OUCH! Septembre 2021

Votre publication mensuelle de conscientisation à propos de la Sécurité

Une étape simple pour sécuriser vos comptes

Est-ce qu'il semble que les cybercriminels aient une baguette magique pour accéder à votre courrier électronique ou à vos comptes bancaires et que vous ne puissiez rien faire pour les arrêter? Ne serait-il pas formidable s'il y avait une seule mesure que vous pouviez prendre pour vous protéger des cybercriminels et vous permettre de tirer le meilleur parti de la technologie en toute sécurité? Bien qu'aucune mesure unique n'arrête tous les cybercriminels, l'une des mesures les plus importantes que vous puissiez prendre est d'activer ce qu'on appelle l'authentification à deux facteurs (parfois appelée 2FA, vérification en deux étapes ou authentification multi-facteur) sur vos comptes les plus importants.

Le problème avec les mots de passe

Lorsqu'il s'agit de protéger vos comptes, vous utilisez probablement déjà un type de mot de passe. Il existe plusieurs façons de vous authentifier sur un compte: quelque chose que vous avez, quelque chose que vous savez, quelque chose que vous êtes, quelque part vous êtes. Lorsque vous utilisez plusieurs méthodes d'authentification, vous ajoutez une couche de protection supplémentaire contre les cybercriminels - même s'ils piratent une méthode, ils devront toujours contourner le ou les facteurs supplémentaires pour accéder à votre compte. Les mots de passe prouvent qui vous êtes basé sur quelque chose que vous connaissez. Le danger avec les mots de passe est qu'ils constituent un point de défaillance unique. Si un cybercriminel peut deviner ou compromettre votre mot de passe, il peut accéder à vos comptes les plus importants. De plus, les cybercriminels développent des techniques plus rapides et meilleures pour deviner, compromettre ou contourner les mots de passe. Heureusement, vous pouvez riposter avec l'authentification à deux facteurs.

L'authentification à deux facteurs

L'ajout d'une authentification à deux facteurs est une solution bien plus sécurisée que de se fier uniquement aux mots de passe. Cela fonctionne en exigeant non pas une mais deux méthodes différentes pour vous authentifier. De cette façon, si votre mot de passe est compromis, votre compte est toujours protégé. Un exemple est votre carte ATM; lorsque vous retirez de l'argent d'un guichet automatique, vous utilisez en fait une forme d'authentification à deux facteurs. Pour accéder à votre argent, vous aurez besoin de deux choses: votre carte bancaire (quelque chose que vous avez) et votre code PIN (quelque chose que vous connaissez). Si vous perdez votre carte bancaire, toute personne qui trouve votre carte ne peut pas retirer votre argent car elle ne connaît pas votre code PIN. Il en va de même s'ils n'ont que votre code PIN et non la carte. Un attaquant doit avoir les deux pour compromettre votre compte bancaire. Le concept est similaire pour l'authentification à deux facteurs; vous avez deux niveaux de sécurité.

Utilisation de l'authentification à deux facteurs en ligne

L'authentification à deux facteurs est quelque chose que vous configurez individuellement pour chacun de vos comptes.

C'est en fait assez simple: vous n'avez généralement rien d'autre à faire que de synchroniser votre téléphone mobile avec votre compte. De cette façon, lorsque vous devez vous connecter à votre compte, non seulement vous vous connectez avec le nom d'utilisateur et le mot de passe de votre compte, mais vous utilisez également un code unique à usage unique que vous obtenez à partir de votre téléphone. L'idée est que la combinaison de votre mot de passe et d'un code unique est requise pour vous connecter. Habituellement, ce code unique sera envoyé par SMS sur votre appareil mobile ou par e-mail. Votre téléphone peut également disposer d'une application mobile (telle que l'application Google ou Microsoft Authenticator) qui générera le code unique pour vous. Lorsque cela est possible, les applications mobiles sont considérées comme l'option la plus sûre pour obtenir votre code unique.

Ce qui rend cela si simple, c'est que vous n'avez généralement à le faire qu'une seule fois à partir de l'ordinateur ou du périphérique que vous utilisez pour vous connecter. Une fois que le site Web ou votre compte reconnaît votre appareil, vous n'avez souvent besoin que de votre mot de passe pour vous connecter. Chaque fois que vous essayez (ou que quelqu'un d'autre essaie) de vous connecter avec votre compte mais à partir d'un autre ordinateur ou appareil, il devra à nouveau utiliser l'authentification à deux facteurs. Cela signifie que si un cybercriminel obtient votre mot de passe, il ne peut toujours pas accéder à votre compte car il ne peut pas accéder au code unique.

N'oubliez pas que l'authentification à deux facteurs n'est généralement pas activée par défaut, vous devrez donc l'activer vous-même pour chacun de vos comptes les plus importants, tels que la banque, les investissements, la retraite ou la messagerie personnelle. Bien que cela puisse sembler plus de travail au début, une fois configuré, il est très facile à utiliser.

Rédacteur invité

Lysandra Capella a plus de 15 ans d'expérience dans le domaine de la sécurité et de la technologie de l'information. Elle est instructrice du SANS Institute en formation pour SANS AUD507, axée sur la mesure et la gestion des risques. Lorsqu'elle n'enseigne pas, Lysandra soutient les équipes de direction dans la formulation de la stratégie, l'assurance de la sécurité et la gouvernance informatique. https://www.linkedin.com/in/lysandracapella/.

Ressources

Simplifier les mots de passe: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Gestionnaire de mots de passe: https://www.sans.org/newsletters/ouch/password-managers/