Emails frauduleux (phishing): cinq règles d'or pour ne pas se faire arnaquer !

Je suis constamment importuné par des demandes d'aide provenant de proches. Je sais, à l'usage, que ce sont des tentatives d'escroqueries mais ça m'agace !

J'ai une mauvaise nouvelle pour tous ceux que se laissent prendre et répondent à ces mails frauduleux. Il semble qu'à l'avenir, les victimes de hameçonnage pourraient être moins bien protégées par la justice, notamment pour se faire rembourser des dépenses frauduleuses.

Je reviens sur ces arnaques pour quelques précisions. Qu'on les regroupe sous le terme de phishing ou hameçonnage, les emails frauduleux peuvent nous coûter très cher. Ils prennent la forme d'une relance de son opérateur, des services fiscaux ou de sa banque pour mettre ses données personnelles à jour, pour régler un impayé, voire pour être remboursé d'un trop-perçu.

Je suppose que vous vous appuyez sur un jugement pour expliquer que nous serons moins protégés face à un hameçonnage ?

La cours de Cassation a rendu un arrêt concernant le cas de hameçonnage d'un client du Crédit Mutuel. La banque, qui refusait de rembourser des montants prélevés grâce à des mails imitant son logo, a bénéficié d'un jugement favorable. C'est donc à nous de faire très attention et de déjouer les tentatives de phishing.

Je suis preneur de conseils si vous en avez bien entendu !

Il existe quelques réflexes simples pour éviter de tomber dans le piège.

1. Afficher l'adresse mail du destinataire

En cas de doute sur la nature d'un mail, il est impératif de vérifier l'adresse de l'expéditeur. Si l'expéditeur dispose d'une adresse liée à un service de messagerie destiné aux particuliers (@hotmail.fr ou @gmail.com, par exemple), passez votre chemin.

2. Ne jamais cliquer sans vérifier que votre fournisseur d'électricité vous a effectivement envoyé un mail. Un passage par votre compte client vous évitera des déboires.

3. Ne jamais répondre à une demande de paiement même semblant légitime sans vérifier le protocole de sécurité HTTPS.

4. Ne jamais appeler un numéro de téléphone intégré au mail. En cas de doute, il faudra chercher soi-même le numéro du service client en question, afin de vérifier l'authenticité de la demande.

5. Ne jamais faire confiance (même à ses proches) !

En début d'année, une campagne de frauduleuse envahissait WhatsApp. En promettant des billets d'avion gratuits sur Air France, les auteurs de la fausse publicité ont pu compter sur le bouche à oreille pour faire circuler leur escroquerie. Le message renvoyait vers un faux site, dont l'URL était: http://ạirfrance.com. La présence d'un point sous le premier "a" aura alerté les plus observateurs.

Avril 2018 Serge AVEILLAN