OUCH ! Novembre 2024

La lettre d'information mensuelle de sensibilisation à la sécurité

Ne laissez pas les cyber-criminels vous voler vos économies : sécurisez vos comptes bancaires !

Une arnaque et un compte bancaire vide

Émilie passait un jeudi chargé comme d'habitude. Elle buvait son café du matin lorsqu'elle a vu sur son téléphone un message de sa banque qui disait : "Avez-vous effectué cette transaction ? Répondez OUI ou NON". Elle a froncé les sourcils. Elle n'avait fait aucun achat ce jour-là. C'était peut-être une erreur.

Elle a répondu "NON", et quelques minutes plus tard, elle a reçu un appel. C'était une femme qui prétendait faire partie du service des fraudes de sa banque, et qui lui parlait calmement, avec un ton professionnel. "Nous avons détecté des activités inhabituelles sur votre compte. Pour la sécurité, nous avons besoin de vérifier quelques détails." Émilie, toujours endormie, s'est exécutée. L'interlocutrice a guidé Émilie pendant une série d'étapes, lui demandant son mot de passe bancaire et lui indiquant de confirmer les notifications de confirmation sur son téléphone. "Cela bloquera l'accès au hacker", a assuré la femme. Émilie a suivi les étapes, ne réalisant pas qu'elle tombait dans le piège.

Quelques heures plus tard, le téléphone d'Émilie a de nouveau sonné. Cette fois, c'était une notification : 5 000 euros avaient été débités de son compte en banque. Complètement paniquée, elle s'est connectée à son compte en banque, mais c'était trop tard. Son mot de passe ne fonctionnait plus sur l'application. Son compte était bloqué. Puis elle a vu un autre retrait se produit, et un autre encore.

Émilie a compris immédiatement. L'appel du "service de fraude" était un coup monté, une attaque bien orchestrée par un cyber-criminel qui était maintenant en contrôle de son compte. Émilie a rapidement appelé sa banque en espérant pouvoir sauver son compte en banque à temps.

Pourquoi vous devez protéger vos comptes bancaires

Nos comptes bancaires en ligne, comptes chèques, comptes d'épargne et comptes d'investissement, contiennent plus que de l'argent ; ils représentent des années de dur labeur, de projets d'avenir et de stabilité financière. Les cybercriminels sont constamment à l'affût d'opportunités pour accéder à votre argent, et une seule erreur peut entraîner des pertes financières considérables. Si vous pensez qu'un simple mot de passe empêchera ces criminels d'accéder à votre compte, vous vous trompez.

Les cybercriminels d'aujourd'hui sont intelligents, sournois et implacables. Il est essentiel d'être proactif dans la sécurisation de vos comptes bancaires. Non seulement vous éviterez ainsi tout accès non autorisé, mais vous aurez également l'esprit tranquille en sachant que votre argent durement gagné est en sécurité.

Cinq étapes pour barrer la route aux cybercriminels

1. **Activez dès maintenant l'authentification multifactorielle (AMF) :** L'authentification multifactorielle ajoute une couche de sécurité supplémentaire à vos comptes en ligne en vous demandant de vérifier votre identité par au moins deux méthodes : quelque chose que vous connaissez (mot de passe), quelque chose que vous avez (téléphone), ou quelque chose que vous êtes (empreinte digitale ou reconnaissance faciale). Même si un cybercriminel obtient votre mot de passe, il aura toujours besoin du deuxième facteur pour accéder à votre compte. Optez toujours pour l'AMF lorsqu'elle est disponible, en particulier pour les comptes bancaires.

2. **Utilisez des mots de passe forts et uniques :** créez des mots de passe forts et uniques pour chaque compte. Plus votre mot de passe est long et comporte de caractères, mieux c'est. Une possibilité consiste à utiliser une phrase de passe, c'est-à-dire un mot de passe composé de plusieurs mots. Vous n'avez pas une bonne mémoire ? Pas de problème. Utilisez un gestionnaire de mots de passe pour vous aider à créer et à conserver tous ces mots de passe longs et uniques.

3. **Les escroqueries sont constantes, ne tombez pas dans le panneau :** l'un des moyens les plus faciles pour les cyber-attaquants d'accéder à vos comptes est de vous demander votre autorisation. Ils créent des emails, des SMS ou même des appels téléphoniques qui semblent provenir de votre banque ou de votre institution financière. Vérifiez toujours la source avant de cliquer sur des liens, de télécharger des pièces jointes ou de répondre à des messages ou à des appels téléphoniques. Plus le sentiment d'urgence est grand, plus l'email, le message ou l'appel téléphonique est susceptible d'être une attaque. La meilleure façon de vous protéger est de vous rendre directement sur le site officiel de votre banque en tapant l'adresse dans votre navigateur, ou de rappeler votre banque ou votre institution financière en utilisant un numéro de téléphone de confiance.

4. **Suivez de près vos comptes :** prenez l'habitude de vérifier fréquemment vos comptes financiers pour détecter toute transaction inhabituelle. Mieux encore, la plupart des institutions financières proposent des alertes automatiques en cas de retraits importants ou d'activités suspectes. La mise en place d'alertes automatisées peut vous aider à détecter rapidement les transactions frauduleuses et à prendre des mesures rapides pour minimiser les dommages. Si quelque chose ne vous semble pas normal, n'attendez pas et agissez immédiatement.

5. **Gardez vos appareils bien verrouillés :** votre téléphone, votre ordinateur portable et votre tablette sont comme les coffres-forts de votre monde financier. Protégez-les avec un mot de passe de verrouillage fort et les dernières mises à jour logicielles. Nous vous recommandons d'activer la mise à jour automatique.

Rédacteur invité

Elizabeth Rasnick est professeure adjoint au Centre de cybersécurité de l'université de Floride occidentale. Elle a de l'expérience en programmation et a fait partie d'une équipe d'intervention en cas d'incident. Elle est vice-présidente senior de l'affilié de WiCyS en Floride et est titulaire d'un doctorat en technologie de l'information.

Ressources

Les trois principaux moyens utilisés par les cyber-attaquants pour vous cibler :
https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Déclencheurs émotionnels, comment les cyber-attaquants vous piégent :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Traduit pour la Communauté par : Juliette Busson