MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

1er mai 2024

ALERTECYBERGEND

Piratage de compte de messagerie électronique au préjudice d'une pharmacie de la Somme, suivi d'une tentative d'escroquerie.

POINT DE SITUATION

Ce lundi 29 avril 2024, la **boite mail professionnelle d'une pharmacie** samarienne est **piratée**. Usurpant l'**identité du pharmacien**, l'auteur des faits adresse un mail à l'un des fournisseurs de l'officine et passe **frauduleusement** une commande importante de produits, en prenant soin de modifier l'adresse de livraison.

Souhaitant s'assurer de la **légitimité** de cette commande, le prestataire contacte la victime pour lui demander de confirmer la transaction. Réalisant être **victime du piratage** de son **compte de messagerie** et d'une **tentative d'escroquerie**, le pharmacien obtient l'annulation de la commande **passée à son insu**.

Sans la **vigilance** du fournisseur, le **préjudice** aurait été de plus de 9 000 euros dès cette première commande.

En pratique, l'**attaquant** a pu obtenir l'accès à la boîte mail de plusieurs manières : un mot de passe peut-être **trop facile à deviner**, l'utilisation du même mot de passe **sur plusieurs sites** dont l'un a été piraté ou encore suite à un **message d'hameçonnage** voire dans certains cas, en raison de la présence d'un **virus voleur de mot de passe** sur un des équipements de la victime.

MESSAGERIE PIRATÉE, QUE FAIRE ?

- ✔ **Vérifier l'absence de règle de filtrage ou de redirection de vos messages** qui auraient pu être mises en place par le cybercriminel pour intercepter ou se faire renvoyer automatiquement vos messages ;
- ✔ **Activer la double authentification** si elle est disponible : cette fonctionnalité vous demandera un code de confirmation, transmis par exemple par SMS, chaque fois qu'un nouvel appareil tentera de se connecter à votre compte ;
- ✔ **Changer le mot de passe** : si vous pensez être victime du piratage de votre boîte mail, réinitialisez au plus vite le mot de passe de votre messagerie et de tous les sites où vous l'utilisiez, en vous assurant d'utiliser un nouveau mot de passe solide que vous n'utilisez sur aucun autre site ;
- ✔ **Déconnectez de votre compte tout appareil ou session active inconnus** : vérifiez l'historique des connexions dans les paramètres de votre compte. Si vous identifiez des appareils ou sessions actives qui ne vous appartiennent pas, sauvegardez les preuves (capture d'écran, photo) puis déconnectez ou supprimez ces connexions suspectes. Sans cela, il pourrait être possible au cybercriminel de rester connecté à votre compte même après que vous ayez changé votre mot de passe ;
- ✔ **Prévenir les contacts** de votre compte de messagerie afin qu'ils ne deviennent pas victimes des cybercriminels à leur tour ;
- ✔ **Alerter votre banque** et surveiller vos comptes bancaires à la recherche de toute transaction suspecte dont vous ne seriez pas à l'origine ;
- ✔ **Déposer plainte** : en fonction du cas d'espèce et du préjudice subi, plusieurs infractions peuvent être retenues contre les attaquants, allant du piratage informatique à l'atteinte au secret des correspondances, en passant par l'usurpation d'identité et l'escroquerie ;
- ✔ **Si vous ne pouvez plus vous connecter à votre compte de messagerie** et pensez votre boîte mail piratée, contactez le service de messagerie concerné pour signaler votre piratage et demander la réinitialisation de votre mot de passe.