VICTIME DE CYBERMALVEILLANCE

En cas de piratage ou d'infection par un virus

- ✔ Déconnectez l'appareil d'internet ou du réseau informatique
- ✔ Réalisez une analyse complète au moyen de votre antivirus
- ✔ Restaurez ou réinstallez le système à partir d'une sauvegarde antérieure à l'attaque
- ✔ Au besoin, faites vous assister par un professionnel qualifié

En cas de fraude bancaire (*opérations frauduleuses*)

Faites **immédiatement** opposition sur votre carte bancaire et contactez votre banque

Dans tous les cas

- ✘ Ne paniquez pas / n'agissez pas dans la précipitation
- ✘ Ne cliquez pas sur un lien internet ou mms douteux
- ✘ Ne fournissez jamais vos coordonnées bancaires ou de CB
- ✘ Ne payez pas de rançon / n'envoyez pas d'argent n'achetez pas de coupons de prépaiement (PCS…)
- ✔ Conservez les éventuelles preuves (captures d'écran, e-mails ou messages)
- ✔ Au moindre doute, changez vos mots de passe
- ✔ Prenez contact avec la gendarmerie pour déposer plainte

LIENS UTILES

Infos, assistance et bonnes pratiques ➲ **cybermalveillance.gouv.fr**

Portails officiels Perceval, Pharos, THÉSÉE
➲ **service-public.fr** → **« arnaque sur internet »**

Site de l'ANSSI ➲ **cyber.gouv.fr**

Contre les SPAMS ➲ **signal-spam.fr** / **33700**

Application Gendarmerie / Police « Ma Sécurité »
➲ **masecurite.interieur.gouv.fr**

Réalisé et édité par la CPTM du GGD88 – **NE PAS JETER SUR LA VOIE PUBLIQUE**

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

GENDARMERIE DES
VOSGES

CYBERMALVEILLANCE
ASSURER SA SÉCURITÉ NUMÉRIQUE

FICHE D'INFORMATIONS

Victime de cyberdélinquance, n'hésitez pas à contacter votre brigade locale

ASSUREZ VOTRE CYBERSÉCURITÉ

Dix mesures essentielles pour assurer votre sécurité numérique

1. Protégez vos accès avec des **mots de passe solides**
   - ☛ longs, complexes et différents selon vos usages
   - ☛ changer les au moindre doute ou régulièrement en prévention
2. **Sauvegardez** vos données régulièrement
3. Appliquez rapidement les **mises à jour** sur tous vos appareils
   - ✔ les mises à jour corrigent les failles de sécurité
4. Utilisez un **antivirus** (gratuit ou payant) et le tenir à jour
   - → effectuez des analyses approfondies de façon régulière
5. Ne téléchargez vos applications que sur les **sites officiels**
6. Méfiez-vous des **messages inattendus ou alarmistes**
   - ✘ risque d'arnaque par hameçonnage
   - ✔ vérifiez l'adresse mail de l'expéditeur
   - ✘ ne cliquez sur aucun lien, ne suivez jamais les instructions
   - ✔ demandez toujours confirmation à l'émetteur par un autre moyen
7. **Vérifiez** les sites sur lesquels vous faites vos achats
   - ✔ contrôlez que le site n'est pas une copie frauduleuse
   - → consultez les sites de protection des consommateurs/les avis
8. **Maîtrisez vos réseaux sociaux**
   - ☛ sécurisez en l'accès avec un mot de passe solide et unique
   - ✔ définissez les autorisations (*uniquement vos amis*)
   - ✘ ne relayez pas d'informations non vérifiées (*fake news*)
9. Séparez vos usages **personnels et professionnels**
10. Évitez les réseaux WiFi publics ou inconnus (***non sécurisés***)
    - ☛ privilégiez la connexion de votre abonnement 3G/4G/5G

IDENTIFIEZ LES MENACES

VIRUS INFORMATIQUE
Programme malveillant qui perturbe le fonctionnement d'un appareil informatique voire dérobe les informations personnelles qu'il contient.

PIRATAGE INFORMATIQUE (*ou HACKING*)
Intrusion illicite dans un système informatique par un cybercriminel en vue de nuire à la victime (*vol de données, piratage de compte* ...)

HAMEÇONNAGE (*ou PHISHING*)
Mail ou sms frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance (*administrations, banques ...*)

ARNAQUE AU FAUX SUPPORT TECHNIQUE
Consiste à effrayer la victime (message bloquant l'ordinateur) en indiquant un problème technique grave afin de la pousser à payer un pseudo-dépannage informatique.

RANÇONGICIEL (*ou RANSOMWARE*)
Logiciel malveillant qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en retrouver l'accès.

CHANTAGE À LA WEBCAM OU À L'ORDINATEUR PIRATÉ
Escroquerie qui vise à faire croire à la victime que ses équipements ont été piratés dans le but de la faire chanter.

FRAUDE AU FAUX CONSEILLER BANCAIRE
Tromperie qui consiste à faire valider à la victime des opérations frauduleuses sur ses comptes en se faisant passer pour son conseiller.

ARNAQUE À LA CARTE BANCAIRE
Utilisation des coordonnées de la carte bancaire de la victime pour réaliser des achats frauduleux (*après vol ou piratage des numéros*).

SPAM TÉLÉPHONIQUE OU ÉLECTRONIQUE
Appel, sms ou e-mail transmis à des fins publicitaires, commerciales ou malveillantes.