Hameçonnage internet

Vous avez été victime d'hameçonnage internet ?

Nous vous invitons à surtout ne pas répondre à ce mail et à le supprimer. C'est la seule chose à faire ! Si vous avez déjà été victime de ce type de malveillance, allez à la brigade de Gendarmerie de Magny-les-Hameaux. Les gendarmes vous donneront la conduite à suivre.

Comment se protéger contre une tentative de phishing / hameçonnage ?

1. Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.
2. Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

   Vérifiez l'adresse du site qui s'affiche dans votre navigateur.
3. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

   En cas de doute, contactez si possible directement l'organisme concerné
4. pour confirmer le message ou l'appel que vous avez reçu.

Victime d'hameçonnage, que faire ?

1. **Au moindre doute, contactez l'organisme concerné :** en cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.
2. **Faites opposition immédiatement :** si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte, faites opposition immédiatement auprès de votre organisme bancaire ou financier.
3. **Conservez les preuves** et, en particulier, le message d'hameçonnage reçu.
4. **Déposez plainte :** si vous avez constaté que des informations personnelles servent à usurper votre identité ou si vous constatez des débits frauduleux sur vos comptes bancaires, déposez plainte au commissariat de police ou à la brigade de gendarmerie dont vous dépendez. Vous pouvez également adresser votre plainte par écrit au procureur de la République du tribunal judiciaire dont vous dépendez en fournissant toutes les preuves en votre possession. Si vous êtes un particulier, vous pouvez être accompagné gratuitement dans cette démarche par une association de France Victimes au 116 006 (appel et service gratuits), numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9h à 19h.
5. **Changez immédiatement vos mots de passe :** si vous avez malencontreusement communiqué un mot de passe, changez-le immédiatement sur le site ou service concerné, ainsi que sur tous les autres sites ou services sur lesquels vous utilisiez ce mot de passe compromis (tous nos conseils pour gérer au mieux vos mots de passe).
6. **Signalez tout message ou site douteux à Signal Spam :** si vous avez reçu un message douteux, ne cliquez par sur les pièces jointes ou sur le lien suspect.

   Si le message comporte un lien, positionnez le curseur de votre souris sur ce lien (sans cliquer). Cela affichera alors la véritable adresse vers laquelle il redirige afin d'en vérifier la vraisemblance.

   Si vous avez cliqué sur le lien, vérifiez l'adresse du site Internet qui s'affiche dans votre navigateur.

   Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un

seul caractère peut changer dans l’adresse du site pour vous tromper. Ne répondez pas à ces messages suspects et signalez-les à Signal Spam qui est associé à la CNIL pour identifier les principaux émetteurs de spams et mener les actions de luttes nécessaires.

7. **Signalez l’adresse d’un site d’hameçonnage à Phishing Initiative :** vérifiez l’adresse du site Internet qui s’affiche sur votre navigateur. Si elle ne correspond pas exactement au site concerné, il s’agit très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l’adresse du site pour vous tromper.

   Face à un site suspect, vous pouvez le signaler à Phishing Initiative qui bloquera l’adresse de ce site et demandera sa suppression.
8. **Besoin de plus de conseils ?**

   Pour être conseillé dans vos démarches, contactez la plateforme Info Escroqueries du ministère de l’Intérieur au 0 805 805 817 (appel et service gratuits de 9h à 18h30 du lundi au vendredi).

Infos pratiques

Piratage d'un système informatique

Un système informatique (ou système d'information) désigne tout appareil, équipement ou ensemble de ces matériels, permettant de traiter et stocker des données. L'intrusion dans un système informatique se définit comme l'accès non autorisé à ce système par un tiers. Cela peut concerner un ordinateur, un appareil mobile, un objet connecté, un serveur ou le réseau d'une organisation. En pratique, les pirates peuvent recourir à différentes méthodes pour s'introduire dans un système informatique comme l'utilisation d'une faille de sécurité ; la mauvaise configuration d'un logiciel ou d'un équipement ; l'infection par un logiciel malveillant (virus informatiques) ; la récupération d'identifiants de connexion par le biais d'un appel ou d'un message frauduleux (hameçonnage) ; etc.

L'origine de l'intrusion peut être interne (un collaborateur mécontent ou négligeant ou bien encore un prestataire) ou bien externe (cybercriminels). Par la suite, le cybercriminel peut chercher à se propager dans les autres équipements du réseau attaqué. Le piratage d'un système informatique peut donc être d'une grande gravité pour l'organisation qui en est victime puisqu'elle peut entraîner le vol, voire la perte totale, des informations du système touché.

Que faire en cas de piratage d'un système informatique ? Confiner les équipements concernés, préserver les preuves, identifier les origines de l'intrusion, déposer plainte, signaler à la CNIL

IDEM...

Un SMS promettant un gain ? Un clic sur Internet pour contacter une administration ou un professionnel ? Attention, il s'agit peut-être d'arnaques ou de pièges aux numéros surtaxés et Internet+, dont le coût sera prélevé directement sur la facture de téléphone !

Liens utiles
Que faire en cas de phishing ou hameçonnage ?
Signalement auprès de la CNIL
Gendarmerie 2.0 : un service de prise de rendez-vous en ligne
Plus d'information sur la Gendarmerie de Magny-les-Hameaux
Testez vos connaissance