Pour la population, par le gendarme

Gendarmerie nationale

De supposés audits de Cybersécurité en ligne… ...Vigilance !

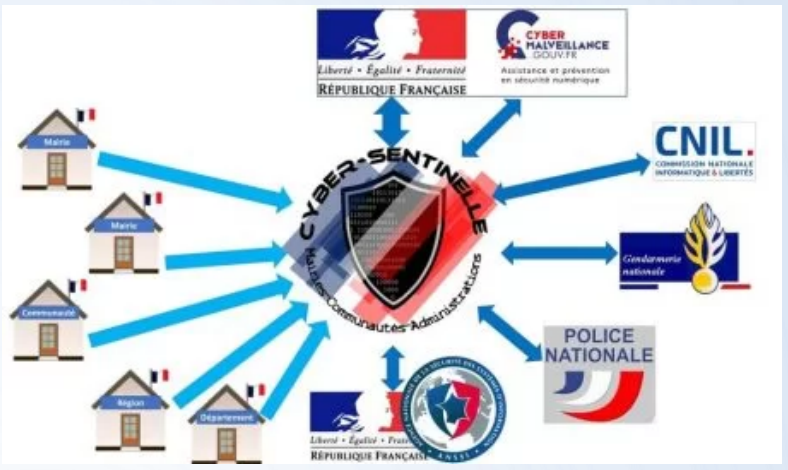
CYBER-SENTINELLE

Pour les collectivités, contre les virus et cyber-attaques

La société « Cyber-Sentinelle » existe bien et propose sur son site internet des services en matière de cybersécurité. Mais les démarches commerciales de cette structure sont litigieuses.
En effet, prétextant un audit de Cybersécurité réalisé à distance, les mairies reçoivent des factures sans avoir souscrit le moindre contrat, au préalable.

Deux communes de l'Aube viennent d'être abusées, la Gendarmerie de la Meuse appelle donc les élus du département à la plus grande vigilance.

D'autant plus, qu'il n'existe aucun partenariat entre les forces de l'ordre ou les autres institutions et cette société, bien qu'elle le laisse supposer sur son site internet avec la présence des logos de l'ANSSI, cybermalveillance.gouv, de la Gendarmerie Nationale, de la Police et de la CNIL.



Nos conseils en matière de cybersécurité:

Effectivement, c'est un constat, les cyberdélinquants ciblent de plus en plus les mairies, les collectivités territoriales, les administrations ou les hôpitaux, notamment par rançongiciel. Mais une bonne hygiène informatique suffit dans la majorité des cas à vous protéger.

En premier lieu, dialoguez avec votre prestataire informatique pour connaître votre niveau de protection et définir avec lui vos besoins.

LES MOTS DE PASSE

Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.

LES SAUVEGARDES

Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

LES MISES À JOUR

Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.

Pour tester gratuitement et en toute sécurité :

Votre Mot de Passe : https://www.security.org/how-secure-is-my-password/

Ou la sécurité de votre réseau : https://www.monservicesecurise.ssi.gouv.fr/

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

AMF

#PRÉSENTS POUR LES ÉLUS

La région Grand-Est a également mis en place un Centre Régional d'Assistance aux Victimes d'Attaques Informatiques, qui délivre un service gratuit d'assistance aux PME, ETI (Entreprises de taille intermédiaire), collectivités et associations du territoire : https://cybersecurite.grandest.fr/

0 970 512 525

Pour toute urgence composez le 17
(ne pas répondre à ce présent message de prévention)