CYBERSÉCURITÉ

MEMENTO COLLECTIVITÉS

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

Prévention - assistance

- informations utiles / guides pratiques
- **Sency-Crise** / **ImpactCyber**

cybermalveillance.gouv.fr

ANSSI | Agence nationale de la sécurité des systèmes d'information

Sites de l'ANSSI

- informations utiles / guides pratiques
  cyber.gouv.fr
- diagnostic gratuit par un aidant cyber
  monaide.cyber.gouv.fr

Grand Est Cybersécurité
CENTRE D'ASSISTANCE DE PROXIMITÉ

CSIRT de la Région Grand-Est
pour les collectivités et PME / ETI

- prévention
- scan de vulnérabilité
- assistance / aide aux victimes
  en cas d'attaque cyber

cybersecurite.grandest.fr

0970 512 525 (***non surtaxé***)

CYBERGEND

Contact

Gendarmerie des Vosges
Référent cybersécurité

Adjudant-chef Jérémie Roy

jeremie.roy@gendarmerie.interieur.gouv.fr

06.18.72.62.29

Liens utiles

17 CYBER
Mon assistance en ligne

MonAideCyber
INNOVATION ANSSI

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

GROUPEMENT VOSGES GENDARMERIE DÉPARTEMENTALE

CYBERMALVEILLANCE

ASSURER LA CYBERSÉCURITÉ DES COLLECTIVITÉS

FICHE D'INFORMATIONS

#PRÉSENTS POUR LES ÉLUS

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

CYBERSÉCURITÉ

QUELLES CYBERMENACES ?

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 ...*)

ATTAQUE EN DÉNI DE SERVICE (*ou DDoS*)

Action malveillante → envoi de multiples requêtes visant à saturer un serveur afin de provoquer une panne ou un fonctionnement dégradé du service.

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.

DÉFIGURATION DE SITE INTERNET (*ou DÉFACEMENT*)

Modification par un pirate de l'apparence d'un site web.

VOL ET DIFFUSION DE DONNÉES

Un pirate profite d'une faille de sécurité pour s'introduire dans un système et récupérer toutes les informations possibles.
Les données volées peuvent ensuite être revendues sur le darkweb.

ARNAQUE AU FAUX RIB

Consiste à tromper la victime, en usurpant l'identité d'un créancier avec lequel elle est en relation (entreprise, artisan, notaire …), afin de lui faire réaliser un virement vers un compte bancaire détenu par un escroc.

En 2024

1 690 infractions numériques ont visé des administrations (**+ 42%**).

312 dépôts de plaintes ont concerné les seules collectivités.

1 collectivité sur 10 déclare avoir déjà été victime de cyberattaque (s).

CYBERSÉCURITÉ

BONNES PRATIQUES

- ✔ Protéger le système informatique, le réseau, les postes de travail
  - ☛ antivirus, pare-feu bien configuré
  - ☛ accès sécurisé aux données, chiffrement
  - ☛ usage limité et responsable des clés usb
  - ☛ sécuriser la **messagerie électronique**
  - ☛ ne pas oublier les **appareils mobiles** smartphones, tablettes …
- ✔ **Former / sensibiliser** les agents aux risques cyber
  - ☛ séparer les usages **pro** / **perso**
- ✔ S'appuyer sur des professionnels de confiance ou référencés
- ✔ Politique de **mot de passe** rigoureuse / authentification multifacteur
- ✔ Réaliser et gérer les **sauvegardes** (*les tester*)
- ✔ Effectuer les **mises à jour** régulièrement (*sites officiels*)
- ✔ Sécuriser ses **accès extérieurs** → déplacements / télétravail
- ✔ Préparer des scénarios de **gestion de crise** et de reprise d'activité

EN CAS D'ATTAQUE

- → Isolez les systèmes attaqués
  - ☛ couper toutes les connexions internet
- → Alertez immédiatement votre support informatique
  - ☛ identifier l'origine de l'attaque et son étendue
- → Préservez les preuves de l'attaque et **DÉPOSEZ PLAINTE**
- → Notifiez l'incident à la CNIL (**72 H**) / Gérez votre communication