Prise de contrôle d'un profil sur les réseaux sociaux/d'une boîte mail

Version PDF

La prise de contrôle d'un profil sur les réseaux sociaux/ d'une boîte mail, qu'est-ce que c'est?

Cette infraction peut prendre plusieurs formes.

Vous ne pouvez plus accéder à votre compte/profil en ligne/boîte mail et/ou vous constatez que quelqu'un y a manifestement accédé sans votre consentement.

ou

Quelqu'un se sert de votre compte/profil en ligne/boîte mail pour envoyer des messages ou faire des publications en votre nom.

D'une manière générale, on parle d'infraction contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes.

Si le contenu de votre compte/profil/boîte mail est altéré, effacé, voire rendu hors d'usage, on parlera alors de sabotage des systèmes informatiques.

Ce type de faits peut intervenir dans un contexte personnel (violences intra-familiales, harcèlement, conflit professionnel...) mais il est le plus souvent le fait d'un individu choisissant ses victimes au hasard, selon les opportunités qui se présentent à lui. Vous ne devez alors pas vous sentir personnellement ni directement visé.

De quoi avez-vous besoin pour déposer plainte ?

Veuillez, dans la mesure du possible, relever les traces et éléments suivants :

- URL (adresse internet) exacte du site/compte/profil concerné ;
- ID (numéro d'identification) unique du site/compte/profil concerné ;
- Si possible, une capture d'écran de la page ou du message concerné ;
- Votre adresse e-mail ;
- Date et heure exacte de cette constatation ;
  - Aperçu des éléments faisant apparaître que quelqu'un a accédé sans autorisation à votre boîte e-mails (par ex. compte rendu inaccessible, messages envoyés à votre nom, messages supprimés sans votre consentement,...);
  - Date, heure, fuseau horaire et adresse IP des dernières connexions à la boîte e-mails, si disponibles (informations consultables uniquement si vous avez encore accès à la boîte);
  - Des photos ou des captures d'écran montrant les traces laissées par le "hacker".
- Date et heure et fuseau horaire du ou des conversation(s) que vous auriez eu avec le(s) suspect(s) ;
- Contenu des mail envoyés par le suspect (à joindre en annexe) + en-tête complet (header) (https://mxtoolbox.com/public/content/emailheaders/);
- Description des actes accomplis à la demande du suspect ;

Que pouvez-vous encore faire ?

- Prévenir tous vos contacts afin que ceux-ci ne se laissent pas tromper par celui qui utilise vos données ;
- Exécutez le programme antivirus sur l'appareil infecté mais également sur tous vos appareils connectés (smartphone, tablette, ordinateur, ...) ;
- Modifiez les mots de passe de l'ensemble de vos comptes (même ceux qui ne semblent pas impactés) ;
- Modifiez vos questions de sécurité ;
- Activez la vérification en deux étapes si possible ;
- Prenez contact avec le fournisseur de service de votre profil/ service de messagerie si le piratage ne vous permet plus d'y accéder ; des options de récupération sont généralement à votre disposition.
- Des options de récupération sont souvent disponibles.

Comment éviter d'être à nouveau victime ?

Afin d’éviter d’être à nouveau victime de ce type de faits,

- Veillez à configurer de manière efficace les règles de sécurité relatives à l'accès à vos ressources en ligne.
- Activer la connexion via double authentification (2FA) lorsque cette option est proposée.

Où pouvez-vous trouver plus d'informations ?

Vous devriez pouvoir trouver davantage d'informations sur la page "Aide/Helpdesk" ou dans les options de sécurité du service/site concerné.