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

AOUT 2018

Date	Délit	Endroit :	Type de lieu	Type de mode opératoire	Flag
06.08	Escroquerie	Ch de Riant-Mont	Internet	Escroquerie type Microsoft (PC soi-disant infecté)	
17.08	Dommages à la propriété	Rte d'Entreroches / Bavois	Véhicule	Lacéré pneus	
23.08	Vol par effraction	Rte d'Yverdon	Chantier	Forcé porte d'un entrepôt	
24.08	Vol simple	Gare CFF	Véhicule	Emporté porte-monnaie laissé dans l'habitacle	

Conseil du mois / information

Cyber-escroquerie

Inciter à transférer de l'argent sur internet

MICROSOFT :

Escroquerie où les auteurs appellent des victimes potentielles en Suisse en se faisant passer pour des techniciens de Microsoft et, après avoir pris le contrôle de l'ordinateur, entreprennent des actions dommageables pour leurs intérêts financiers. Les appels peuvent se faire en anglais, en allemand ou en français.

Mode opératoire :

Les auteurs appellent en général sur le téléphone fixe de la victime, se présentant comme employé de Microsoft. Ils effrayent la victime en lui disant qu'un virus a été détecté sur son ordinateur et qu'il s'agit de le réparer impérativement. Pour se faire ils poussent la victime à télécharger un programme qui permet aux escrocs de prendre le contrôle de la machine. Il est alors proposé un abonnement à un soi-disant logiciel anti-virus. Si la victime accepte ils se rendent sur des sites pour l'achat de ce logiciel, en demandant à la victime de rentrer des données bancaires ou personnelles, pouvant être utilisé pour des paiements illicites en leur faveur.

Conseils :

Si un tel appel vous parvient, n'y donnez aucune suite, raccrochez immédiatement.
Si pour une raison ou une autre vous avez suivi les instructions et donné le contrôle à distance de votre ordinateur, veuillez mettre en œuvre les mesures suivantes :

- Bloquez immédiatement votre carte de crédit et le paiement correspondant.
- Supprimez le logiciel de contrôle à distance et scannez votre ordinateur avec un logiciel antivirus.
- Changez tous les mots de passe qui auraient pu être compromis ou sauvegardés sur votre ordinateur.
- Sauvegarder le numéro de l'appelant, la date et l'heure d'appel; les coordonnée communiquées par l'appelant (nom, prénom.)
- Enregistrer les informations relatives au paiement effectué (bénéficiaire, montant, etc.)

La sauvegarde de ces éléments facilitera l'enregistrement de la plainte, ainsi que les opérations d'enquête.

Pour terminer, informez-vous sur les sites suivant :
www.skppsc.ch et www.scoci.ch

G. Perruchoud adj