MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

10 février 2025

ALERTECYBERGEND80

La semaine dernière, une **commune de la Somme** nous signalait une cyberattaque : son **compte de messagerie** avait été **piraté**. Ayant accès aux mails de la mairie, le hacker a pu se faire passer pour une entreprise locale (avec laquelle la commune avait des relations d'affaires) et relancer une **facture** d'environ **80 000 €** dont le **RIB** avait été préalablement **falsifié**.
Ainsi dupée, la commune a procédé au paiement.
La **réaction** rapide de la commune a permis de récupérer les **fonds** et de limiter les **dégâts**.

LA COMPROMISSION DE COMPTES MAIL AU CŒUR DE NOMBREUSES CYBERATTAQUES …

La compromission de messagerie électronique est un **vecteur d'attaque** très efficace car elle permet aux pirates d'**usurper** l'identité d'une **personne de confiance**, comme un **collègue**, un **supérieur hiérarchique** ou un **partenaire commercial**. Les victimes sont plus susceptibles de croire un courriel provenant d'une personne qu'elles connaissent et en qui elles ont **confiance**, ce qui les rend plus **vulnérables** aux attaques.

… AVEC DE GRAVES CONSÉQUENCES, TANT SUR LE PLAN PERSONNEL QUE PROFESSIONNEL !

Voici quelques-uns des risques potentiels :

- **Accès à des informations sensibles** : Les boîtes de réception contiennent souvent des informations personnelles, financières, professionnelles, précieuses pour les pirates.
- **Usurpation d'identité** : Un compte piraté permet d'envoyer des e-mails frauduleux au nom de la victime, propageant des logiciels malveillants, des arnaques, etc.
- **Accès à d'autres comptes** : Les e-mails servent souvent à la récupération de mots de passe d'autres services (réseaux sociaux, comptes bancaires, …).

QUELQUES CONSEILS POUR SE PROTÉGER

En prenant les précautions suivantes, vous réduirez considérablement les risques de compromission de votre compte de messagerie et vous protégerez vos données personnelles et financières :

- **Mots de passe forts** : Utilisez des mots de passe uniques et complexes pour votre compte de messagerie et changez-les régulièrement.
- **Authentification multi-facteurs (MFA)** : Activez l'authentification multi-facteurs pour ajouter une couche de sécurité supplémentaire à votre compte.
- **Vigilance** : Soyez vigilant face aux emails suspects et ne cliquez JAMAIS sur des liens ou des pièces jointes provenant d'expéditeurs inconnus ou douteux.
- **Sécurité de l'appareil** : Protégez votre ordinateur et vos appareils mobiles avec un antivirus et un pare-feu.
- **Mises à jour** : Assurez-vous que votre système d'exploitation, votre navigateur et votre logiciel antivirus sont toujours à jour.