Alerte à l'hameçonnage

Sur Internet la fraude par hameçonnage a augmenté de 350% depuis le début du confinement !

Voici un message que j'ai reçu ce matin de soi-disant ma banque. Intrigué par la teneur de ce message, je l'ai analysé (voir pièce jointe : *analyse d'un phishing*)

J'ai cliqué volontairement sur le lien pour voir vers quoi le pirate veut que j'aille et j'ai obtenu une copie conforme de la page d'accès aux comptes (voir deuxième page jointe : *Fac-similé de la saisie d'identifiants*) avec ironiquement les alertes à la vigilance face aux fraudes…

Si j'avais saisi dans cette page mes identifiants, ceux-ci seraient arrivés chez le pirate !!!

J'ai transféré le message sur le site alerte@securite.lcl.fr de ma banque.

J'ai détruit ensuite le mail

Si vous voyez ce type de message :

- Ne répondez pas au message
- Ne cliquez pas sur le lien proposé dans le message
- De manière générale, ne communiquez jamais vos identifiants à partir d'un mail.

Ce qu'il faut faire

- Fermez votre messagerie et allez directement, avec votre navigateur Internet, sur le site de l'organisme. Ouvrez votre compte avec vos identifiants.
- Vérifiez si vous avez sur le site original une alerte

Qu'est-ce que le phishing par internet ?

Le phishing (ou « hameçonnage ») est une technique d'escroquerie par Internet de plus en plus utilisée par les pirates informatiques pour voler des données personnelles telles que :

- votre nom et votre adresse,
- vos coordonnées (téléphone, adresse postale, etc.),
- votre date de naissance,
- votre numéro de compte bancaire,
- votre numéro de sécurité sociale,
- vos identifiants de connexion Internet à des sites bancaires ou à des sites marchands...
- vos identifiants et mots de passe de messagerie,
- etc.

Pour obtenir ces informations, les pirates envoient un courriel frauduleux qui semble provenir de l'Administration (service des Impôts, Assurance Maladie, Caisse d'allocations familiales), d'une banque ou d'une société reconnue (opérateur téléphonique, opérateur d'énergie, site de e-commerce, etc.).

Si vous avez déjà répondu à un mail frauduleux :

- **modifiez les mots de passe** transmis par inadvertance ;
- prévenez l'organisme dont l'identité a été usurpée ;

Jean MIGUET