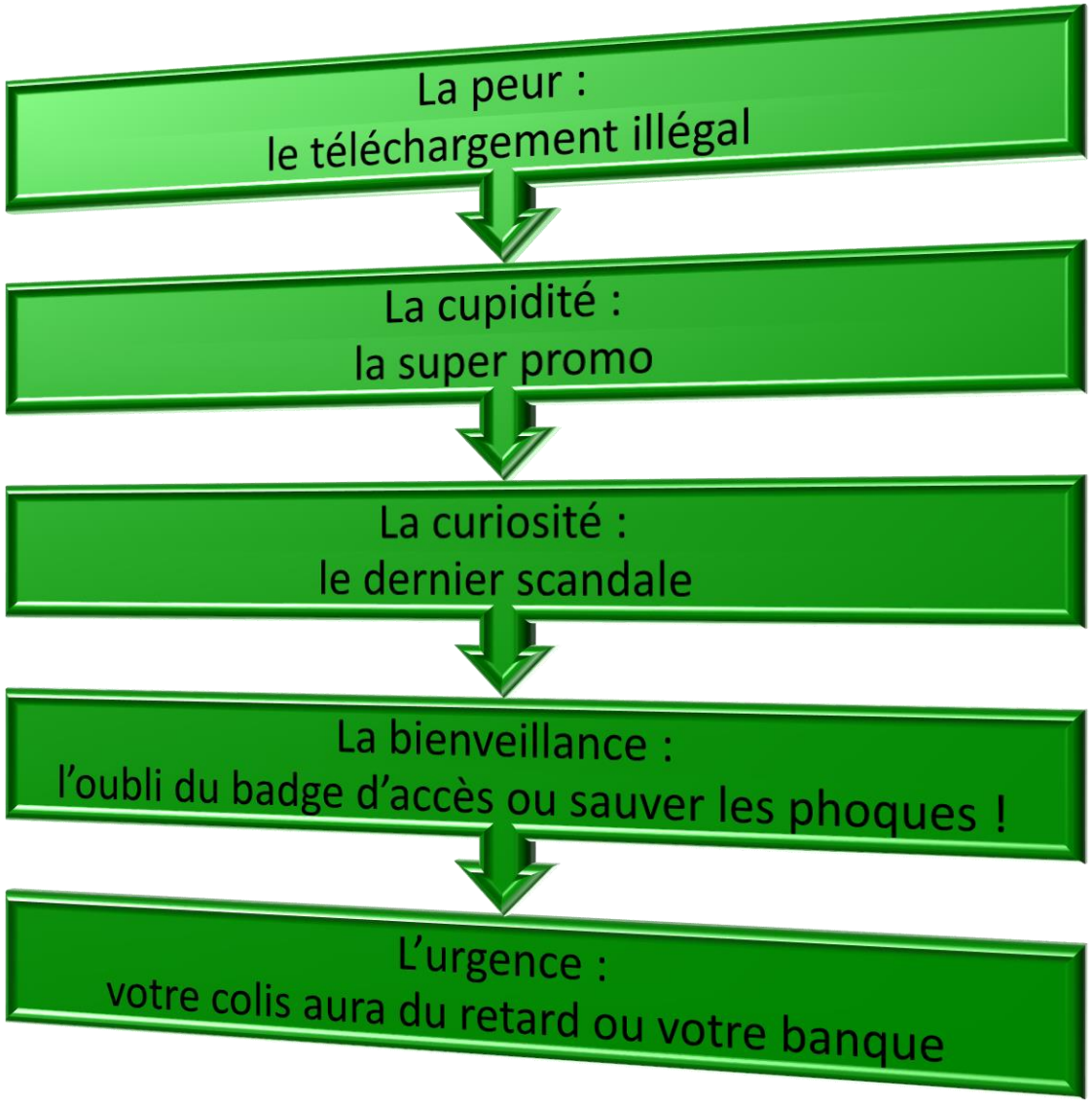


Illustration en vidéo

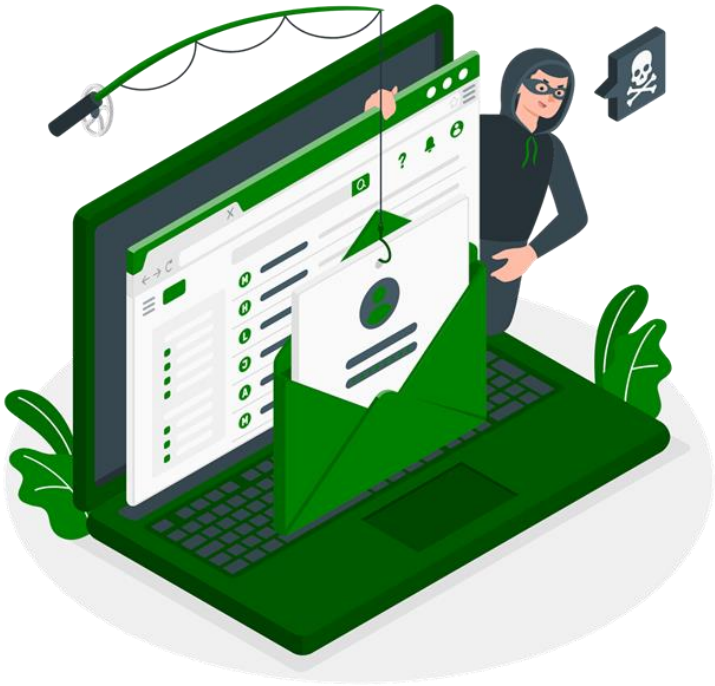
Mot de passe volé par un logiciel malveillant

Avec l'aimable autorisation de l'agence Cases luembourg

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Le Phishing (hameçonnage)

L’hameçonnage (phishing)



La pêche aux infos personnelles

L'Assurance Maladie — mon compte — mon parcours d'assuré

Bonjour ,

Nous vous informons que vous avez un remboursement en attente d'un montant de **169,20 €** sur votre espace personnel.

La carte enregistrée sur votre espace personnel n'a pas été créditée pour le motif suivant :

Le numéro de mobile enregistré sur votre espace personnel ne correspond pas à celui associé à votre compte bancaire.

Détails de remboursement:

Référence : AWL-20/982KDJ
Montant: : **169,20 €**

Pour accepter le paiement rapide en ligne, cliquez sur le lien suivant et sélectionnez une méthode de remboursement.

- Modifier mes informations personnelles.

Votre assurance maladie
18 5375 Boulevard de Vaugirard, 75015 Paris, France

Autres exemples de mail tendancieux

Message du 20/10/21 02:10
De : "Group Service" <pimkies@dfyoxc.owler.com>
A :
Copie à :
Objet : Asurance Maladie | Ameli.Fr

Adresse douteuse

De : E-service Clients BRED <BRED_secureID9593.noreply@zwina.com>
Envoyé : Thursday, October 29, 2020 9:51:42 AM
À : prenom.nom@courriel.fr
Objet : Au sujet de la sécurité de votre compte! #Re-664366

L'urgence…

SÉCURITÉ SOCIALE
L'Assurance Maladie

Bonjour

Votre caisse d'assurance maladie vous informe que vos remboursements de frais à recevoir

Nous vous demandons de mettre à jour vos données pour que votre remboursement soit effectué dans les plus délais.

Montant: 249.98 Euro

Référence: Ameli-A8005W

https://www.assure.ameli.fr

Nous vous remercions et nous vours prions agréer nos salutations distingués.

Votre caisse d'assurance maladie Ameli

L'aubaine !

Exemple un peu moins grossier

Attrait

Mise en confiance

Ce lien vous renverra vers un site frauduleux

Ce site existe, c'est une vitrine pour le dispositif PASRAU, soutenu par le Groupement d'intérêt public de modernisation des intérêt déclarations sociales (GIP-MDS) qui édite le site Net-Entreprise.fr

Exemple par SMS

Les Smartphone Android sont de plus en plus réactifs.

Google propose de bloquer et de signaler.

CONSEILLER NUMÉRIQUE France services

AGRICULTURES & TERRITOIRES CHAMBRE D'AGRICULTURE LOIR-ET-CHER

Quels Indices ?

1. Une notification de la messagerie ou de l'antivirus
➔ N'ignorez pas leur avertissement et assurez-vous régulièrement que votre antivirus est activé et à jour.

2. Un email d'un service ou d'une société dont vous n'êtes pas client.

3. Un nom d'expéditeur inhabituel.

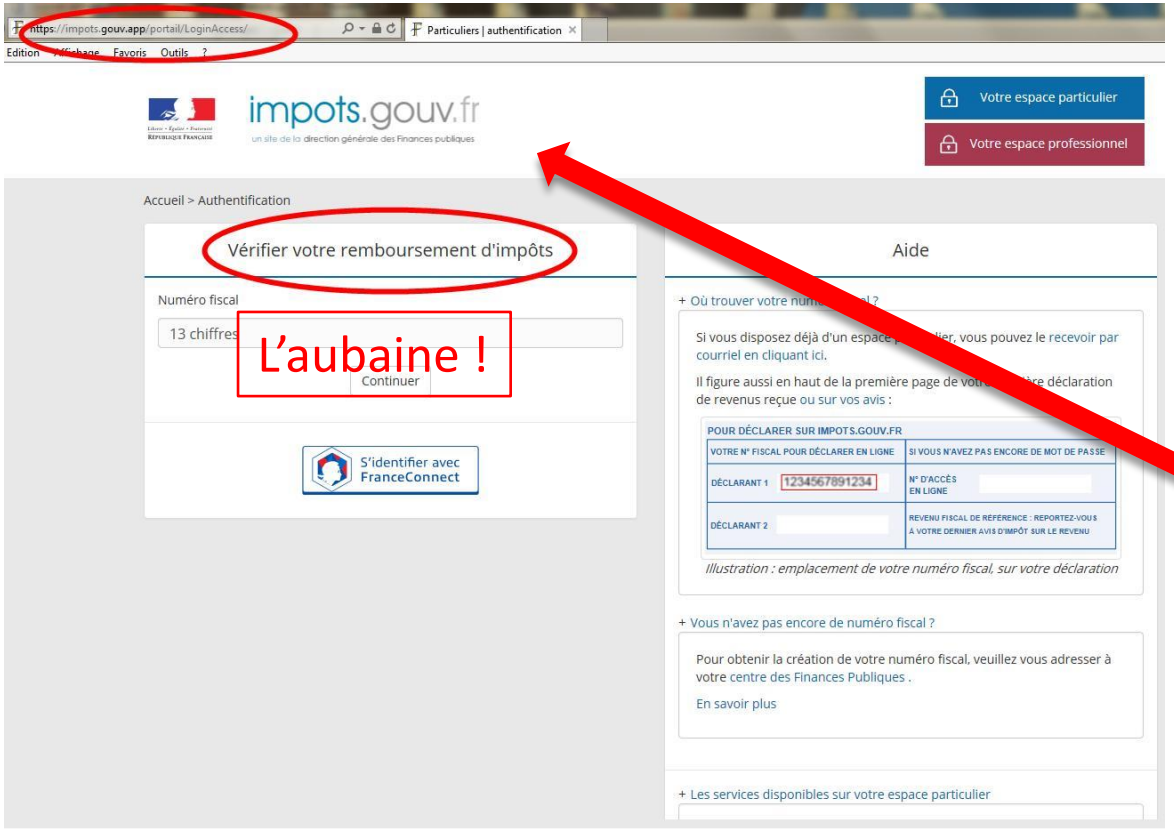
4. Une adresse d'expédition fantaisiste.

5. Un lien court / masqué / incompréhensible.

6. Le père noël : Un colis inattendu, un gain subit, un remboursement inespéré ou son complice le père fouettard : Une facture impayée, un compte bloqué, une carte désactivée

7. Une incitation à cliquer sur un lien ou une pièce-jointe

Phishing : Exemple de faux site



impots.gouv.app

≠

impôts.gouv.fr

➔ Vous remarquez que les 2 sites sont en http«S» !!

Un cas concret

Le phishing

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

5 RÉFLEXES À AVOIR LORS DE LA RÉCEPTION D'UN COURRIEL

5 RÉFLEXES AVEC LES COURRIELS

N'AYEZ JAMAIS PAS UNE CONFIANCE AVEUGLE DANS LE NOM DE L'EXPÉDITEUR

MÉFIEZ-VOUS TOUJOURS DES PIÈCES JOINTES

NE RÉPONDEZ JAMAIS À UNE DEMANDE D'INFORMATIONS CONFIDENTIELLES

MEME SI CA VOUS SEMBLE OFFICIEL NE CLIQUEZ PAS LE LIEN DANS LE MAIL

PASSEZ TOUJOURS VOTRE SOURIS AU-DESSUS DES LIENS

FAITES ATTENTION AUX CARACTÈRES ACCENTUÉS DANS LE TEXTE ET A LA QUALITÉ DU FRANÇAIS OU DE LA LANGUE PRATIQUÉE PAR VOTRE INTERLOCUTEUR

PARAMÉTREZ CORRECTEMENT VOTRE LOGICIEL DE MESSAGERIE

CONSEILLER NUMÉRIQUE France services

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE LOIR-ET-CHER

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

LES BOTNETS

Une menace Sérieuse !

Qu’est-ce qu’un botnet ? Définition

- **Groupe d'ordinateurs** ou de dispositifs **sous** le **contrôle** d'un attaquant, utilisé pour mener des activités malveillantes contre une victime ciblée.

- Combinaison des mots “robot” et “réseau” (*network* en anglais) pour représenter la nature d'une cyberattaque utilisant un botnet.

- Responsables de certaines des pannes Internet les plus répandues, mettant hors service de grandes organisations et des infrastructures de réseau à partir d'une attaque par déni de service distribué (DDoS).

- Créer un réseau d’appareils « zombies ».

Des usages multiples

- **Lire et écrire des données système** : un attaquant demande aux appareils d'envoyer des fichiers à un serveur central qui les examinera pour y déceler d'éventuelles données sensibles.
- **Envoyer des spams par e-mail : accès aux comptes de messagerie =**
  → envoyer des courriels à des destinataires ciblés.
  → L'email peut contenir un **malware** pour le **propager**
  → l'utiliser dans une **campagne de phishing.**
- **Surveiller l'activité des utilisateurs** : Pas rare que le logiciel malveillant d'un botnet comprenne un keylogger qui **enregistre** les frappes sur le **clavier de l'utilisateur** et **envoie** les informations volées **à un serveur** contrôlé par l'attaquant, ce qui lui permet d'**accéder** à des **comptes en ligne** comme des sites bancaires.
- Analyser le réseau local à la **recherche de vulnérabilités supplémentaires** : scanne autant de dispositifs que possible **depuis** le poste local donc **derrière le pare feu**
  Si **micrologiciel obsolète**, le malware peut **exploiter la vulnérabilité** et **ajouter** l'appareil vulnérable au **réseau zombie**.

Exemple de DDoS célèbre : Amazon

- Une **attaque par déni de service** a pour but de **surcharger un réseau ou une cible afin d'entraver son bon fonctionnement**.

- **Amazon Web Services**, division d'Amazon dédiée aux services de cloud computing pour les entreprises et particuliers, a subi en **février 2020** une **attaque DDoS** sans précédent **pendant 3 jours** de manière **ininterrompue**, enregistrant un volume record de **2,3 Térabits par seconde**. Malgré tout, AWS a été capable d'encaisser sans connaître de dysfonctionnements majeurs.

- **Plus grosse attaque DDoS jamais enregistrée**, avec un volume de surcharge inédit, on parle de **"téra-attaque"**.
  Pour anticiper ce type d'attaque dites Volumétriques,, il est nécessaire de **protéger en amont ses accès internet** par des solutions hébergées au cœur du réseau FAI (Fournisseur d'Accès Internet) ou d'installer dans le cloud une solution de redirection pour **nettoyer et supprimer le trafic indésirable**.

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Les Logiciels malveillants / Virus

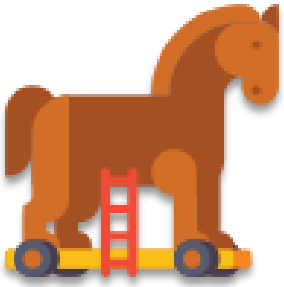
Différents types

Virus :
code qui se colle à un autre programme

Ransomware :
Blockage/cryptage puis rançon

Spyware :
Enregistrer tout

Scareware :
Faire peur pour pousser à la faute ou chantage



Cheval de Troie (Trojan) :
Faire ouvrir les portes puis répandre d'autres armes

Keylogger :
Enregistre les frappes du clavier

Adware :
Diffusion de publicités

Quels symptômes

Ouverture inopinée de fenêtres (Popups)

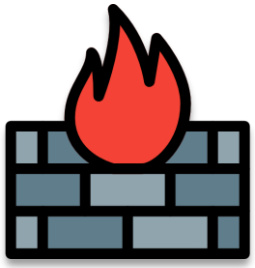
Blocage de certaines ou toutes fonctions de l'ordinateur

Lenteur inhabituelle, Blocages

Apparition/disparition d'icônes sur le Bureau

Réduire le risque

Avoir un appareil et des logiciels à jour



Avoir un pare-feu actif

Smartphones/tablettes
Téléchargez uniquement sur les magasins officiels

Avoir un antivirus actif ET à jour

Avoir un navigateur web à jour

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Ransomware (Rançongiciels)

EXTORSION de FONDS !

Action :

- **Bloque l'accès à un ordinateur ou à ses fichiers en les chiffrant.**
- **Demande une rançon pour obtenir l'accès.**

Vecteurs de Diffusion :

- **Piece jointe ou lien dans un email**
- **Navigation sur un site compromis (clic sur lien ou pas)**
- **Intrusion dans le système.**

But recherché :

- **Argent**
- **Terreur**

Cibles principales:

- **PME, Grands groupes, Administrations, gouvernements, particuliers.**

Se protéger

- Sauvegarde -

- Sauvegarde -

- Sauvegarde -

- Sauvegarde -

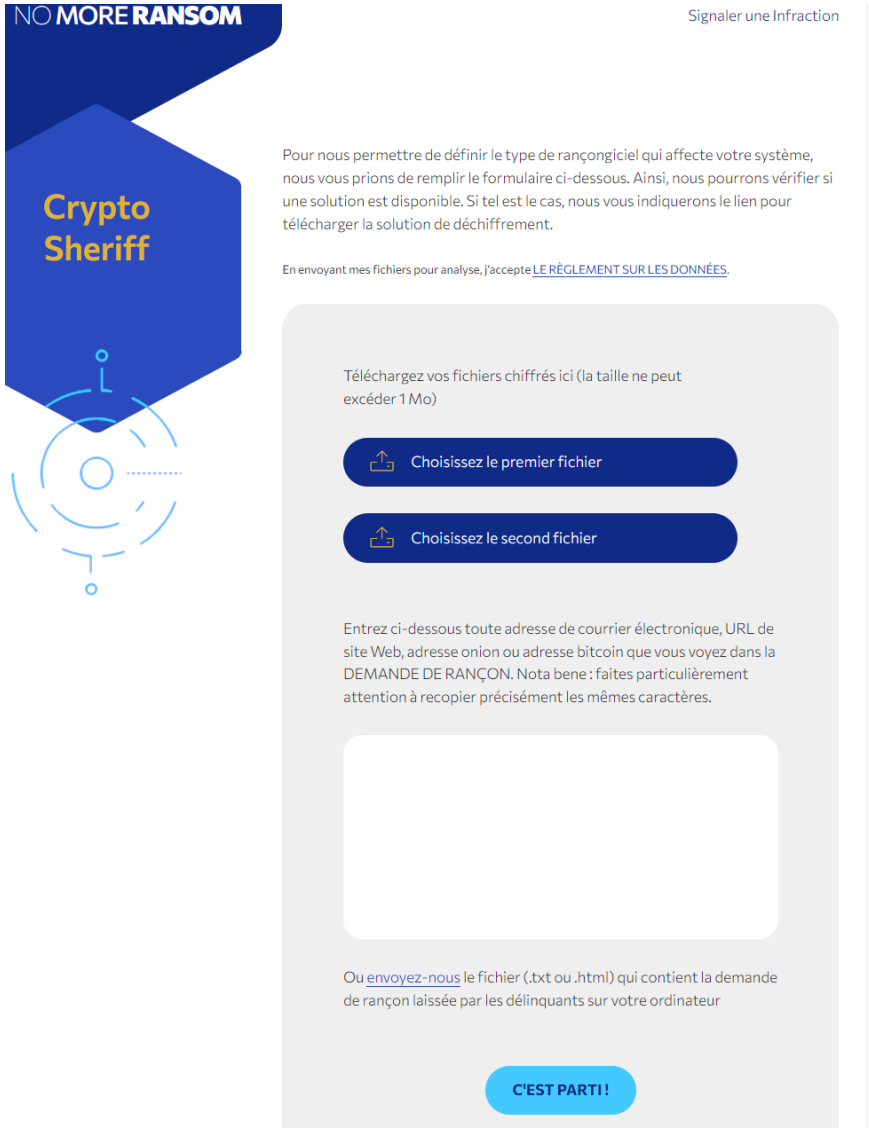
- Sauvegarde -

- Sauvegarde -

- Sauvegarde -

- Sauvegarde -

Outils en ligne



- Crypto Sheriff : (Nécessite 2 fichiers cryptés) www.nomoreransom.org/fr/index.html

- Liste d'outils de déchiffrement : moreransom.org/fr/decryption-tools.html

Des ransomwares Célèbres

- **WinLock :** 2010 - Affiche des images pornographiques - rançon par SMS surtaxé
- **Cryptolocker :** 2013 - Cryptage RSA2048 bits + serveur C&C. Propagation sur réseau comme un vers.
- **SamSam :** 2015 puis 2018 (institutions) - Par serveurs linux (faille redHat Jbtools)
- **Locky :** 2016 - Macro dans une facture Word
- **Petya :** 2016 - Remplace le MBR et chiffre la MFT (dès le boot) - Puis **«NotPetya» =** Exploite la Faille réseau EternalBlue divulguée par la NSA
- **Hermés 2.1 :** 2017 **-** Cryptage RSA-2048 – Rançon Bitcoins
- **WannaCry :** 2017 épidémie mondiale. Rançon Bitcoins. EternalBlue - Faille Windows mise à jour 2 mois avant! = 230 000 Pc touchés.
- **RYUK :** 2018 **-** Désactive la restauration système - Issu de Hermés 2.1
  2021 - réplication sur réseau
- **GrandCrab :** 2018 - PJ mail «romantique» puis chantage pornographique - Chat pour apprendre a payer en Bitcoins ! - Arrêt 2019 après + 2Milliards$
- **Zeppelin :** 2019 - multiple cryptage - Ransomware as a service (Raas) = vendu plusieurs millions - Grosses entreprises (Santé/Techno/Enseignement)
- **REvil/Sodinokibi :** 2019 - Membres de GranCrab (?) - Raas - Apple, Acer, P. Fabre…

Un exemple d'attaque par RansomWare

Acer, victime d'une attaque par ransomwares inédite avec 50 millions de dollars de rançon

- En **2021**, le fabricant informatique **Acer** a été victime d'un rançongiciel pour lequel il s'est vu demander par les hackers la somme record de **50 millions de dollars** en échange de la restitution de ses données. Ceux-ci menaçaient notamment de faire fuiter des **informations sensibles**, comme des documents financiers de ses filiales en Australie, Malaisie, Vietnam, Indonésie, Singapour, USA, Inde, Philippines et au Japon. Acer a émis une contre-proposition de 10 millions de dollars, refusée par les hackers.

- **Motif évoqué par le groupe Desorden** : « prouver notre point de vue selon lequel Acer est très en retard dans ses moyens de cybersécurité sur la protection de ses données et est un **réseau mondial de serveurs vulnérables**. »

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Arnaque au faux ordre de virement bancaire (FOVI)

Faux Ordre Virement Interbancaire

Obtenir un Ordre de Virement

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.

FOVI

DE QUOI PARLE T-ON ?

- Faux tests informatiques.
- Usurpation d'identité (directeur).
- Action directe auprès de la banque détentrice des comptes.
- Utilisation d'un logiciel espion (cheval de Troie).

Par téléphone

Collecte en amont

Ton persuasif et/ou autoritaire

Méthodes très élaborées qui reposent essentiellement sur la manipulation

Cadre habituel ou suite à des négociations imprévues et récentes

Possède des détails précis sur l'entreprise et son PDG

PRECAUTIONS

- ✓ Utiliser des logiciels originaux et à jour sur le réseau informatique et les ordinateurs de l'entreprise.
- ✓ Protéger ses ordinateurs par un antivirus performant et à jour.
- ✓ Ne pas mettre d'informations stratégiques sur le site Internet de l'entreprise.
- ✓ Sensibiliser l'ensemble des personnels sur ce type d'escroquerie.
- ✓ Alerter les personnels sur l'importance de ne pas divulguer sur les réseaux sociaux des informations concernant l'entreprise.
- ✓ Instaurer un protocole de virements bancaires connus uniquement des responsables (banque, chef entreprise, comptable). Créer des mots d'authentification pour réaliser ces virements.
- ✓ Exclure les paiements de fin de semaine afin de pouvoir réagir rapidement auprès des banques en cas d'attaque avérée et réalisée par les escrocs.
- ✓ Accroître la vigilance lors des périodes scolaires et des remplacements de titulaires de postes par des stagiaires

SI VOUS ÊTES VICTIME

- FAITES UN SIGNALEMENT
- DEMANDEZ LA SUSPENSION DU VIREMENT
- ALERTEZ LA BANQUE ET DEMANDEZ LE RETOUR DES FONDS
- CONSERVEZ LES PREUVES
- CHANGEZ LE MOT DE PASSE
- DÉPOSEZ PLAINTE

Sefri-Cime : une arnaque au président colossale

L'arnaque au président est une attaque qui consiste à se faire passer pour un dirigeant afin de demander des ordres de virement vers un faux compte.

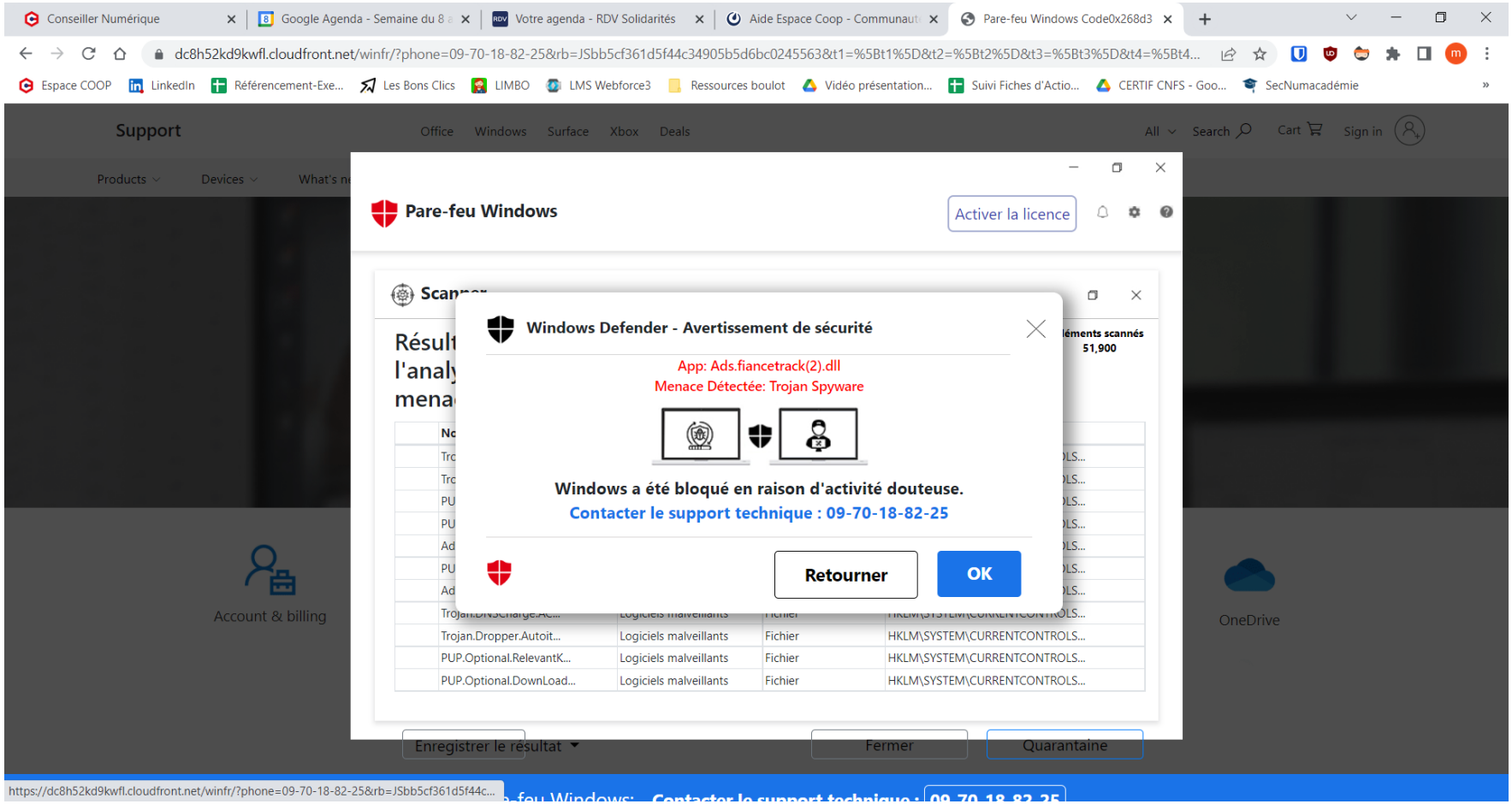
- **Sefri-Cime,** promoteur immobilier, a subi une arnaque au président de grande ampleur.
  Une **comptable** a reçu des **emails** d'un cybercriminel se faisant passer pour **son dirigeant**, qui lui demandait **d'effectuer discrètement des opérations bancaires** en vue d'une prochaine introduction en bourse.
  Un **deuxième escroc**, se faisant passer pour un **avocat** de la société KPMG, a également demandé des **virements bancaires** à cette même personne.

- Au total, **33 millions** d'euros ont ainsi été détournés par les cybercriminels, un montant record en France.

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

L’arnaque au faux support informatique

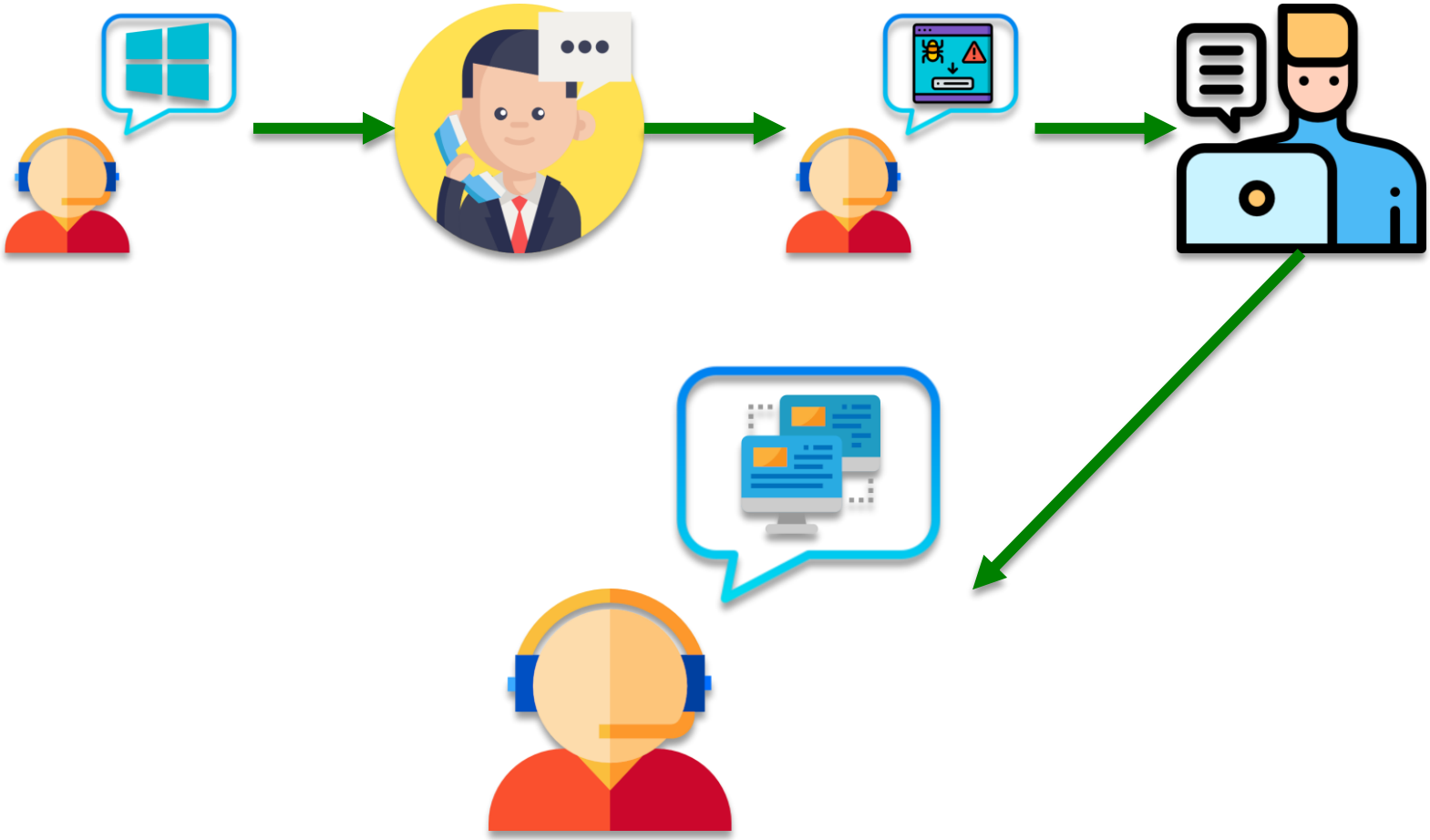
Scénario d’un faux support informatique



CONSEILLER NUMÉRIQUE France services

AGRICULTURES & TERRITOIRES CHAMBRE D'AGRICULTURE LOIR-ET-CHER

Le principe



Les prétextes

- Simulation d'infection de virus sur votre ordinateur :
  La personne essaiera ainsi de vous vendre un antivirus pour éviter le problème à l'avenir.

- Machine soi-disant lente et dysfonctionnante :
  La personne va supprimer quelques fichiers temporaires sur votre disque dur et aller modifier des paramètres en vous embrouillant vocalement, afin de vous faire croire qu'elle à réellement résolu des problèmes sur votre ordinateur.

- Tentative d'installation de logiciels douteux, voire malveillants :
  La personne va reprendre de faux arguments comme utilisés ci-dessus, afin de naviguer à distance sur votre ordinateur, pour y installer des logiciels inutiles, voire douteux/dangereux. (Cas plus rare)

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Arnaque à la romance (nigériane)

Arnaque à la romance (Escroquerie Sentimentale)

- ✓ Faux Profils attractif - Ca « matche »
- ✓ Mise en confiance/Déclaration d'amour
- ✓ Situation difficile
- ✓ Soucis de santé
- ✓ Frais imprévus
- ✓ Urgence soudaine
- ✓ Demande d'argent
- ✓ Disparition

Quels sont les signes ?

Que (ne pas) faire ?

Soyez très prudent quant aux données personnelles que vous partagez sur les réseaux sociaux / sites de rencontre.

Pensez toujours aux risques. Les escrocs sont présents sur les sites les plus réputés.

Ne vous précipitez pas et posez des questions.

Vérifiez que la photo ou le profil n'est pas utilisé sur d'autres sites.

Soyez **attentif** aux fautes d'orthographe/grammaire, à leurs **contradictions** et **excuses**, par ex. la panne de caméra.

Ne partagez pas d'informations qui pourraient vous amener à subir du chantage.

Si vous acceptez une rencontre de visu, dites à vos **amis/famille** où vous allez.

Méfiez-vous des demandes de fonds.
N'envoyez jamais ni argent, ni données de carte de crédit, de compte en ligne, de copies de documents personnels.

Ne leur versez jamais de **paiement initial**.

Ne transférez pas d'argent pour un tiers : le blanchiment d'argent est un délit pénal.

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Signaler une fraude à la carte bancaire (Perceval) ou une arnaque : Thésée, Pharos (Démarche en ligne)

Perceval : https://www.service-public.fr/particuliers/vosdroits/R46526

Signaler une fraude à la carte bancaire (Perceval)

- Service accessible via FranceConnect: Préparez vos identifiants et votre numéro de carte bancaire.
- Ce service permet de signaler une fraude à la carte bancaire si vous remplissez les conditions suivantes :
  - ❑Vous êtes toujours en possession de votre carte bancaire
  - ❑Vous n'êtes pas à l'origine des achats en ligne
  - ❑Vous avez déjà fait opposition à la carte auprès de votre banque

CONSEILLER NUMÉRIQUE France services

AGRICULTURES & TERRITOIRES CHAMBRE D'AGRICULTURE LOIR-ET-CHER

Pharos : https://www.internet-signalement.gouv.fr/PharosS1/

signaler un contenu illicite de l'Internet

Thésée : https://www.service-public.fr/particuliers/vosdroits/R47160

Signaler un ransomware ou rançongiciel (THESEE)

Ministère chargé de l'intérieur

Se munir d'une adresse mail

Si votre ordinateur est bloqué et qu'un message vous invite à verser de l'argent en échange d'un retour à la normale, vous pouvez signaler cette escroquerie.

Accéder à la démarche en ligne

Vérifié le 16 mai 2022 - Direction de l'information légale et administrative (Premier ministre)

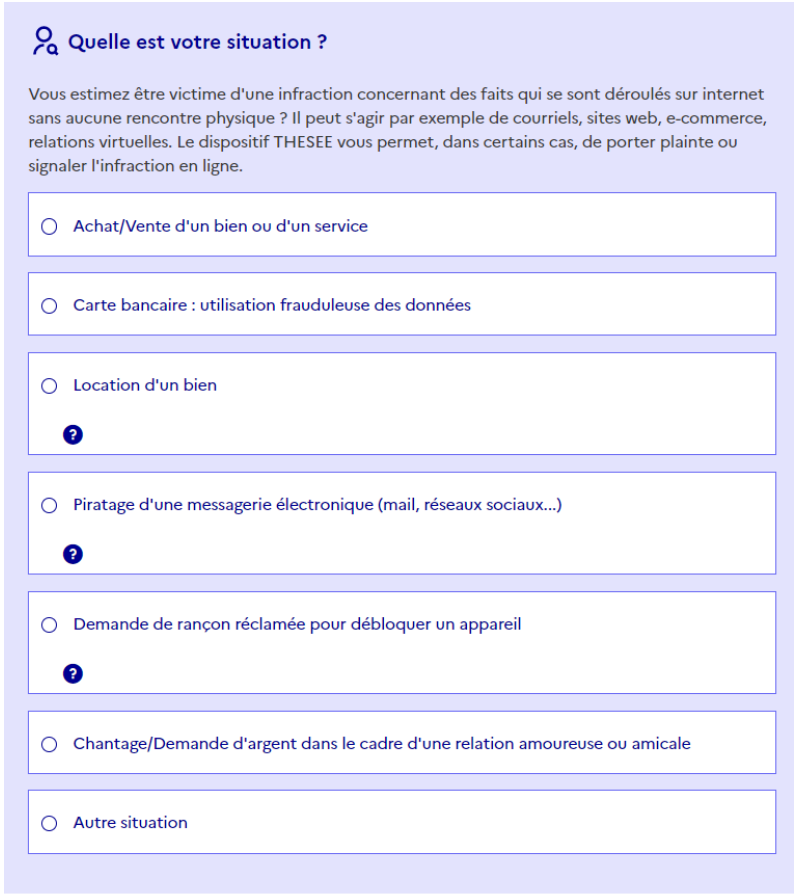
Pour toute explication, consulter les fiches pratiques :

→ Ransomware ou rançongiciel

Signalement global sur le service-public.fr

Arnaque sur internet (THESEE, Pharos, ...)

Certaines infractions relèvent de la cybercriminalité. Il peut s'agir de piratage de votre boite mail, d'extorsion d'argent pour débloquer votre ordinateur ou encore, d'un compte Facebook piraté.



Quelle est votre situation ?

Vous estimez être victime d'une infraction concernant des faits qui se sont déroulés sur internet sans aucune rencontre physique ? Il peut s'agir par exemple de courriels, sites web, e-commerce, relations virtuelles. Le dispositif THESEE vous permet, dans certains cas, de porter plainte ou signaler l'infraction en ligne.

- ○ Achat/Vente d'un bien ou d'un service
- ○ Carte bancaire : utilisation frauduleuse des données
- ○ Location d'un bien
- ○ Piratage d'une messagerie électronique (mail, réseaux sociaux...)
- ○ Demande de rançon réclamée pour débloquer un appareil
- ○ Chantage/Demande d'argent dans le cadre d'une relation amoureuse ou amicale
- ○ Autre situation

- Ransomware ou rançongiciel
- Piratage d'une messagerie électronique (mail, réseaux sociaux...)
- Phishing (hameçonnage)
- Fraude liée à un achat sur internet
- Fraude liée à une location sur internet
- Chantage / Menaces lors d'une relation amoureuse ou amicale sur internet

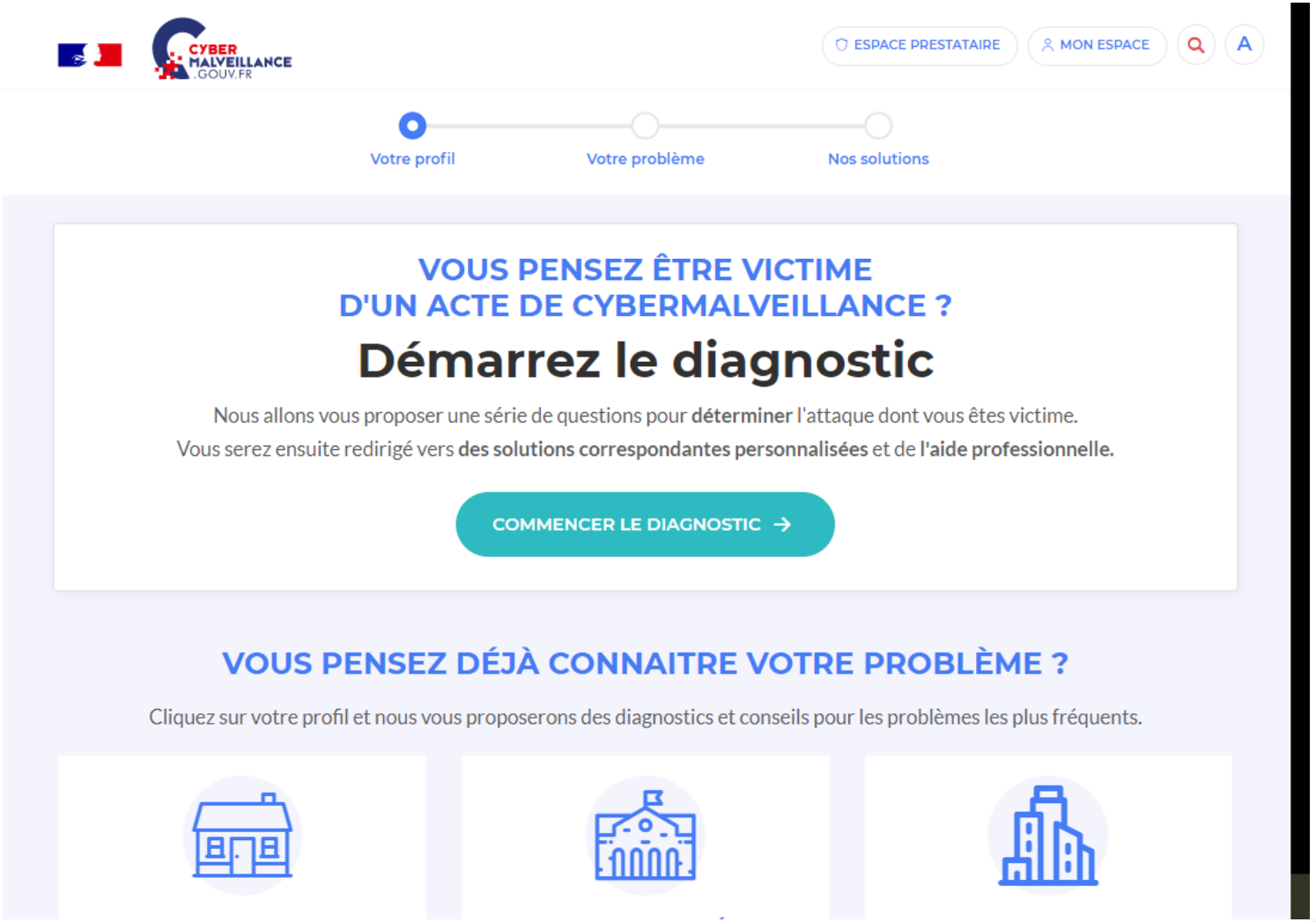
https://www.service-public.fr/particuliers/vosdroits/N31138

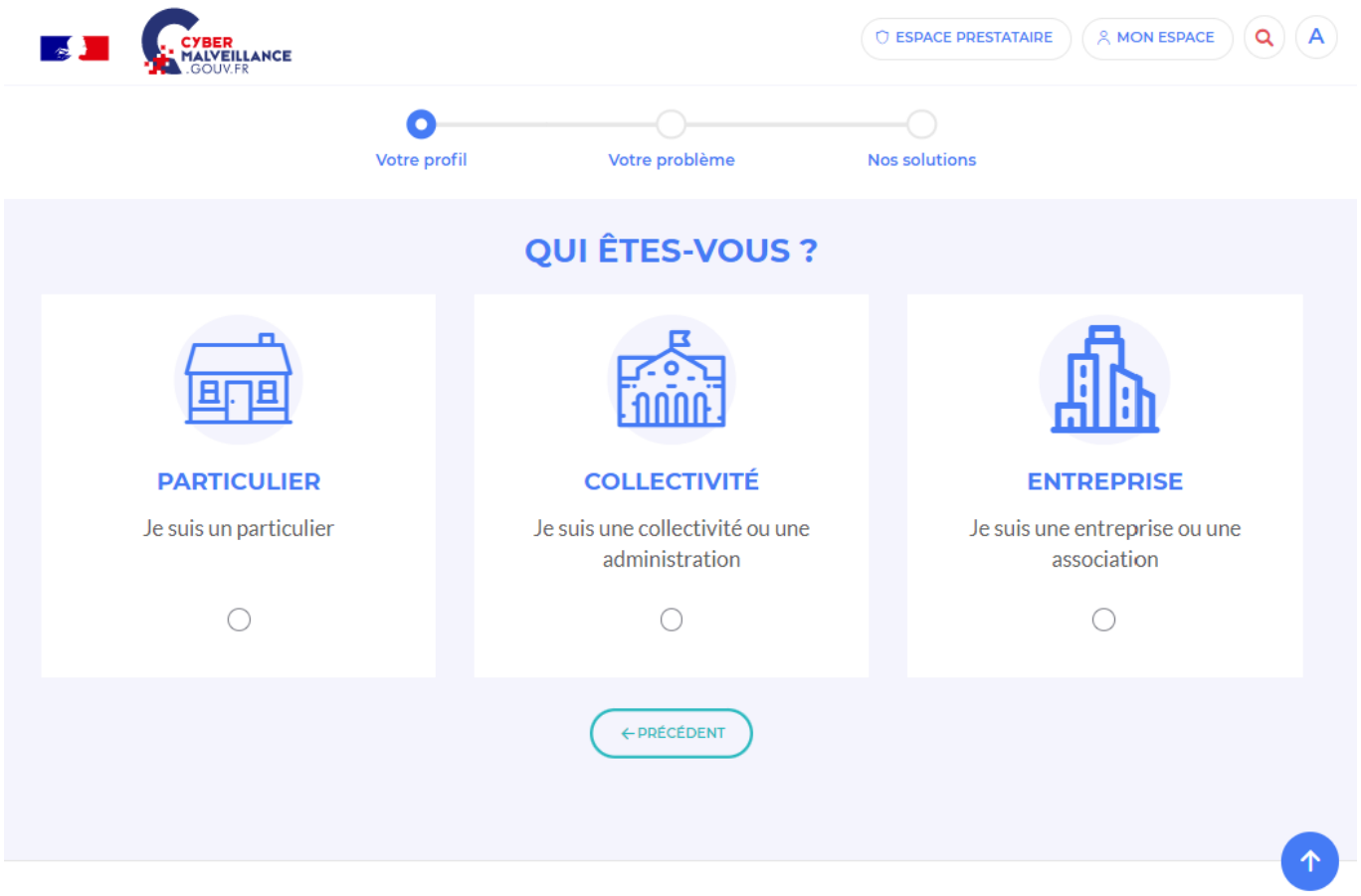
AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Conclusion

Diagnostic rapide en ligne

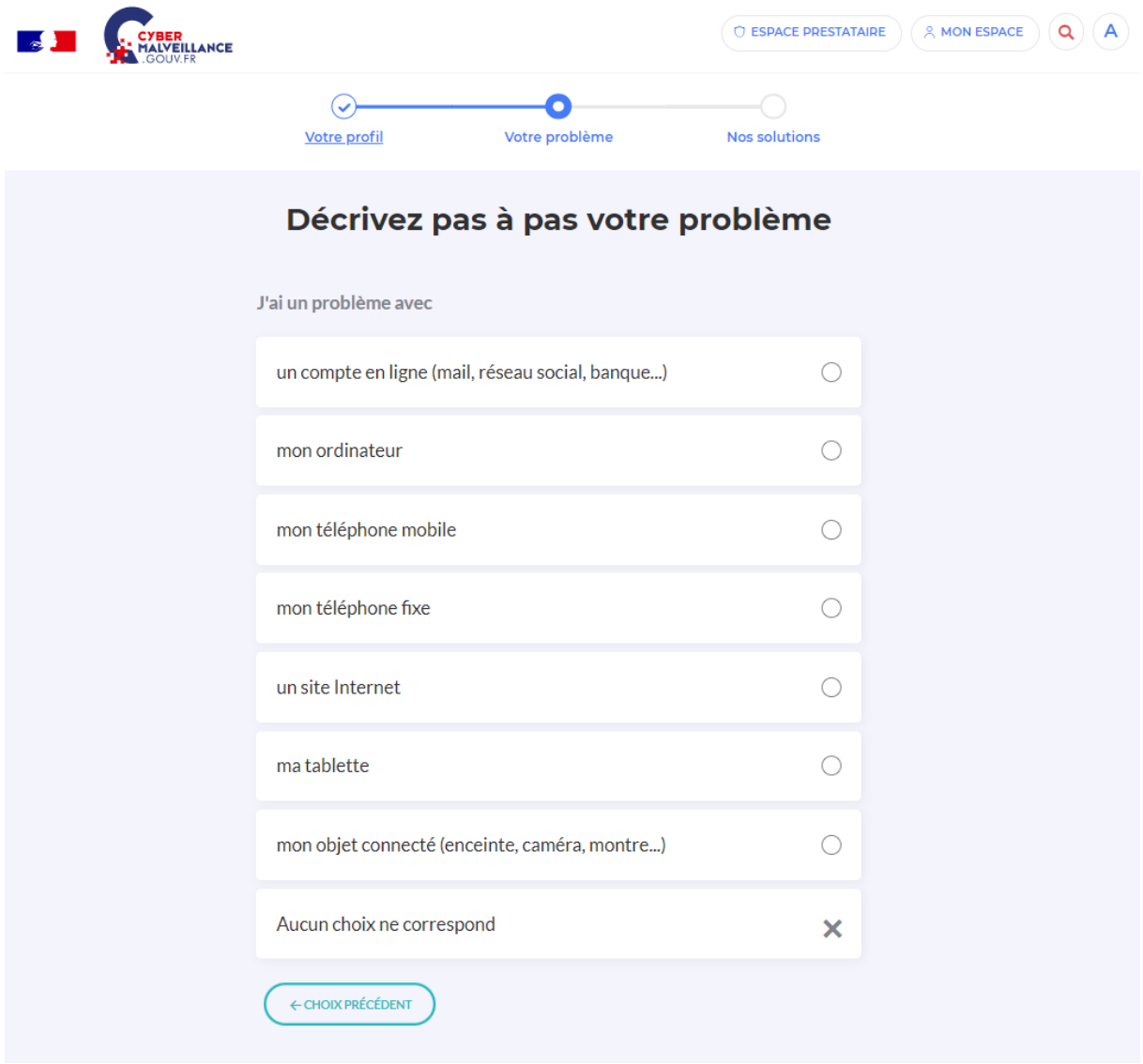
https://www.cybermalveillance.gouv.fr/diagnostic




CYBER MALVEILLANCE .GOUV.FR
ESPACE PRESTATAIRE
MON ESPACE
A
Votre profil
Votre problème
Nos solutions
QUI ÊTES-VOUS ?
PARTICULIER
Je suis un particulier
COLLECTIVITÉ
Je suis une collectivité ou une administration
ENTREPRISE
Je suis une entreprise ou une association
← PRÉCÉDENT
RÉPUBLIQUE FRANÇAISE
CYBER MALVEILLANCE .GOUV.FR
À PROPOS
Qui sommes-nous ?
DIVERS
Plan du site
NOUS SUIVRE

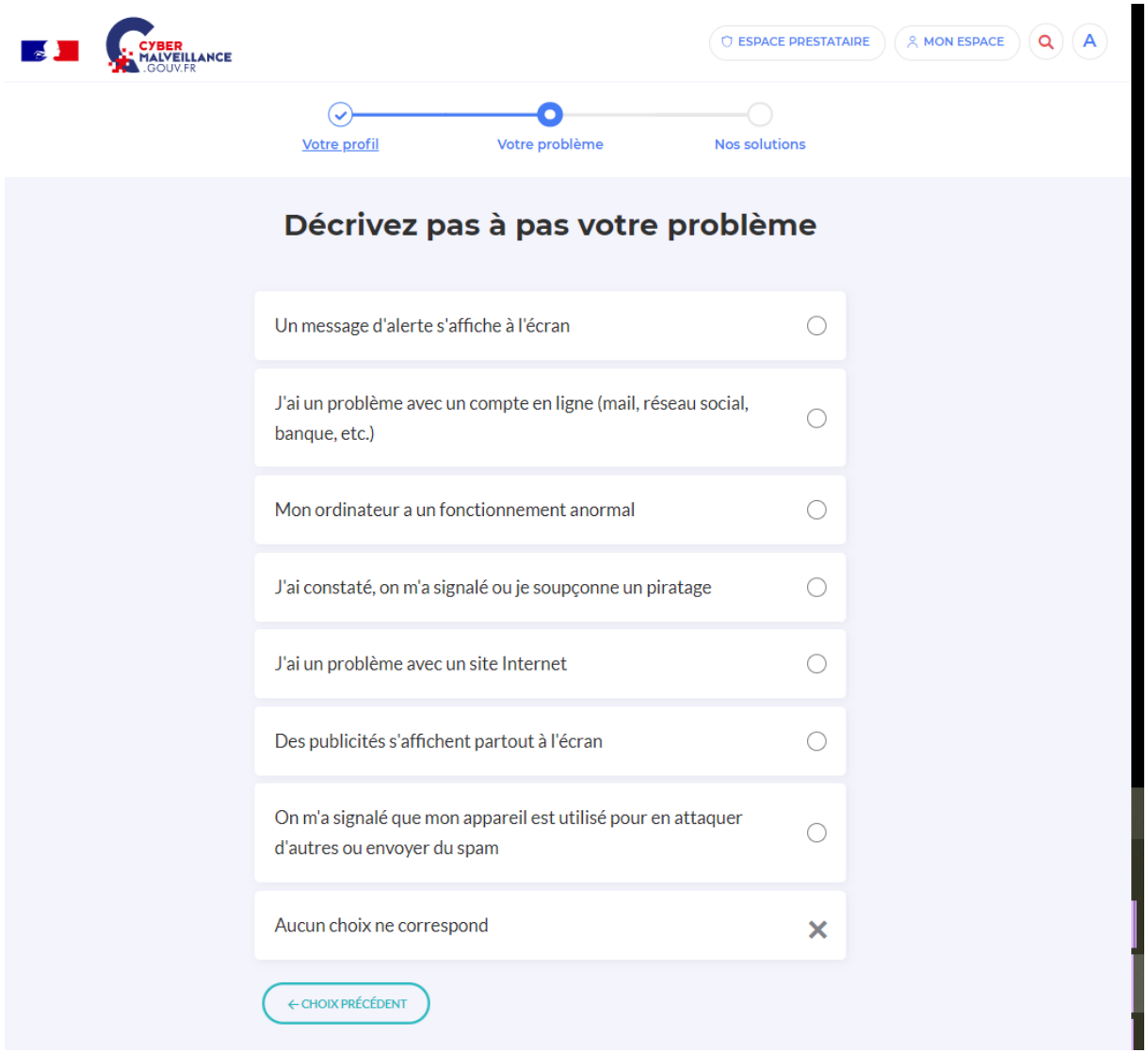
Diagnostic rapide en ligne

https://www.cybermalveillance.gouv.fr/diagnostic



CONSEILLER NUMÉRIQUE France services

AGRICULTURES & TERRITOIRES CHAMBRE D'AGRICULTURE LOIR-ET-CHER


CYBER MALVEILLANCE .GOUV.FR
ESPACE PRESTATAIRE
MON ESPACE
Votre profil
Votre problème
Nos solutions
Décrivez pas à pas votre problème
Un message d'alerte s'affiche à l'écran
J'ai un problème avec un compte en ligne (mail, réseau social, banque, etc.)
Mon ordinateur a un fonctionnement anormal
J'ai constaté, on m'a signalé ou je soupçonne un piratage
J'ai un problème avec un site Internet
Des publicités s'affichent partout à l'écran
On m'a signalé que mon appareil est utilisé pour en attaquer d'autres ou envoyer du spam
Aucun choix ne correspond
← CHOIX PRÉCÉDENT


CYBER MALVEILLANCE .GOUV.FR
ESPACE PRESTATAIRE
MON ESPACE
A
Votre profil
Votre problème
Nos solutions
Récapitulatif de votre situation / problème
Cliquez pour modifier vos réponses
Je pense être victime de cybermalveillance. Je suis un particulier
J'ai un problème avec mon ordinateur
Des publicités s'affichent partout à l'écran
← CHOIX PRÉCÉDENT
VALIDER →

AGRICULTURES & TERRITOIRES
CHAMBRE D'AGRICULTURE
LOIR-ET-CHER

Usurpation d'identité, comment s'en protéger ? Les conseils de Bercy

Quelques règles de base sont à appliquer :

- **Choisissez un mot de passe sûr** en alternant les majuscules et minuscules, les chiffres, etc.
- **N'utilisez pas un mot de passe unique sur tous vos comptes**, alternez-les en fonction des sites.
- **Ne partagez pas vos mots de passe** et prenez vos précautions lors de leur utilisation sur d'autres ordinateurs que le vôtre.
- **Vérifiez l'authenticité d'un expéditeur** avant d'envoyer des informations personnelles ou sensibles par mail.
- **Evitez d'inscrire votre adresse mail principale sur des sites dont vous n'êtes pas certain de la fiabilité.**
- **Soyez attentif à vos relevés de compte bancaire.**
- **Détruisez tout papier comportant des informations personnelles avant de le jeter**.

Quels recours en cas d'usurpation d'identité ?

- Si vous constatez une usurpation d'identité, **collectez tous les éléments prouvant l'infraction** (captures d'écrans, URL des pages concernées, justificatifs etc.).

Vous pourrez ensuite vous tourner vers le ou les sites sur lesquels l'usurpation d'identité a eu lieu et leur **demander d'intervenir pour la suppression des informations vous concernant**.

- Vous êtes par ailleurs en droit de déposer une **plainte pénale** auprès d'un commissariat de police, d'une gendarmerie ou du procureur de la République.
- La plateforme gouvernementale cybermalveillance.gouv.fr peut vous aider à identifier un organisme à même de vous accompagner dans vos démarches dans votre périmètre géographique.

Impunité ?

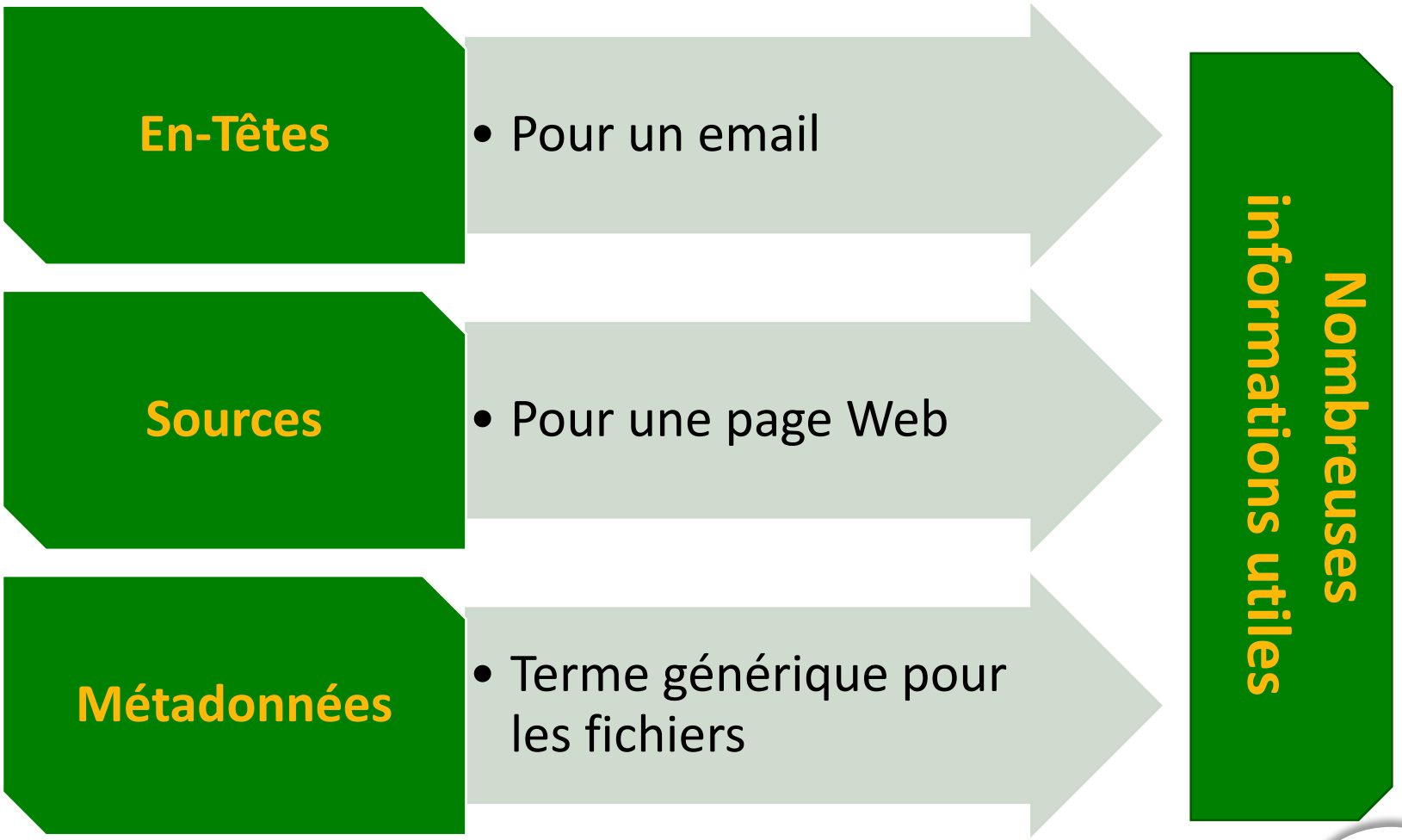
En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

• **Escroquerie** (article 313-1 du code pénal) : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (article 313-3 du code pénal).

• **Usurpation d'identité** (article 226-4-1 du code pénal) : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (article 225-5 du code pénal).

• **Accès frauduleux à un système de traitement automatisé de données** (article 323-1 du code pénal) : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. La tentative des délits prévus par les articles 323-1 à 323-3-1 est passible des mêmes peines.

Pour aller plus loin



Sources

Sources hameçonnage :
https://www.cybermalveillance.gouv.fr/medias/2020/01/Memo_hameconnage.pdf
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing
https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage
https://www.arobase.org/phishing/identifier-message-piege-phishing.htm

Sources arnaque sentimentale :

Sources définition ingénierie sociale :
https://www.kaspersky.fr/resource-center/threats/malware-social-engineering
https://www.kaspersky.fr/resource-center/definitions/what-is-social-engineering
https://www.onisep.fr/Ressources/Univers-Formation/Formations/Post-bac/diplome-d-etat-d-ingenierie-sociale

Sources Botnets : https://www.proofpoint.com/fr/threat-reference/botnet

Sources vers informatique : https://softwarelab.org/fr/ver-informatique/

Sources

Ressources générales :

https://www.economie.gouv.fr/particuliers/protection-usurpation-identite

https://www.cybermalveillance.gouv.fr/cybermenaces

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite

https://www.interieur.gouv.fr/Contact/Contacter-une-brigade-de-gendarmerie-ou-un-commissariat-de-police

Choisir un mot de passe solide : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

Collectivités locales : https://www.collectivites-locales.gouv.fr/sites/default/files/migration/depliant_fovi_3pages.pdf

Agence Nationale de la sécurité des systèmes d'information ANSSI : https://www.ssi.gouv.fr/

Mooc : https://secnumacademie.gouv.fr/

Chaine Luxembourgeoise https://www.youtube.com/user/CASESLuxembourg/about
https://trustbox.cases.lu/

Comment reconnaître un mail de phishing ou d'hameçonnage : https://dai.ly/x850yry

Sources

Sources Exemples :
https://www.databreaches.net/
https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html

Sources Signalement :
Tout contenu illicite : https://www.internet-signalement.gouv.fr/
SPAM par mail : https://signal-spam.fr/
SPAM vocal et SMS : https://www.33700.fr/

Merci de votre participation !

Cet atelier vous était présenté par :

Franck JACQUET
Conseiller Numérique
Pôle Ressources/Légumes

11-13-15 Rue Louis Joseph Philippe
CS41808
41018 Blois
Tél. : 02 54 55 20 00
Mobile : (+33) 06 35 54 24 91
chambre-agriculture-Loir-et-Cher

Financé par GOUVERNEMENT Liberté Égalité Fraternité
FRANCE RELANCE
Financé par l'Union européenne NextGenerationEU