Info Délits Plus
Février 2014
Division prévention criminalité

Attention aux escroqueries à l'assistance technique par téléphone !

Depuis quelques mois, on entend de plus en plus fréquemment parler en Suisse d'une nouvelle technique d'escroquerie : l'arnaque à l'assistance technique par téléphone. Le mode opératoire est toujours le même. Il consiste à se faire passer pour un collaborateur du service d'assistance de Microsoft ou d'une compagnie d'antivirus reconnue et d'infiltrer l'ordinateur de sa victime. Le but est d'installer un logiciel espion et de récupérer des informations personnelles sensibles, comme les mots de passe ou les données bancaires. Le fraudeur, parlant généralement anglais, prétend contacter la victime au nom d'une entreprise officielle et essaie de la convaincre de l'existence d'un problème dans son ordinateur. Il lui propose alors de prendre le contrôle de la machine pour y installer un anti-virus ou un logiciel susceptible de régler ledit problème. Dans certains cas, la victime est elle-même priée de se rendre sur un faux site de l'organisation, créé par les escrocs pour l'occasion, afin d'y acheter le produit en question. Les fraudeurs ont alors le champ libre pour installer un cheval de Troie, un logiciel espion, dans l'ordinateur de leur victime, et de récupérer les données bancaires et autres mots de passe.

Une victime qui a récemment vécu une mésaventure similaire, nous explique comment cela s'est déroulé. " *J'avais un ordinateur qui datait de 2006. Dernièrement, au moment d'actualiser l'écran, ce dernier est devenu bleu et la machine s'est bloquée. Comme la machine était vieille, je n'ai pas été particulièrement surpris. J'ai reçu alors un coup de téléphone d'un homme parlant anglais, qui s'est annoncé comme étant un technicien de Windows Amérique qui aurait reçu une notification l'informant que mon ordinateur avait un problème et que les anti-virus n'étaient pas à jour.*

J'ai raccroché, lui expliquant qu'il était plus logique que je rachète un nouvel ordinateur, le mien étant de toute façon devenu obsolète. J'ai donc acheté un nouvel ordinateur et le même homme m'a rappelé le lendemain pour m'expliquer que ce n'était pas la machine qui était infectée mais mon adresse e-mail et que si je n'agissais pas, mon nouvel achat serait également à jeter. Bien que sceptique, je lui ai alors transmis mon adresse IP, les codes d'accès et identifiants de mon adresse e-mail etc, par lesquels ils ont pu piloter mon ordinateur à distance.

Il a travaillé dessus pendant presque 3 heures. Il m'a finalement proposé d'acheter un anti-virus puissant, pour un montant de Frs 285.- et m'a dirigé vers un site "Windows USA", extrêmement bien fait, pour le payer. Alors que je ne me souvenais plus de mon code "secure" pour payer avec ma carte de crédit, il m'a proposé de payer par Western Union. Au moment du paiement, j'ai pu lire sa destination, soit le Sri Lanka, et ai réalisé que mon argent n'était pas transité vers la Californie, comme il me l'avait assuré.

J'ai de suite téléphoné à la compagnie de cartes de crédit pour y faire opposition et j'ai dû remplir un formulaire de contestation.

J'ai dû changer l'adresse IP de mon ordinateur et un technicien de Swisscom s'est déplacé pour extraire le cheval de Troie installé par les fraudeurs.

Je me suis fait avoir comme un bleu !"

Que faire lorsqu'on est confronté à ce genre de situation?
Si une situation similaire vous arrive, la seule réaction recommandée est de raccrocher le téléphone et de suivre les conseils suivants :

Conseils !
- Changez les mots de passe de tous vos comptes financiers !
- Informez immédiatement votre banque/poste et vérifiez vos derniers relevés !
- Modifiez les codes d'accès de toutes vos sessions et messageries !
- Effectuez un "scan" complet de votre ordinateur pour vérifier si un logiciel espion est installé sur votre machine ou contactez un spécialiste informatique !
- Prenez contact avec la maintenance de votre hébergeur, expliquez la situation et demandez de modifier votre adresse IP !
- Si besoin, reformatez votre ordinateur !
- Déposez plainte si vous avez été volé ou contactez la police !

Quelques conseils pour éviter une telle arnaque:
- N'acceptez jamais une offre de maintenance provenant d'un service inconnu !
- N'achetez aucun logiciel anti-virus proposé par un tel correspondant !
- Ne donnez en aucun cas le contrôle de votre ordinateur, sauf si vous pouvez confirmer qu'il s'agit d'un représentant légitime d'une équipe d'assistance technique dont vous êtes déjà client !
- **Ne transmettez jamais vos données bancaires** !

Liens utiles
- Prévention suisse de la criminalité
  http://www.skppsc.ch/10/fr /chercher hameçonnage

- Site officiel de Microsoft,
  http://www.microsoft.com/fr-fr/security/online-privacy/avoid-phone-scams.aspx

- La page Facebook de la Police cantonale :
  https://www.facebook.com/policevd,

- Le fil Twitter de la Police cantonale :
  https://twitter.com/Policevaudoise

Cliquez sur le lien pour lire le magazine de la Polcant,

http://www.vd.ch/fr/autorites/departements/dse/police-cantonale/publications/polcant-information

www.petitchaperonrouge.com
Le site de la Div prév, avec rubrique cinéma et âges conseillés

Pour obtenir plus d'information ou des conseils, contactez les gérants de sécurité :

Région Est, Aigle : Adj Borloz Christian, 021 557 88 05
Région Ouest, Bursins : Adj Genton Etienne, 021 557 44 66
Région Nord, Yverdon : Adj Mermod Willy, 024 557 70 27
Région Lausanne Ouest : Adj Perruchoud Gilles, 021 644 83 36
Région Lausanne Est : Ipa Bourquenoud Christian, 021 644 82 77

La Division prévention de la criminalité sera présente à **Habitat & Jardin du 8 au 16 mars 2014 à Beaulieu / Lausanne, halle 1, stand 105.** Les gérants de sécurité répondront à vos questions sur la prévention des délits et vous expliqueront comment renforcer la sécurité de votre logement, avec du matériel de démonstration et des films.