OUCH! Juin 2023

Votre bulletin mensuel sur la sensibilisation à la sécurité

Sécuriser vos comptes financiers

Aperçu

Vos comptes financiers sont une cible privilégiée pour les cybercriminels. Vous avez de l'argent et ils sont prêts à tout pour vous le voler. Par comptes financiers, nous entendons non seulement vos comptes de chèques ou d'épargne, mais aussi vos investissements, votre retraite et vos comptes de paiement en ligne tels que PayPal. Heureusement, quelques mesures simples et fondamentales vous permettent de vous protéger.

Comment attaquent-ils ?

Les banques investissent des sommes considérables dans la sécurisation de leurs systèmes, ce qui rend extrêmement difficile le piratage par un cybercriminel. C'est pourquoi les cybercriminels s'en prennent plutôt à vous et à vos comptes. Ils savent que vous n'avez pas votre propre équipe de sécurité pour vous protéger, et qu'il est donc beaucoup plus facile de vous pirater qu'une banque. Voici les deux façons les plus courantes de vous prendre pour cible et tenter de vous voler votre argent :

Mots de passe : Chacun de vos comptes financiers est protégé par un mot de passe. Si un cybercriminel parvient à deviner ou à compromettre l'un de ces mots de passe, il peut se faire passer pour vous et transférer votre argent sur des comptes bancaires qu'il contrôle. Il existe de nombreuses façons d'obtenir votre mot de passe. L'une des méthodes les plus courantes consiste à infecter votre ordinateur avec des logiciels malveillants. Une fois votre ordinateur infecté, ils peuvent s'emparer de votre nom d'utilisateur et de votre mot de passe lorsque vous accédez au site web de votre banque. Une autre méthode courante consiste à envoyer des courriels d'hameçonnage qui prétendent provenir de votre banque. Lorsque vous cliquez sur le lien contenu dans l'e-mail, vous pensez vous connecter au site web de votre banque, mais en réalité, vous vous connectez à un faux site web contrôlé par les criminels. Cela leur permet de récupérer votre nom d'utilisateur et votre mot de passe, qu'ils peuvent ensuite utiliser pour se connecter en votre nom.

Demander : Les cybercriminels peuvent simplement vous demander votre mot de passe ou vous demander de leur transférer de l'argent. Ces attaques d'ingénierie sociale commencent souvent par un appel téléphonique. Les cybercriminels savent qu'une fois qu'ils vous ont fait parler, il leur est beaucoup plus facile d'utiliser l'émotion pour vous faire commettre une erreur. C'est pourquoi vous commencez à voir de plus en plus d'e-mails de phishing, de messages vocaux et de bannières d'avertissement qui créent un sentiment d'urgence en vous disant que vous devez appeler un numéro de téléphone pour résoudre un problème ou pour profiter d'une opportunité exceptionnelle avant qu'elle n'expire. Une fois que vous avez appelé le numéro de téléphone, les criminels créent un énorme sentiment de pression pour que vous leur donniez accès à vos comptes ou que vous transfériez votre argent sur d'autres comptes pour eux. Par exemple, ils peuvent vous dire qu'ils sont de l'assistance technique ou du gouvernement, que votre ordinateur est infecté et que si vous n'agissez pas maintenant, vous perdrez tout votre argent.

Vous protéger

Heureusement, sécuriser vos comptes bancaires est plus simple que vous ne le pensez. Voici les étapes clés pour vous protéger.

Soyez méfiant : avant toute chose, vous êtes votre meilleure défense. Si vous recevez un courriel, un message texte, un message vocal ou une bannière d'avertissement de votre navigateur qui vous semble étrange ou suspect, il peut s'agir d'une attaque. Plus le sentiment d'urgence est grand et plus on vous presse d'agir IMMÉDIATEMENT, plus il est probable qu'il s'agisse d'une attaque.

Utilisez des mots de passe forts / AMF : Protégez chacun de vos comptes financiers et personnels par un mot de passe long et unique. Vous ne vous souvenez plus de tous ces mots de passe uniques ? Envisagez d'utiliser un gestionnaire de mots de passe pour les mémoriser et les stocker en toute sécurité. La meilleure façon de protéger chacun de vos comptes financiers est d'activer une fonction appelée authentification multifactorielle (AMF) sur chaque compte.

Contrôle : Enfin, contrôlez tous vos comptes financiers. Vous pouvez mettre en place des alertes automatiques qui vous enverront un courrier électronique ou un SMS chaque fois que de l'argent est transféré sur vos comptes ou en est retiré. Vous pouvez ainsi détecter rapidement toute transaction non autorisée ou suspecte. Plus vite vous détecterez un problème et le signalerez à votre banque, plus vous aurez de chances de récupérer votre argent.

Rédacteur Invité

Lynn Dohm est la directrice exécutive de Women in CyberSecurity (WiCyS). Grâce à son expérience dans le secteur de l'enseignement de la cybersécurité et à sa participation active à des programmes financés par des subventions et à des organisations à but non lucratif, Lynn défend l'importance de la diversification de la main-d'œuvre dans le domaine de la cybersécurité et sensibilise le public à cette question.
Twitter : @lynn_dohm. LinkedIn : https://www.linkedin.com/in/lynndohm/.

Ressources

Les déclencheurs émotionnels Comment les cybercriminels vous piègent :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Les attaques par hameçonnage deviennent de plus en plus travaillées :
https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/password-managers/
Authentification multifactorielle :
https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Traduit pour la communauté par : Juliette Busson