SENSIBILISATION CYBERSÉCURITÉ 2025-2026

Ce livret a pour objectif de rappeler les principaux enseignements issus des ateliers de sensibilisation animés par la Gendarmerie de la Lozère et le Centre de Gestion de la Fonction Publique Territoriale de la Lozère.

Il synthétise les risques majeurs liés aux cybermenaces ainsi que les bonnes pratiques de sécurité numérique à adopter au quotidien.

Il présente également les grands principes du Règlement général sur la protection des données (RGPD), en rappelant les obligations qui encadrent la collecte, l'utilisation et la protection des données personnelles dans le cadre des missions de service public.

L'objectif est de fournir des repères clairs et opérationnels afin de renforcer la vigilance et la conformité au sein de la collectivité.

GENDARMERIE NATIONALE
GROUPEMENT DE LA LOZÈRE

CDG48
CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DE LA LOZÈRE

LE HAMEÇONNAGE

Chorus Pro

Bonjour,

Vous trouverez ci-dessous vo

Factures reçues :

VOTRE FACTURE

Cordialement,

Chorus Pro

Avis de contravention ref: 30016032

Bonjour

ANTAI-INFO-AMENDES

Vous avez un retard paiement de **135,00€**
Dossier référence **30016032**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES

Bonjour,

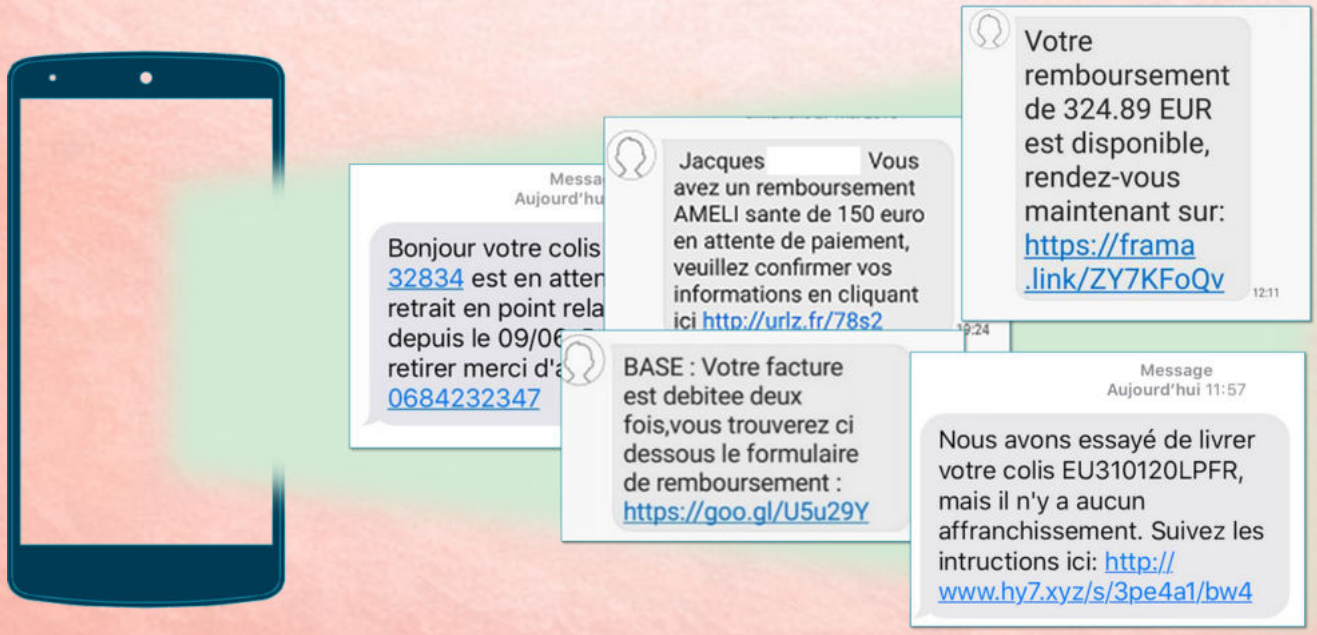
Après les derniers calculs annuel sur l'exercice 2020 et les projection sur 2021, nous sommes heureux de vous annoncer qu'une ligne budgétaire exceptionnelle a été débloqué pour relancer l'économie locale.

Aux fins de raccourcir les délais de traitement, il est ainsi demandé à chaque collectivité territoriale de remplir le formulaire dont le lien figure ci-dessous et de générer votre candidature au plus vite :

https://www.impots.gouv.fr/recensementCL_2021

Cordialement.

Par mail ou par SMS, le hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.



Votre remboursement de 324.89 EUR est disponible, rendez-vous maintenant sur: https://frama.link/ZY7KFoQv

Jacques Vous avez un remboursement AMELI sante de 150 euro en attente de paiement, veuillez confirmer vos informations en cliquant ici http://urlz.fr/78s2

Bonjour votre colis 32834 est en atter retrait en point rela depuis le 09/06 retirer merci d'a 0684232347

BASE : Votre facture est debitee deux fois,vous trouverez ci dessous le formulaire de remboursement : https://goo.gl/U5u29Y

Message
Aujourd'hui 11:57

Nous avons essayé de livrer votre colis EU310120LPFR, mais il n'y a aucun affranchissement. Suivez les intructions ici: http://www.hy7.xyz/s/3pe4a1/bw4

LE HAMEÇONNAGE

COMMENT S'EN PROTÉGER ?

L'expéditeur

- **L'expéditeur est-il connu ?**
- **L'adresse correspond-elle à qui elle prétend être ?**

officiel@aucunrapport.com

nom boite mail sans intérêt

nom de domaine **à vérifier !**

Les adresses des services de l'Etat finissent par gouv.fr
Celles du Département finissent par lozere.fr

Le contexte

- **Urgence / menace ? => SPAM !**
- **Trop beau pour être vrai ? => SPAM !**

L'aspect visuel du mail n'a aucune importance (IA, traducteurs, correcteur..)

Premier piège : les liens

- **Le mail (ou le sms) tente de me rediriger via un lien ?**

Je vérifie l'URL en passant la souris dessus

http://www.chorus.hello.yalaaa.pro/fr/accueil

protocole non sécurisé **il faut un protocole httpS**

sous-domaine trompeur

nom de domaine à vérifier

emplacement de la page sur le site sans intérêt

Je ne sais plus vérifier l'URL ? Je me rend sur le site par une recherche sur navigateur sans cliquer sur le lien

Second piège : les pièces jointes

Je ne peux pas vérifier les pièces jointes. Je me méfie et m'assure de la légitimité du mail avant de les consulter

LE VISHING

Le vishing est l'abréviation de « voice phishing », ce qui implique d'escroquer les personnes par téléphone. Les objectifs finaux sont similaires au hameçonnage, mais elles utilisent différentes techniques.

Une fois que l'assaillant a attiré l'attention de la victime, il en tire parti pour l'inciter à céder des informations financières sensibles ou les données personnelles de la personne qui répond au téléphone.

Arnaques les plus courantes

Compte bancaire ou de carte de crédit compromis

Obtenir les informations du compte bancaire ou de la carte de crédit d'une victime

Offres de prêt ou d'investissement non sollicitées

Attirer les victimes en leur offrant la possibilité d'investir dans un projet ou d'obtenir un prêt

Escroquerie à Medicare ou à la sécurité sociale

Utiliser l'état de la victime comme levier pour convaincre la cible qu'elle doit céder ses données personnelles

LE VISHING

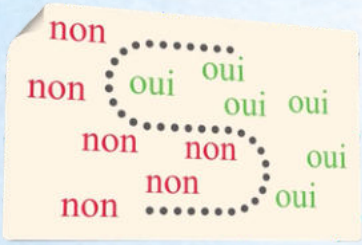
COMMENT S'EN PROTÉGER ?

Ne prenez pas l'appel

- **Si vous voyez un numéro suspect, laissez-le aller à la messagerie vocale. Vous pouvez vérifier son importance en vérifiant vos messages.**
- **En cas de doute, raccrochez sans vous justifier**

Détectez les manipulations

Lorsqu'une situation de crise survient, notre cerveau a d'autant plus tendance à recourir aux biais cognitifs, parce qu'il est sous pression. Ces biais sont exploités.

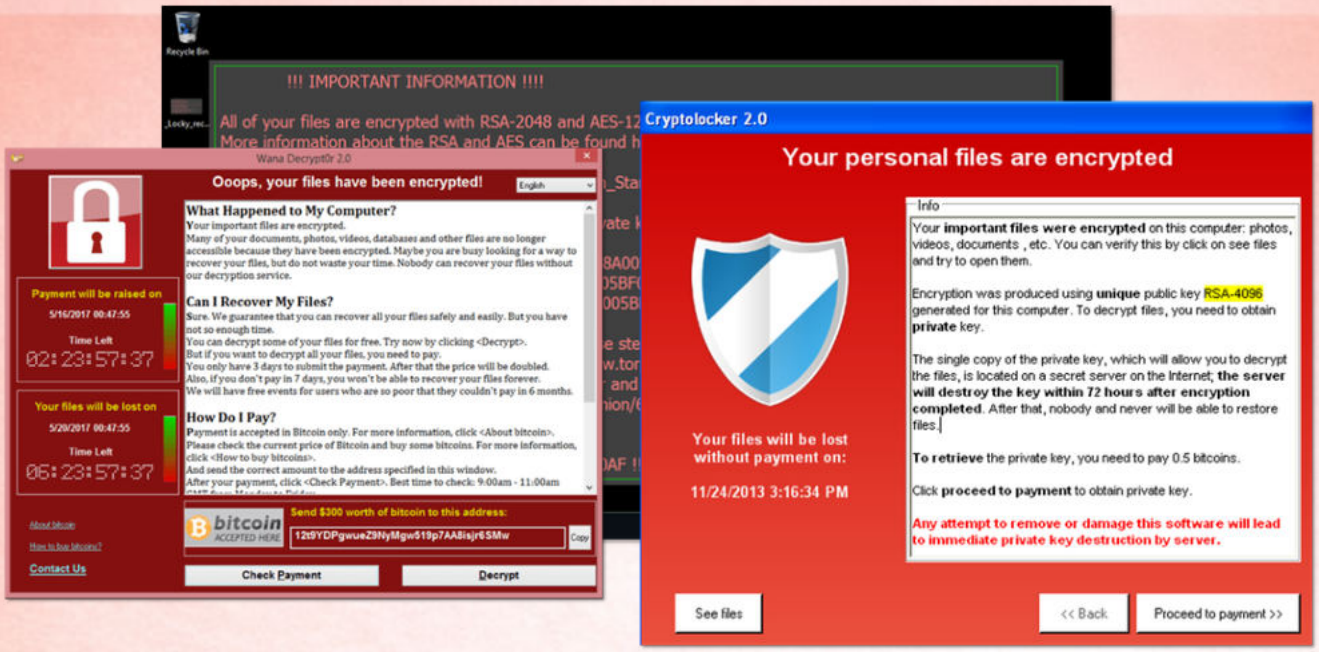


Biais d'engagement : un individu continue de prendre des décisions allant dans le sens d'une décision initiale même si cette décision initiale a conduit à un échec.

- **Méfiez vous de l'urgence et des menaces**
- **Apprenez à reconnaitre les actes préparatoires vous incitant à répondre à l'affirmatif, vous piégeant dans un processus engageant.**
- **Dire "oui" vous engage inconsciemment**

Astuce : exercez vous lors des démarchages au jeu du "ni oui, ni oui"

RANÇONGICIEL / PIRATAGE



Les rançongiciels (ou ransomware, cryptolocker) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon (généralement en cryptomonnaie) pour en obtenir de nouveau l'accès.

Le piratage correspond à l'accès, la modification, l'altération ou la suppression, non autorisés à des données informatiques.

Il pourra s'agir d'une défiguration de site internet mais également d'actions non visibles, bien plus malveillantes (stockage de fichiers illégaux, etc...).

RANÇONGICIEL / PIRATAGE

COMMENT S'EN PROTÉGER ?

Des systèmes à jour

- Avoir un système d'exploitation **ACTUEL** et **maintenu** par son éditeur
- **Mettre à jour** régulièrement les **logiciels** utilisés

Antivirus

- Protection contre l'ensemble des codes malveillants (virus, malware, etc...)
- Gratuit ou payant, mais doit être **à jour**

Gestion des droits

- Une session **« Administrateur »** permet d'installer de nouveaux programmes et de modifier certains réglages dans le système (comme désactiver l'antivirus). L'utilisation de cette session dans le cadre courant est à **PROSCRIRE**
- Dans la vie personnelle, il est possible de créer une session **utilisateur** aux droits restreints

Je ne paye pas la rançon

Pour une collectivité, payer la rançon est illégal. De plus, vous n'êtes pas certain de récupérer vos données ou qu'elles ne seront pas rendues publiques ou utilisées à des fins frauduleuses.

EN CAS DE CYBERATTAQUE

Comment je m'en rends compte

Le curseur se déplace tout seul sur l'écran, documents changeant de nom et d'extension, téléchargements, ralentissement très inhabituel, message de rançon...

Procédure au CD48

1/ **DÉBRANCHEZ** LA MACHINE D'**INTERNET** OU DU **RÉSEAU**

2/ **PAS D'EXTINCTION** DE L'APPAREIL COMPROMIS

3/ ALERTEZ AU PLUS VITE LE SUPPORT INFORMATIQUE

4/ PRÉVENEZ VOS COLLÈGUES DE L'ATTAQUE EN COURS

5/ N'UTILISEZ PLUS L'ÉQUIPEMENT POTENTIELLEMENT COMPROMIS

6/ PRÉVENIR LE DÉLÉGUÉ A LA PROTECTION DES DONNÉES

Dans la vie personelle

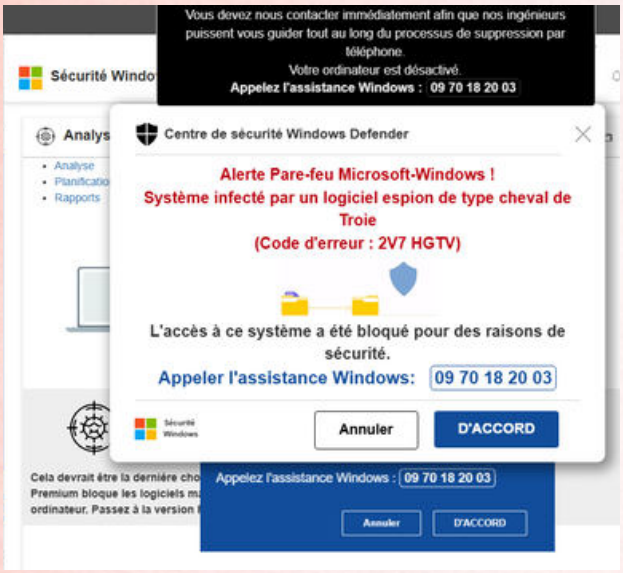
GENDARMERIE NATIONALE – GROUPEMENT DE LA LOZÈRE

17 CYBER
Mon assistance en ligne

Vous pouvez aussi contacter par téléphone la brigade de votre commune. Brigade de Mende : 04 66 49 54 72

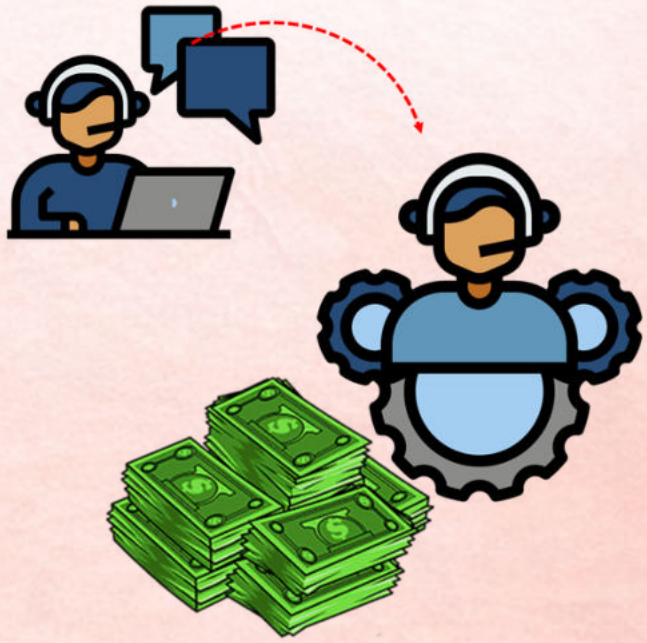
ESCROQUERIE AU FAUX SUPPORT TECHNIQUE

L'arnaque au faux support technique consiste à effrayer la victime généralement par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte ou de vol de ses données.



Ce type de message peut apparaitre sur votre navigateur lors de la visite de certains sites, même officiels.

La victime est invitée à appeler un numéro du "support Windows".
Le faux technicien Windows berne la victime, prend la main sur l'ordinateur, subtilise les mots de passe et installe des programmes malveillants.



Les interlocuteurs savent se montrer très convaincants, et peuvent se transférer votre appel entre eux pour rendre plus crédible l'arnaque.

ESCROQUERIE AU FAUX SUPPORT TECHNIQUE

COMMENT S'EN PROTÉGER ?

Le navigateur

- S'il est **à jour**, votre navigateur a plus de chance de bloquer l'affichage du piège
- Paramétrer le navigateur pour **bloquer les pop-up**

Anti-spam

- Équiper son navigateur ou son système d'une **solution anti-pub** est aujourd'hui **INDISPENSABLE**
- Il existe plusieurs solutions (gratuites ou payantes), de l'extension de navigateur aux produits de type VPN

Et si ça vous arrive ?

Agiter la menace et l'urgence est une technique bien connue de manipulation de la victime. Bien souvent, il ne s'agit que d'une fenêtre **pop-up en plein écran sur votre navigateur**.

- Appuyer sur **"echap"** permet de quitter le mode plein écran.
- Par précaution, respecter la **procédure "en cas de cyberattaque"**

USURPATION D'IDENTITÉ

L'usurpation d'identité est le fait de se faire passer pour quelqu'un dans le but d'obtenir quelque chose ou de faire valoir un droit.

De : paul.artuso481@hotmail.com
Salut Christian, c'est Paul, Je m'excuse de te déranger, je suis un peu embêté. Est-ce que tu peux m'aider

De : christian.morel@wanadoo.fr
Bonjour Paul, rien de grave ?

De : paul.artuso481@hotmail.com
Non, enfin, si, je n'en avais parlé à personne, mais j'ai eu quelques problèmes de santé ces derniers temps. Je suis monté à Paris pour voir un professeur et je me suis fait volé toutes mes affaires à la gare. Peux tu me rendre un service ?

De : christian.morel@wanadoo.fr
Bien sur. Geneviève est au courant ?

De : paul.artuso481@hotmail.com
Non, non elle n'est pas au courant, je ne veux pas l'inquiéter. Je suis à la poste de Paris. On me laisse me servir de l'ordinateur. Le plus simple c'est que tu ailles au bureau de tabac pour demander des coupons PCS. Ils t'expliqueront. Prêtes moi 250 €, je te les rend dès que je rentre,

L'usurpateur peut avoir pris le contrôle d'un compte au détriment de son propriétaire (messagerie, réseau social, site administratif, etc...).

Il peut aussi créer un compte de toutes pièces, suffisamment crédible pour usurper l'identité de sa cible.

USURPATION D'IDENTITÉ

COMMENT S'EN PROTÉGER ?

Un bon mot de passe

Vos mots de passe sont individuels et incessibles.

- Un mot de passe robuste = 12 caractères min, combinant MAJUSCULE, minuscule, ch1ffre et caractères $p€cîàu%
- On évite d'y mettre : nom, prénom, dates, nom de la structure, du service, SIRET, etc ...

Variez vos mots de passe

Afin de les retenir facilement, constituez vos mots de passe d'un bloc commun et d'une méthode de variation. Le bloc commun doit respecter les règles ci dessus.

exemple

Bloc commun : $Aligot010101

Variation : première et dernière lettre du site consulté à la fin

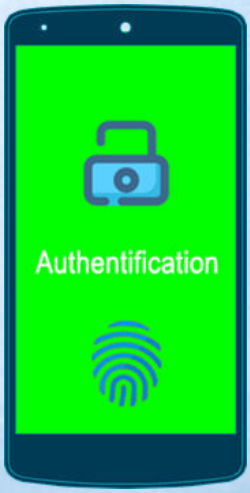
mots de passe constitués

Pour le site Orange : $Aligot010101Oe

Pour l'allumage du PC Windows : $Aligot010101Ws

Bonnes pratiques

- Pas de mot de passe dans le navigateur
- Cacher / mettre sous clé mon carnet papier des mots de passe
- Je ne stocke pas mes mots de passe dans un document numérique non sécurisé
- J'utilise un gestionnaire de mots de passe sécurisé si besoin
- J'utilise la double authentification



LES FAUX ORDRES DE VIREMENT

La fraude aux faux ordres de virement (FOVI) est un type d'escroquerie particulier qui, par usurpation d'identité, vise à conduire une victime à réaliser un virement de fonds vers un compte frauduleux.

Bonjour,

J'espère que vous allez bien.

Je vous écris pour vous informer que j'ai récemment changé de banque et souhaiterais mettre à jour les coordonnées bancaires actuellement enregistrées pour le versement de mon salaire. Je vous serais reconnaissant(e) si cette modification pouvait être prise en compte avant le prochain traitement de la paie.

Pourriez-vous me préciser la procédure à suivre pour transmettre mes nouvelles informations bancaires ? Je les communiquerai dans les plus brefs délais.

De nouvelles coordonnées bancaires vous sont adressées par e-mail avec des caractéristiques de messagerie très proches de celles du fournisseur et/ou de l'interlocuteur habituel (message , facture, expéditeur identique).

[Concretement]

DOMICILIATION

FPE CHARENTON
1 PLACE DES MARSEILLAIS
94220 CHARENTON LE PONT

TITULAIRE

DONS COMMUNE DE PONTARION

Un faux appel aux dons partant de la boite mail de la collectivité, redirigeant vers un RIB frauduleux.

Une demande de modification de RIB d'un salarié, adressée au service RH.

Code banque	Code guichet	N° de compte	Clé
16598	00001	32125690001	47

IBAN (International bank account number)	BIC
FR7616598000013212569000147	FPELFR21XXX

Financière des paiements électroniques, S.A.S. au capital de 725 640 euros, RCS Créteil B 753 886 092, TVA intracommunautaire FR80753886092. 1 place des Marseillais, 94220 Charenton-Le-Pont.

Une facture par mail précisant une modification de RIB de la part de l'entreprise

LES FAUX ORDRES DE VIREMENT

COMMENT S'EN PROTÉGER ?

La confidentialité

- Ne **communiquez pas d'information susceptible de faciliter le travail des escrocs** (noms des différents managers, chefs de division, moyens de règlement, listing fournisseurs...)
- Généralisez l'utilisation de **mots de passe solides** pour les comptes de messagerie et activez la **double authentification** pour limiter les risques de piratage

La vérification

- Prenez le temps de **vérifier**, surtout dans l'urgence et sous la pression, les demandes de virement
- **Contactez le numéro habituel connu** en interne et non celui fourni par l'escroc pour contre-vérifier

Bon à savoir

Il existe une multitude de scénarios pour cette fraude : appels du président de la société ou de son avocat, d'un faux titulaire de marché, mise sous pression d'un faux cadre hiérarchique. Les interlocuteurs peuvent être multiples et le numéro de théâtre **très convaincant**.

Cependant, **la demande de modification de RIB doit TOUJOURS être vérifiée en réalisant un contre appel.**
Dans la vie personnelle, cette escroquerie existe également. Soyez très vigilant dès que vous enregistrez un RIB (notaire par exemple).

BONNE PRATIQUE
INTELLIGENCE ARTIFICIELLE

L' Intelligence Artificielle (ou IA) est de plus en plus présente dans notre quotidien, notamment au travers de nouveaux produits ou services dont l'utilisation n'est pas encore encadrée. Elle repose cependant sur des algorithmes gourmands en données, souvent personnelles, et son usage nécessite le respect de certaines précautions.

Données personnelles

- **Ne renseignez aucune donnée personnelle dans vos prompts**
- **Ne renseignez aucune pièce jointe sans y avoir supprimé au préalable toute donnée personnelle (résumé de réunions, synthèse documentaire, etc.)**
- **Ne partagez aucune donnée confidentielle sur la structure**
- **N'enregistrez pas la voix des personnes sans avoir récolté au préalable leur consentement (réunions)**

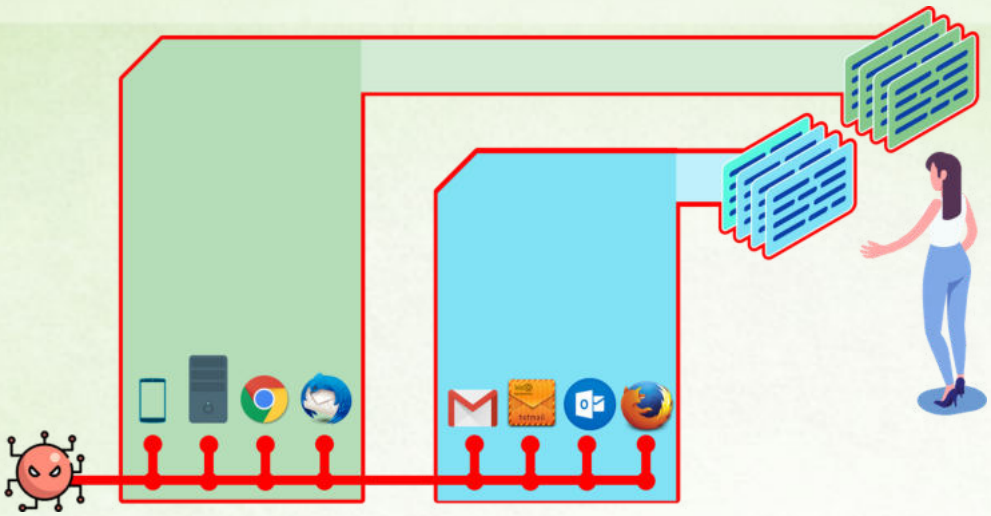
Gardez un œil critique

L'utilisation de ces outils ne doit pas remplacer la prise de décision humaine ni négliger l'expertise humaine et le raisonnement associé.

Soyez conscients que les réponses générées par des outils IA peuvent être sujettes à des erreurs et doivent être évaluées avec soin.

BONNE PRATIQUE

SÉPARER LES USAGES PRO / PERSO



Vie pro

Gestion des incidents facilitée
Évite l'engagement de la responsabilité individuelle
Outils choisis et protégés par la politique de sécurité
Détection des arnaques facilitée

Vie perso

Centres d'intérêts différents
Niveau de vigilance différent
Discours privé différent du discours public
Pas de politique de sécurité informatique

Il est très efficace de séparer les usages professionnels de ceux personnels

Mauvaises pratiques

- Utiliser son mail professionnel pour créer des comptes personnels
- Transférer des documents professionnels vers une adresse e-mail personnelle pour travailler chez soi
- Stocker des fichiers professionnels sur un cloud personnel non autorisé
- Utiliser un ordinateur professionnel pour télécharger des contenus personnels
- Se connecter à des services professionnels depuis un équipement personnel non sécurisé
- Utiliser une clé USB perso au travail

BONNE PRATIQUE
TÉLÉPHONE

Les arnaques téléphoniques sont réalisées le plus souvent pour inciter les victime à rappeler vers un numéro surtaxé. Tout comme le SPAM par mail, elles peuvent avoir aussi pour objectif de collecter des données personnelles et aboutissent sur des escroqueries.

BLOCTEL : Ce service gratuit de l'Etat permet d'éviter les prospections commerciales
https://www.bloctel.gouv.fr/

DÉSABONNEMENT :
Désabonnez-vous ou supprimez les comptes que vous n'utilisez plus

NE RAPPELEZ PAS !
Les appels en absence laissés sans message, sont souvent des arnaques !

FILTRAGE :
Certains opérateurs téléphoniques proposent des systèmes de filtrage

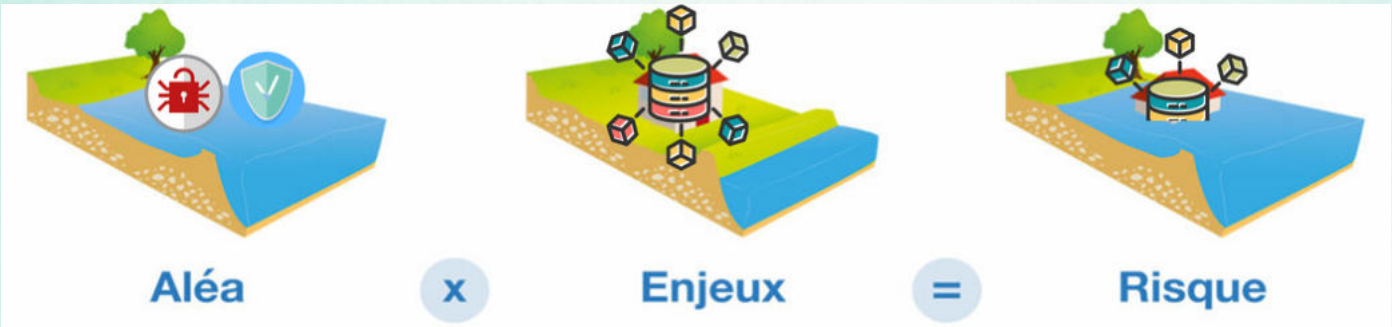
Sécuriser ses téléphones professionnels et personnels

Professionnel ou personnel, le téléphone doit être sécurisé afin d'éviter un accès non autorisé à vos contacts, vos services (notamment messagerie) et autres données stockées sur votre appareil.

- **Code, schéma ou empreinte, il est INDISPENSABLE d'utiliser un moyen de verrouillage du téléphone**
- **Code PIN de la carte SIM : proscrire l'utilisation des codes comme 0000, 1234, 4321**

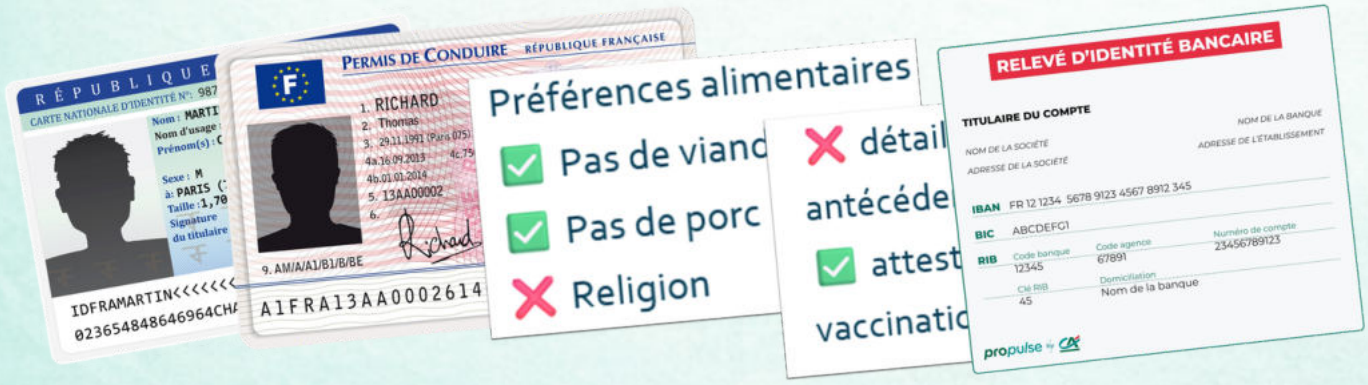
RÈGLES SUR LES DONNÉES PERSONNELLES
PRINCIPE DE MINIMISATION

En réduisant au minimum les données collectées, on réduit le risque pour les personnes en cas de fuite de données.



[art.5.1.c du RGPD]

Les données personnelles collectées doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire au regard de la finalité du traitement.



Vous devez être capable de justifier la collecte et la conservation de chaque donnée que vous demandez (texte de loi, intérêt légitime, consentement ...)

Par exemple :

- **Ne collecter que les justificatifs nécessaires à l'instruction du droit**
- **Éviter le stockage centralisé de pièces scannées non nécessaires**
- **Ne pas demander d'information inutile**
- **Éviter les jugements et les annotations**

RÈGLES SUR LES DONNÉES PERSONNELLES
PRINCIPE DE TRANSPARENCE

[art.5.1.a du RGPD]

Les données personnelles doivent être traitées de manière légale, loyale et transparente vis-à-vis des personnes concernées.

En pratique, cela signifie que les organisations doivent fournir des informations claires, compréhensibles et facilement accessibles sur la manière dont leurs données sont collectées, utilisées, conservées et partagées.

Qui informer et quand le faire ?

- en cas de **collecte directe des données** (exemples : formulaire, souscription d'un contrat, ...) **=> au moment du recueil des données, sur le document concerné**
- en cas de **collecte indirecte des données personnelles**, lorsque les données ne sont pas recueillies directement auprès des personnes (exemples : données récupérées auprès de partenaires...). **=> dès que possible (lors du premier contact par exemple)**

Quelles informations donner ?

- Le **modèle** de mention d'information est disponible sur l'intranet : **Accueil > Services généraux > Règlement Général sur la Protection des Données**
- Contacter le délégué à la protection des données si besoin d'aide : **protectiondonnees@lozere.fr**

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le délégué à la protection des données (DPD, parfois nommé DPO - Data Protection Officer) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données.

En cas de demande d'exercice de droits

Les personnes disposent de droits sur leurs données personnelles : **vous devez leur permettre de les exercer si vous recevez une demande**. Contactez le DPD ou un référent.

En cas de violation de données

Vous avez envoyé un courriel sensible au mauvais destinataire, vous êtes victime d'un piratage, vous avez perdu un ordinateur du CD48 ? Ces situations doivent être **évaluées rapidement par le DPD** afin de déterminer la nécessité d'une notification à l'autorité de contrôle et, le cas échéant, aux personnes concernées. Prévenez le DPD ou un référent.

Autres cas

- Pour toute question relative aux données personnelles
- En cas de mise en place d'un nouveau traitement de données personnelles, afin d'en vérifier sa conformité
- Recours à un prestataire externe / sous-traitant des données de la collectivité

CONTACT

Collectivités accompagnées par le CDG48 : dpd@cdg48.fr