Delémont, le 11 janvier 2022

Communiqué de presse

Chiffres mensuels de la criminalité

Annexe au tableau daté du 03.01.2022

Attention aux faux techniciens Microsoft

Une cyber escroquerie a refait son apparition. Près d'une dizaine de personnes ont déposé plainte ces dernières semaines après avoir été victimes d'arnaques au faux support informatique, ou aussi appelée « arnaque aux faux techniciens Microsoft ». La police communique quelques conseils simples pour déceler l'arnaque et éviter de donner l'accès à des données et notamment à des codes d'accès bancaires.

L'arnaque au faux support informatique (aussi appelée arnaque Microsoft) consiste à prendre le contrôle de l'ordinateur d'une victime en prétendant agir pour le compte d'un (faux) centre d'assistance informatique. L'objectif est d'obtenir les données du lésé, accéder à ses comptes pour s'enrichir au détriment de la victime. Parfois, l'escroc facture encore son « assistance ».

La prise de contact initiale peut se faire directement par téléphone ou via une fenêtre « pop-up » qui s'ouvre automatiquement à l'écran. Dans ce deuxième cas, il est demandé de téléphoner à un numéro indiqué à l'écran. Dans les deux éventualités, un problème informatique sur le terminal de la cible est avancé. Lenteur, virus ou d'autres symptômes sont expliqués. Se faisant passer pour un employé d'un centre d'assistance informatique connu, la cible est mise en confiance et donne l'accès à distance à son ordinateur. Sous le couvert de la prétendue réparation, le malfaiteur demande des mots de passe, en obtient d'autres en parcourant l'ordinateur et récolte encore bon nombre de données personnelles présentes sur la machine. Mots de passe, codes et autres identifiants de comptes en ligne permettront d'accéder à des comptes bancaires et effectuer des versements. Des commandes peuvent aussi être passées au nom du lésé. Pour couronner le tout, il peut arriver que cette opération de « maintenance » soit facturée et payée en ligne.

Pour se protéger :

- Mettre fin à tous les appels non sollicités provenant de soi-disant opérateurs de Microsoft ou d'autres services d'assistance informatique ;
- Ne pas se fier au numéro qui s'affiche sur l'écran de votre téléphone, il a pu être « truqué » pour correspondre à celui d'une firme de confiance ;
- Ne jamais communiquer des données personnelles (mots de passe ou numéros de cartes de crédit) à d'autres personnes ;
- Ne jamais laisser quelqu'un prendre le contrôle à distance de son ordinateur ;
- Ne pas télécharger de logiciels gratuits à partir de sites internet non fiables ;

- En cas de besoin, toujours utiliser les numéros de téléphone officiels de Microsoft ou des services d'assistance qui sont présents sur les sites officiels ;
- Pour contacter votre institut bancaire, utiliser exclusivement les numéros de téléphone officiels qui sont disponibles, par exemple, sur les extraits de compte.

S'il est trop tard et que quelqu'un a accédé à son ordinateur :

- Couper immédiatement la connexion internet et éteindre l'appareil ;
- Procéder à l'analyse de l'appareil avec un programme antivirus en veillant à ce qu'il soit déconnecté d'internet ;
- Modifiez tous les mots de passe ;
- Solliciter un professionnel pour se faire aider au besoin ;
- Si des données confidentielles ont été communiquées (par ex. des données bancaires ou des informations concernant une carte de crédit), il faut immédiatement contacter la société de cartes de crédit et/ou l'institut bancaire afin de faire bloquer les transactions en cours ;
- Porter plainte auprès de votre police.

D'autres conseils sont disponibles sur le site internet de la Prévention Suisse de la Criminalité (PSC) via le lien suivant : https://www.skppsc.ch/fr/download/betruegerische-supportanrufe-francais/

En cas d'abus, les plaintes peuvent être déposées à la police dans les réceptions.

Personne de contact :
Daniel Affolter, cellule Prévention et Communication à la police cantonale jurassienne, 032 / 420 65 65