SOYEZ CYBER SMART
#CyberMonth

MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2021 : FAITES VOTRE PART. #BECYBERSMART

AUTHENTIFICATION MULTIFACTEUR

Avez-vous remarqué à quelle fréquence les failles de sécurité, le vol de données et l'usurpation d'identité font régulièrement la une des journaux de nos jours ? Peut-être que vous, ou quelqu'un que vous connaissez, êtes victime de cybercriminels qui ont volé des informations personnelles, des informations d'identification bancaires, etc. À mesure que ces incidents deviennent plus fréquents, vous devriez envisager d'utiliser l'authentification multifacteur, également appelée authentification forte, ou authentification à deux facteurs. Cette technologie vous est peut-être déjà familière, car de nombreuses institutions bancaires et financières exigent à la fois un mot de passe et l'un des éléments suivants pour se connecter : un appel, un email ou un SMS contenant un code. En appliquant ces principes de vérification à un plus grand nombre de vos comptes personnels, tels que les emails, les réseaux sociaux, etc., vous pouvez mieux sécuriser vos informations et votre identité en ligne !

QU'EST-CE QUE C'EST

L'authentification multifacteur (MFA) est définie comme un processus de sécurité qui nécessite plusieurs méthodes d'authentification provenant de sources indépendantes pour vérifier l'identité de l'utilisateur. En d'autres termes, une personne souhaitant utiliser le système n'y a accès qu'après avoir fourni deux ou plusieurs éléments d'information qui l'identifient de manière unique.

COMMENT ÇA FONCTIONNE

Il existe trois catégories d'informations d'identification : quelque chose que vous connaissez, possédez ou êtes. Voici quelques exemples dans chaque catégorie.

QUELQUE CHOSE QUE VOUS CONNAISSEZ
- Mot de passe/phrase de passe
- Code PIN

QUELQUE CHOSE QUE VOUS AVEZ
- Jeton de sécurité ou application
- Texte de vérification, appel, email
- Carte à puce

QUELQUE CHOSE QUE VOUS ÊTES
- Empreinte digitale
- La reconnaissance faciale
- Reconnaissance vocale

Pour y accéder, vos identifiants doivent provenir d'au moins deux catégories différentes. L'une des méthodes les plus courantes consiste à se connecter à l'aide de votre nom d'utilisateur et de votre mot de passe. Ensuite, un code à usage unique sera généré et envoyé à votre téléphone ou à votre email, que vous saisirez ensuite dans le délai imparti. Ce code unique est le deuxième facteur.

QUAND FAUT-IL L'UTILISER

MFA doit être utilisé pour ajouter une couche de sécurité supplémentaire autour des sites contenant des informations sensibles, ou chaque fois qu'une sécurité renforcée est souhaitable. MFA rend plus difficile pour les personnes non autorisées de se connecter en tant que titulaire du compte. Selon le Institut national des normes et de la technologie (NIST), le MFA doit être utilisé dans la mesure du possible, en particulier lorsqu'il s'agit de vos données les plus sensibles, telles que votre courrier électronique principal, vos comptes financiers et vos dossiers médicaux. Certaines organisations vous demanderont d'utiliser MFA ; avec d'autres c'est facultatif. Si vous avez la possibilité de l'activer, vous devez prendre l'initiative de le faire pour protéger vos données et votre identité.

ACTIVEZ LE MFA SUR VOS COMPTES IMMEDIATEMENT

Pour savoir comment activer MFA sur vos comptes, rendez-vous sur le site Verrouillez votre connection, qui fournit des instructions sur la façon d'appliquer cette forme de sécurité renforcée à de nombreux sites Web et produits logiciels courants que vous pouvez utiliser. Si l'un de vos comptes n'est pas répertorié sur ce site de ressources, examinez les paramètres de votre compte ou votre profil utilisateur et vérifiez si MFA est une option disponible. Si vous le voyez là-bas, envisagez de le mettre en œuvre tout de suite ! Les noms d'utilisateur et les mots de passe ne suffisent plus à protéger les comptes contenant des informations sensibles. En utilisant l'authentification multifacteur, vous pouvez protéger ces comptes et réduire le risque de fraude en ligne et d'usurpation d'identité. Pensez également à activer cette fonctionnalité sur vos comptes de réseaux sociaux !

CONTACTEZ L'EQUIPE DU MOIS DE SENSIBILISATION A LA CYBERSECURITE DE CISA

Merci pour votre soutien et votre engagement continus envers le Mois de la sensibilisation à la cybersécurité et pour aider tous les Américains à rester en sécurité en ligne. Veuillez envoyer un courriel à notre équipe au CyberAwareness@cisa.dhs.gov ou consultez le www.cisa.gov/cybersecurity-awareness-month ou staysafeonline.org/cybersecurity-awareness-month/ pour en savoir plus.