

COMMUNIQUÉ DE PRESSE

Cyberarnaques en hausse dans le Canton de Neuchâtel

Appelée communément l'arnaque au Président, le Canton de Neuchâtel connaît ces dernières semaines une série d'arnaque aux faux ordres de virement internationaux visant les entreprises. Les montants escroqués de cette manière peuvent s'avérer considérables. La police neuchâteloise appelle les entreprises et les particuliers à rester vigilants en matière de cybercriminalité.

Ces dernières semaines, plusieurs entreprises neuchâteloises ont été victimes d'arnaques aux faux ordres de virement ou plus communément appelées l'arnaque au Président. Les montants escroqués aux entreprises par ce biais peuvent être considérables. Depuis le mois d'avril 2021, la police neuchâteloise recense plusieurs tentatives et une escroquerie qualifiée où l'entreprise a versé près de 50'000 francs sur un compte à l'étranger.

L'arnaque au Président consiste, pour l'auteur, à se faire passer pour le patron ou le supérieur hiérarchique d'une entreprise. Par courriel, il contacte un collaborateur du service comptabilité de l'entreprise. Grâce à un subterfuge d'affichage, l'adresse e-mail de l'expéditeur correspond bien à celle du directeur de l'entreprise ou y ressemble. Le soi-disant patron demande alors d'effectuer rapidement un virement d'argent sur un compte étranger.

Afin de prévenir les arnaques au Président, il est conseillé aux employés des entreprises de vérifier scrupuleusement l'adresse de l'expéditeur. Dans le doute, un contact direct avec ses interlocuteurs habituels est à privilégier.

Un logiciel malveillant en circulation dans le canton

La police neuchâteloise rend attentive la population qu'un logiciel malveillant a également été détecté dans le Canton de Neuchâtel. Ce logiciel appelé « FluBot » piège le téléphone de la victime au moyen d'un SMS contenant un lien vers un prétendu message vocal. Ce SMS usurpe souvent l'identité d'une marque de livraison populaire. Une fois le lien activé, le logiciel malveillant « FluBot » est téléchargé et pirate les données confidentielles et sensibles contenues dans le smartphone (comptes, mots de passe, informations bancaires).

Dans ce cas, la police neuchâteloise appelle la population neuchâteloise à une grande prudence et conseille de ne jamais cliquer sur un lien si l'expéditeur est inconnu. Aucune information sensible ou confidentielle ne doit être fournie lors de prises de contacts inhabituelles.

Alors que faire si le logiciel malveillant a tout de même été téléchargé ? La police neuchâteloise recommande de changer de mot de passe depuis un autre appareil, de bloquer les cartes de crédit utilisées sur le smartphone piraté et d'annoncer le cas à la police en prenant une capture d'écran du SMS reçu, du lien complet ainsi que du numéro de téléphone de l'expéditeur. Par ailleurs, il est possible de supprimer l'application suspecte en redémarrant le téléphone en « mode sans échec ». En dernière mesure, il est possible de réinitialiser

l'appareil infecté après avoir sauvegardé les données importantes. Il n'est en revanche par recommandé de restaurer une sauvegarde postérieure à la réception du SMS.

En cas de tentative ou d'escroquerie avérée, la police neuchâteloise peut être avisée par téléphone au 032 889 90 00 ou via l'adresse e-mail pn.cyber@ne.ch. Pour de plus amples informations, de nombreux renseignements sont disponibles sur le site de la Prévention Suisse de la Criminalité (PSC) : www.skppsc.ch/fr

Contact :

**Police neuchâteloise, secteur information et prévention, police.presse@ne.ch,
tél. 032 889 90 00**

Neuchâtel, le 14.07.2021