Info-délits

Division prévention criminalité

Urgence : 117

Votre Gérant de sécurité :
Adjudant Gilles Perruchoud
Route de Lausanne 32
1400 Yverdon-les-Bains
024 557 70 07
078 615 00 20
gilles.perruchoud@vd.ch

CHAVORNAY – BAVOIS

Votre poste de gendarmerie :

Grand-Rue 76
1373 Chavornay
024 557 79 21

SEPTEMBRE 2018

Date	Délit	Endroit :	Type de lieu	Type de mode opératoire	Flag
04.09	Cybercriminalité	Ch de Chaudremont	Internet / Anibis	Escroquerie à l'achat d'un article	
08.09	Tentative vol d'usage	Terrain de foot de Bavois	Véhicule	Tableau de bord endommagé	
10.09	Vol par effraction	Rue de la Cité	Appartement	Brisé et emporté le cylindre	
11.09	Dommages à la propriété	Rue de Couvalau	Voie publique	Bouté le feu à une poubelle	
12. 09	Vol par effraction	Ch de l'Epignau	Villa	Forcé porte-fenêtre cuisine	
15.09	Vol par effraction	Grand'Rue	Café / restaurant	Forcé imposte porte principale	
22.09	Vol par introduction clandestine	Gare CFF	Véhicule	Véhicule ouvert d'une manière indéterminée	
23.09	Vol d'usage	Rue du Jura	Véhicule		
23.09	Vol par effraction	Rue de Sadaz	Caves (2x)	Forcé serrures à l'outil plat	

Conseil du mois / information

Le Phishing

Obtenir des données personnelles
au moyen d'un site web falsifié

Le "phishing" ou hameçonnage est une technique utilisée pour obtenir des données personnelles, le plus souvent de nature bancaire, dans le but de commettre des infractions contre le patrimoine (achats en ligne ou autres transactions). Cette technique est initiée par des personnes individuelles ou par des bandes organisées. Les vecteurs sont les SMS, les courriels et les sites web.

Mode opératoire

Envoi ciblé ou en masse de courriels, SMS, etc, dont l'adresse d'expédition est falsifiée ou imitée (exemple Swisscom). En général il s'agit d'une demande de renouvellement des données personnelles pour des raisons de sécurité. Le message contient souvent un lien amenant à une page web imitée, où il est demandé de remplir un formulaire avec des données personnelles et bancaires. Les adresses de messagerie des courriels de hameçonnage sont très proches, voire identiques à ceux officiels.

Il peut arriver que des courriels de "phishing" ouvrent directement le formulaire à remplir au lieu de contenir un lien. Il arrive aussi que des sites authentiques aient été piratés pour héberger des pages de "phishing". Le contenu du courriel peut invoquer d'autres motifs que ceux liés à la sécurité, par exemple le remboursement d'une facture payée en trop ou à double.

En plus des données bancaires, les auteurs demandent souvent d'autres données personnelles comme les nom et prénom, identifiants et mot de passe d'accès à divers services en ligne, copie de votre carte d'identité.

Conseils

Si vous êtes victime d'un tel message et avez communiqué des données personnelles, pensez à mettre en œuvre les recommandations suivantes :

- Préservez les moyens de preuve en effectuant des Printscreen de l'adresse de l'expéditeur, de l'en-tête de l'email, le lien, les données transmises et les transactions effectuées.
- Changez tous vos mots de passe au profit de mots de passe "forts".
- Prendre rapidement contact avec votre banque pour bloquer le compte compromis ou récupérer la transaction frauduleuse.
- Déposer plainte dans un poste de gendarmerie

Perruchoud adj