



Boîte à outils

Visio du 6 juillet 2023

Objectif : sensibilisation à la sécurité numérique pour protéger à la fois les services municipaux et le mandat d'élu. *"La question n'est plus aujourd'hui de savoir si vous allez faire l'objet d'une attaque mais quand elle vous concernera."*

Présentée par le Colonel De La Cruz et l'Adjudant Duponchel du Groupement de gendarmerie de la Marne

Visionner l'enregistrement



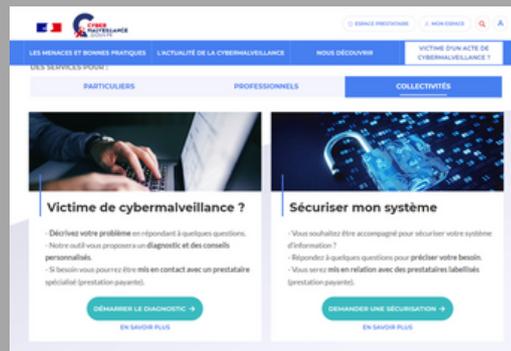
www.cybermalveillance.gouv.fr

LE site internet de référence

Affiches, guides, signalement, plainte...

www.cybermalveillance.gouv.fr

Retrouvez **la fiche des 10 mesures essentielles** pour votre sécurité numérique



Sites utiles : signalements, protection et plainte

Contenu illicite sur internet - PHAROS : <https://www.internet-signalement.gouv.fr>

Spam : <https://www.signal-spam.fr>

Phishing : <https://www.phishing-initiative.fr>

Protection des données personnelles CNIL : <https://www.cnil.fr>

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

Gendarmerie Nationale, brigade numérique (chat 24h/24 7j/7) : <https://www.gendarmerie.interieur.gouv.fr>

Aide financière Région Grand Est

Jusqu'à 5 000€ pour votre diagnostic cyber

www.grandest.fr

Franck OLIVIER

DiagCyber@grandest.fr

03 88 15 67 47

Contact Gendarmerie Nationale

Adresse email et téléphone pour toute question liée à la cybersécurité des collectivités et demande de diagnostic "Diagonal"

Référent cybersécurité Marne

cybergend51@gendarmerie.interieur.gouv.fr

Bureau SOLC : 03 26 68 64 39

Bureau CYBER : 03 26 68 63 15

Grand Est Cybersécurité

Centre régional d'assistance aux victimes d'attaques informatiques.

Ce centre délivre un service gratuit d'assistance aux PME, ETI (Entreprises de taille intermédiaire), collectivités et associations du territoire

C-SIRT Grand Est

www.cybersecurite.grandest.fr

0 970 512 525

Lundi au vendredi 9h-12h30 / 14h-17h30

Déclarez un incident en ligne

Scan gratuit des vulnérabilités de votre infrastructure visible sur Internet

Comment réagir à une cyberattaque ?



1. Débranchez la machine d'Internet ou du réseau informatique

Débranchez le câble réseau et désactivez la connexion Wi-Fi ou les connexions de données pour les appareils mobiles.



2. N'éteignez pas l'appareil

Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint.



3. Alertez au plus vite votre support informatique

Votre support pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque.



4. N'utilisez plus l'équipement potentiellement compromis

Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.



5. Prévenez vos collègues de l'attaque en cours

Une mauvaise manipulation de la part d'un autre collaborateur pourrait aggraver la situation.



DEPOSEZ PLAINTÉ !

Plainte en ligne pour les particuliers

Victime ou témoin d'escroqueries sur internet, la plateforme de signalement et de dépôt de plainte THESEE est disponible. Le dispositif traitement harmonisé des enquêtes et signalements pour les e-escroqueries permet de porter plainte ou de signaler l'infraction en ligne.



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

Certaines infractions relèvent de la...

service-public.fr

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



association@maires51.fr

03 26 69 59 59 www.maires51.fr

Juillet 2023