La Cyber-Lettre de la GENDARMERIE RÉGION GRAND EST

Décembre 2025

LA FIN D'ANNEE, LES FETES, LES CADEAUX … ET LES CYBERATTAQUES

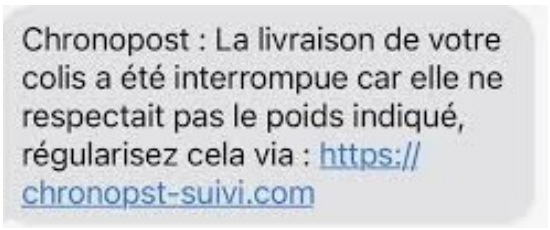
DIFFUSION LIBRE

Vous êtes de plus en plus nombreux à faire vos achats sur Internet. Rien de plus pratique que de trouver le bon cadeau sans quitter son canapé. Mais pendant que vous cliquez, les escrocs, eux, ne chôment pas non plus.

💡 Le faux code promo : un mail vous annonce une réduction exclusive limitée sur votre plateforme préférée ? Il vous suffit d'un clic pour valider votre code promotionnel et accéder à votre boutique favorite. En apparence, tout semble normal sauf qu'il s'agit d'un phishing habilement déguisé.

🌐 Le typosquatting : l'escroc modifie un simple caractère dans l'adresse du site. Par exemple : https://nomdedomaine.fr va devenir https://nomdebomaine.fr. À l'œil nu, difficile de s'en apercevoir. Vous croyez acheter le cadeau parfait… mais vous offrez surtout vos coordonnées bancaires à un inconnu.

📦 La livraison : un message du pseudo livreur vous indique qu'il manque une information ou qu'un supplément est à régler. Là encore, un lien frauduleux vous conduit vers un faux site ou un faux paiement.



💡 Bon à savoir :

Un seul caractère modifié ou ajouté dans le nom d'un site internet suffit à vous renvoyer vers une copie quasi parfaite d'un site légitime détenu par un pirate. C'est ce qu'on appelle le typosquatting.

Un livreur n'a jamais besoin de vos informations bancaires. Il dispose déjà de vos coordonnées pour vous remettre le colis. En cas de reprogrammation, il ne vous demandera qu'une date, une heure et un lieu. **Jamais** il ne sollicitera la communication de vos données personnelles ou de paiement.

⚠ Ne tombez pas dans le piège !

- ✅ Vérifiez toujours l'orthographe de l'adressage d'un site Internet.
- ✅ Méfiez-vous des messages vous demandant vos informations de paiement ou vos données personnelles.
- ✅ En cas de doute, surtout lorsque des données sensibles sont en jeu, faites votre propre recherche sur Internet pour confirmer que vous accédez bien au site officiel.

Vous êtes victime ?

Appelez immédiatement le 📞 **17** ou 💻 contacter :

LE 17 CYBER

Une cyberattaque, échangez avec un cybergendarme - 24h/24 7j/7
https://17cyber.gouv.fr/

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.

CYBERMALVEILLANCE

Pour vous faire assister, vous informer ou vous former
www.cybermalveillance.gouv.fr

THÉSÉE

Déposer plainte en ligne pour les victimes d'e-escroqueries

L'ANSSI

Renforcer le niveau de cybersécurité
https://cyber.gouv.fr

PERCEV@L

Signaler une utilisation frauduleuse de votre carte bancaire sur internet

PHAROS

Signaler un contenu illicite sur internet
www.internet-signalement.gouv.fr

+ D' INFO

🎅 En cette fin d'année, gardez l'esprit festif... mais restez vigilants !

Vous souhaitez joindre un Référent Cyber de la Région de Gendarmerie du Grand-Est ou vous abonner à la Cyber-lettre
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)

01010010 01001001 01010011 01000011 01001000