CONSOMMATION Arnaques sur Internet

Un proche en détresse à l'étranger ? Son mail piraté !

Il existe deux types de pirates mail : ceux qui prélèvent discrètement les informations personnelles et ceux qui rackettent directement nos contacts, par usurpation d'identité. On ne dénombre plus le nombre de victimes, souvent peu à l'aise avec l'informatique.

Un mot de passe trop faible, et c'est la porte ouverte aux hackers qui pillent les informations personnelles pouvant avoir une valeur marchande, directe ou indirecte : identifiants (réseaux sociaux, sites d'e-commerce), coordonnées des contacts, informations bancaires, documents confidentiels...

> « J'ai bien failli marcher. Mais ma femme était convaincue que ce n'était pas possible »

Mais il existe aussi un autre type de piratage. Ses adeptes adressent des courriels directement à nos contacts en usurpant notre identité !

La technique est toujours la même : les pirates suscitent la compassion à travers des messages inquiétants, avant de réclamer de l'argent par virement. Une pratique connue depuis des années mais elle perdure. Il faut dire qu'elle est lucrative.

Tout récemment encore, un retraité de 77 ans résidant à Riedisheim a failli être victime de cette arnaque. Il a été destinataire d'un mail envoyé par son fils. Croyait-il, en tout cas.

« Dans ce mail, mon fils m'expliquait qu'il était en déplacement, qu'on lui avait volé son téléphone et qu'il était dans une situation financière délicate. Il demandait dans la foulée que j'aille lui acheter dans un bureau de tabac cinq cartes de paiement prépayées rechargeables avec des recharges de 250 € l'unité, et que je lui communique ensuite les numéros des cartes », raconte le septuagénaire. « J'ai bien failli marcher. Mais ma femme était convaincue que ce n'était pas possible. Notre fils est enseignant et il ne pouvait pas être en déplacement à l'étranger alors qu'il devait faire sa rentrée. Ma femme a donc contacté l'épouse de mon fils. Cette dernière a raconté qu'ils étaient inondés de coup de téléphone et de mails. C'était bien une arnaque, un piratage de sa boîte mail. »

« Je suis en voyage et j'ai été victime d'une agression »

Des arnaques de ce type, il y en a à la pelle. La variante la plus connue repose sur l'usurpation de l'identité d'un ami proche. Ce dernier donne des nouvelles inquiétantes dans un courriel pressant. Le message type est le suivant : « Bonjour à toi ! J'espère que je ne te dérange pas. Je suis dans une situation désastreuse. Je suis en voyage et j'ai été victime d'une agression. J'ai besoin de ton aide financière afin de rentrer au plus vite, je pourrai te donner plus de détails dans mon prochain mail. C'est vraiment délicat. Réponds-moi vite. » La victime répond alors au message pour obtenir davantage d'informations... Et l'ami en question lui demande en retour de lui faire parvenir un mandat cash pour « résoudre ses problèmes urgents ».

En réalité, plusieurs contacts enregistrés dans le compte mail piraté reçoivent en général ce même mail frauduleux. Si vous recevez un tel message, n'y répondez pas si l'histoire vous paraît complètement absurde. Et si vous avez un doute, vérifiez auprès de la famille ou des connaissances de votre ami. Ou mieux, auprès de votre ami lui-même, par téléphone par exemple.

Boîte mail piratée, le conseil d'un professionnel

Comment éviter ce genre de mésaventure ? « Il faut savoir qu'aucun fournisseur mail (Yahoo, Google, Outlook, etc.) n'est plus sécurisé qu'un autre. Ce type de piratage est possible en raison de la faiblesse des mots de passe utilisés. La meilleure des sécurités est d'adopter un mot de passe fort, impossible à deviner ou difficile à déduire depuis un logiciel de cracking. Si vous êtes victime d'un piratage de compte mail, il faut vous connecter à votre messagerie et modifier votre mot de passe, pour empêcher que le pirate ne s'y connecte à nouveau. Si celui-ci vous a précédé et que votre mot de passe a déjà été changé, il faut alors contacter votre opérateur mail et lui signaler le piratage du compte », explique un spécialiste informatique d'une enseigne réputée.

En réalité, seule la prévention peut permettre de lutter contre ce fléau. Et pour être tranquille, la meilleure précaution consiste à modifier son mot de passe en prenant le soin d'en choisir un qui donnera du fil à retordre aux nombreux pirates (et leurs robots) qui arpentent la toile. ■

ALAIN CHEVAL

QUE FAIRE EN CAS D'ARNAQUE ?

L'escroquerie est définie par le code pénal comme le fait de tromper une personne physique ou morale, par l'usage d'une fausse identité ou l'emploi de manœuvres frauduleuses, afin de la conduire à remettre des fonds, des valeurs ou un bien. Elle est punissable de cinq ans d'emprisonnement et 375 000 € d'amende.

Sur Internet, les escroqueries sont monnaie courante : transaction bancaire sans retour du bien acheté, « phishing » (technique consistant à se faire passer pour votre banque afin d'obtenir vos coordonnées bancaires), utilisation frauduleuse de numéros de carte bleue, escroquerie « à la nigériane » consistant à envoyer un message de demande d'aide visant à obtenir de la victime une participation financière, etc.

Que faire en cas de cyberattaque ou d'arnaque ?

Il est possible que vous fassiez face à des comportements suspects, auquel cas il n'y a pas lieu de déposer une plainte mais qu'il est important de signaler. Si vous êtes vraiment victime d'une arnaque financière, le dépôt de plainte s'impose.

En France, le site portail du ministère de l'intérieur www.internet-signalement.gouv.fr et le numéro INFO ESCROQUERIE (✆0805 805 817, prix d'un appel local) ont vocation à recueillir les signalements d'escroqueries sur Internet et à donner des conseils et répondre aux questions des internautes sur la protection de leur connexion. Peuvent être signalés des contenus ou comportements illicites, c'est-à-dire interdits par la loi française, et non des comportements que vous jugerez simplement immoraux ou nuisibles.

Le dépôt de plainte ne s'applique qu'en cas de préjudice (si vous avez perdu de l'argent). En France, c'est la localisation géographique de l'ordinateur « victime » de l'attaque qui va déterminer où porter plainte.