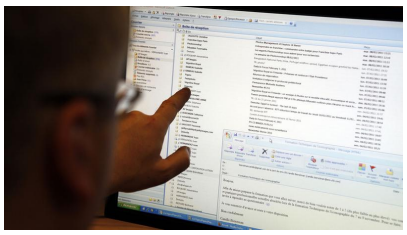
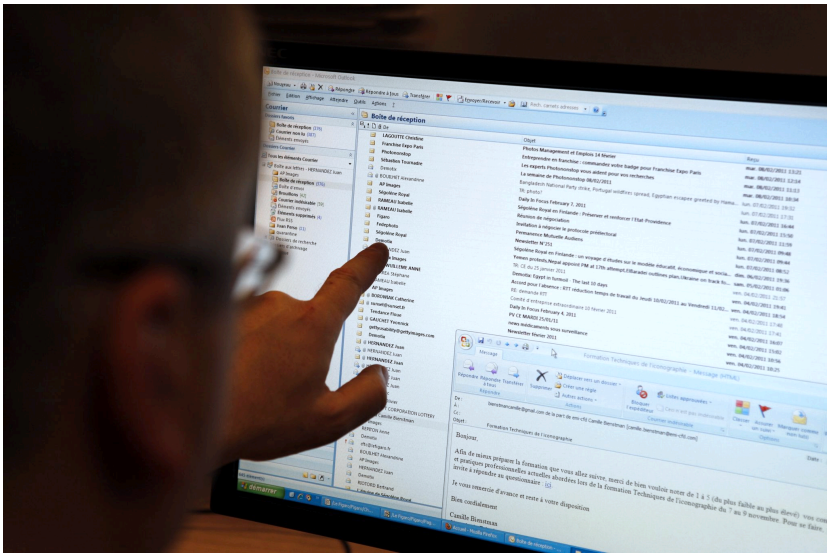
100 fois plus de victimes vol de données personnelles en deux ans en France



100 fois plus de victimes vol de données personnelles en deux ans en France

En 2015, cette pratique visant à dérober des informations personnelles par Internet ou par téléphone a fait plus de 2 millions de victimes en France. C'est cent fois plus qu'il y a deux ans.



Véritable piège pour les internautes, la pratique du phishing ne cesse de se répandre en France. Contraction de «fishing» (pêche) et «phreaking» (piratage de lignes téléphoniques), ce procédé malveillant vise à soutirer des données personnelles (mot de passe, identifiant de connexion, numéros de cartes bancaires). On parle également de «hameçonnage».

Sur la seule année 2015, plus de 2 millions de personnes auraient été victimes du phishing en France. C'est 100 fois plus qu'il y a deux ans, selon Europe 1 qui reprend un rapport de Phishing Initiative, site reconnu par les services de lutte contre la cybercriminalité. Le plus souvent, cette arnaque se manifeste par la réception d'un mail personnalisé provenant d'un organisme financier (banques), d'une entreprise (fournisseur d'Internet, EDF…) ou même d'une administration publique (CAF)… Du moins en apparence.

Car le message en question, aussi crédible et réaliste qu'il puisse paraître, vous invite en réalité à cliquer sur un lien, lequel vous redirige vers un site vous demandant de mettre à jour vos données personnelles. Dès lors, en se faisant passer pour des tiers, les cybercriminels à l'origine de ces mails frauduleux sont en mesure de récupérer vos informations personnelles. «L'augmentation des pratiques de phishing s'explique notamment par le nombre croissant de cybercriminels organisés en réseaux très structurés. D'autant que leurs méthodes sont de plus en plus sophistiquées. Auparavant, des fautes d'orthographe présentes dans les mails permettaient d'éveiller les soupçons. Désormais, c'est plus dur à déceler car ils paraissent davantage crédibles», explique Raphaël Renaud, spécialiste des questions liées au phishing.

Usurpées, les banques comme les grandes entreprises sont, elles aussi, directement concernées par le phishing. En modernisant leurs systèmes de sécurité, elles parviennent parfois à contrer les menaces. C'est le cas de Google qui a bloqué 7000 sites utilisés pour des attaques de phishing en 2015. De leur côté, les établissements bancaires assurent «un service de veille et donc une certaine publicité pour prévenir leurs clients, mais celle-ci est souvent insuffisante», remarque Serge Maître, secrétaire général de l'Association Française des Usagers des Banques (AFUB), avant de souligner que «le cryptogramme et le 3D Secure ont montré leurs limites face aux attaques de phishing.»

Comment réagir face au phishing?

S'il n'est pas encore trop tard, plusieurs méthodes permettent de contrer le phishing. Dans un premier temps, il est préférable de disposer d'un antivirus performant. Ensuite, «l'ultime chose à faire est de ne jamais cliquer dans un lien provenant d'un e-mail. Les services sérieux (banque, opérateurs téléphoniques, etc…) ne vous demandent jamais de changer un mot de passe de cette manière», explique Raphaël Richard avant d'ajouter «qu'il faut directement se connecter sur le site officiel pour ne pas avoir de doute». Enfin, certains sites tels que ou Phishing Initiative permettent de faire vérifier un mail en cas de soupçon mais également de signaler des adresses qui semblent suspectes.

En revanche, si un internaute vient d'être victime de phishing, il doit «déposer plainte si possible devant une brigade spécialisée dans les 48 heures car au-delà, cela devient plus compliqué. Il faut également contacter … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le nombre de victimes de vol multiplié par 100 en deux ans en France*