RENFORCER LA SÉCURITÉ NUMÉRIQUE

AVEC L'AUTHENTIFICATION MULTIFACTORIELLE

QU'EST-CE QUE L'AUTHENTIFICATION MULTIFACTORIELLE ?

L'authentification multifactorielle (MFA) est une méthode de sécurité qui oblige les utilisateurs à fournir au moins deux facteurs de vérification pour accéder à une ressource telle qu'une application, un compte en ligne ou un VPN. Avec le nombre croissant de cybermenaces et de violations de données, il est impératif de mettre en place des méthodes d'authentification fortes pour protéger les comptes en ligne et les informations sensibles.

La MFA combine souvent quelque chose que vous connaissez (un mot de passe), quelque chose que vous avez (un jeton de sécurité) et votre ressemblance (biométrie) pour renforcer la sécurité. Cela ajoute une couche de protection supplémentaire en plus d'un simple mot de passe.

TYPES D'AUTHENTIFICATION MULTIFACTORIELLE

1. AUTHENTIFICATION PAR SMS

Son fonctionnement : Un code d'accès à usage unique (OTP) est envoyé sur votre téléphone portable par SMS. Vous saisissez ce code dans le système pour y accéder.

Avantages : Facile à utiliser, pas de matériel spécialisé requis.

Inconvénients : Peut être intercepté par des pirates informatiques, dépend de la disponibilité du réseau mobile.

2. AUTHENTIFICATION PAR E-MAIL

Son fonctionnement : Un OTP ou un lien de vérification est envoyé à l'adresse e-mail que vous avez enregistrée.

Avantages : Pratique, pas besoin d'appareils supplémentaires.

Inconvénients : Sensible aux attaques de phishing, peut être retardée si les serveurs de messagerie sont lents.

3. APPLICATIONS D'AUTHENTIFICATION

Leur fonctionnement : Les applications logicielles génèrent des OTP temporels que vous saisissez après votre mot de passe.

Avantages : Plus sûres que les SMS, fonctionnent sans connexion Internet.

Inconvénients : Nécessitent un smartphone, peuvent être peu pratiques en cas de perte de l'appareil.

4. AUTHENTIFICATION BIOMÉTRIQUE

Son fonctionnement : Utilise des empreintes digitales, la reconnaissance faciale ou la lecture de la rétine pour vérifier l'identité.

Avantages : Hautement sécurisée, rapide et pratique.

Inconvénients : Nécessite du matériel spécialisé, peut susciter des préoccupations en matière de protection de la vie privée.

5. JETONS MATÉRIELS

Leur fonctionnement : Les appareils physiques génèrent des OTP ou utilisent des balises USB/NFC pour l'authentification.

Avantages : Extrêmement sécurisés, immunisés contre le phishing.

Inconvénients : Coûteux, peuvent être perdus ou volés.

POURQUOI UTILISER L'AUTHENTIFICATION MULTIFACTORIELLE ?

- **Sécurité renforcée :** La mise en œuvre de la MFA fournit une couche de sécurité supplémentaire en plus des simples mots de passe.
- **Protège les données sensibles :** Il est impératif de protéger les informations personnelles et commerciales.
- **Conformité :** Facilite la conformité aux exigences de l'entreprise et réglementaires en matière de protection des données.
- **Réduisent la fraude :** Minimisent le risque d'accès non autorisé et de fraude.

La MFA est un outil simple mais puissant qui renforce considérablement votre sécurité en ligne. En tirant parti d'un ou de plusieurs des différents types de MFA, vous pouvez vous protéger, vous et votre organisation, contre les accès non autorisés et les cybermenaces potentielles.

PHISHME COFENSE
SÉCURITÉ DES E-MAILS

COMMENT REPÉRER UNE TENTATIVE DE PHISHING ?

La capacité à identifier un e-mail de phishing est essentielle pour protéger les informations sensibles contre les cybercriminels. Étant donné que les e-mails de phishing visent à inciter les destinataires à divulguer des informations sensibles telles que des mots de passe, des détails de carte de crédit et d'autres données personnelles, ils présentent de graves dangers.

Les acteurs de la menace se déguisent souvent en entités de confiance, ce qui rend ces scams difficiles à détecter. Être victime d'une attaque de phishing peut entraîner de graves conséquences, notamment le vol d'identité, la perte financière et l'accès non autorisé à des comptes personnels et d'entreprise.

La capacité à reconnaître et à signaler efficacement les e-mails de phishing est essentielle pour vous protéger, vous et votre organisation, contre une cyberattaque. Les indicateurs clés d'un e-mail de phishing incluent les suivants :

1. ADRESSE DE L'EXPÉDITEUR SUSPECTE :

Souvent, les e-mails de phishing proviennent d'une adresse qui semble légitime, mais qui contient de légères fautes d'orthographe ou des caractères supplémentaires.

2. SALUTATIONS INHABITUELLES OU GÉNÉRIQUES :

Les e-mails de phishing utilisent généralement des salutations génériques comme « Cher client » au lieu de s'adresser à vous par votre nom.

3. LANGAGE URGENT OU MENAÇANT :

Les cybercriminels essaient souvent de créer un sentiment d'urgence, en suggérant que votre compte sera fermé ou que vous devez agir immédiatement pour résoudre un problème.

4. PIÈCES JOINTES OU LIENS INHABITUELS

Les e-mails de phishing peuvent contenir des pièces jointes ou des liens inattendus. Pour confirmer la légitimité d'un lien, passez la souris sur celui-ci avant de cliquer.

5. DEMANDE D'INFORMATIONS PERSONNELLES :

Les organisations légitimes ne vous demanderont jamais de fournir des informations sensibles telles que des mots de passe, des détails de carte de crédit ou des numéros de sécurité sociale par e-mail. Si l'expéditeur vous demande de divulguer ce type d'informations par e-mail, il s'agit probablement d'une tentative de phishing.

6. FAUTES D'ORTHOGRAPHE ET DE GRAMMAIRE :

De nombreux e-mails de phishing contiennent des fautes d'orthographe et des erreurs de grammaire grossières, qui sont rares dans les communications professionnelles.

7. URL INCOHÉRENTES :

Un e-mail de phishing peut inclure des URL qui ne correspondent pas au texte auquel elles sont liées, ou elles peuvent vous diriger vers un site Web différent de celui mentionné.

La sensibilisation à ces indicateurs peut vous aider à éviter d'être victime de scams par phishing. Dès lors que vous saurez comment repérer une tentative de phishing, vous pourrez en détecter plus d'une !

PHISHME COFENSE
EMAIL SECURITY

COMMENT LES PIRATES INFORMATIQUES ESSAIENT DE VOUS TROMPER ?

Alors que les cyberattaques sont de plus en plus sophistiquées, les employés doivent être vigilants et conscients de la multitude de façons dont les pirates informatiques peuvent accéder à des informations sensibles. Des stratagèmes de phishing aux deepfakes, les cybercriminels ne cessent de faire évoluer leurs méthodes.

VOICI QUELQUES-UNES DES FAÇONS DONT VOUS POURRIEZ ÊTRE EXPOS LA CYBERCRIMINALIT :

SCAN D'UN CODE QR

Les codes QR sont partout, des restaurants aux publicités et même aux cartes de visite. Bien qu'ils soient très pratiques, ils présentent également un risque important. Les cybercriminels utilisent des codes QR malveillants qui renvoient directement à des sites Web de phishing pour voler vos informations personnelles ou infecter votre appareil avec des logiciels malveillants.

Trois façons de se protéger :

- Vérifiez la source du code QR.
- Évitez de scanner les codes QR de sources inconnues ou suspectes.
- Utilisez des scanners de codes QR qui peuvent vérifier les URL avant de les ouvrir.

PAR SMS

Les pirates informatiques envoient des SMS trompeurs pour inciter les gens à partager des données privées ou à cliquer sur un lien malveillant. Ces messages semblent souvent provenir d'une source fiable, comme une banque ou un organisme gouvernemental.

Trois façons de se protéger :

- Méfiez-vous des SMS non sollicités, en particulier ceux qui demandent des informations personnelles.
- Ne cliquez pas sur les liens et ne téléchargez pas de pièces jointes d'expéditeurs inconnus.
- Vérifiez la légitimité du texte en contactant directement l'organisation.

PAR TÉLÉPHONE

Les escrocs appellent souvent des personnes et se font passer pour des entités légitimes pour leur soutirer des informations sensibles. Ces appelants utilisent souvent un langage manipulateur pour créer un sentiment d'urgence ou de peur.

Trois façons de se protéger :

- Ne fournissez pas d'informations personnelles par téléphone à moins d'être certain de l'identité de l'appelant.
- Vérifiez les informations d'identification de l'appelant en contactant directement l'organisation.
- Méfiez-vous des appels non sollicités demandant des informations sensibles.

PAR-DESSUS VOTRE ÉPAULE

Les attaquants regardent par-dessus votre épaule pour observer votre écran ou votre clavier afin de voler des informations sensibles, telles que des mots de passe et des codes PIN. Cette tactique, appelée « espionnage par-dessus l'épaule », peut se produire dans des lieux publics comme les cafés, les aéroports ou même dans votre bureau.

Trois façons de se protéger :

- Regardez bien autour de vous lorsque vous saisissez informations sensibles.
- Utilisez des écrans de confidentialité sur vos appareils et verrouillez-les toujours lorsque vous les laissez sans surveillance.
- Protégez votre clavier lorsque vous saisissez des mots de passe ou des codes PIN.

EN SE FAISANT PASSER POUR QUELQU'UN EN QUI VOUS AVEZ CONFIANCE

Les deepfakes utilisent l'intelligence artificielle pour créer des vidéos ou des enregistrements audio hyperréalistes, mais faux. Les cybercriminels peuvent utiliser des deepfakes pour se faire passer pour des dirigeants d'entreprise ou d'autres personnes de confiance, ce qui entraîne d'importantes failles de sécurité.

Trois façons de se protéger :

- Soyez prudent face aux demandes inattendues ou inhabituelles, même si elles semblent provenir de personnes connues.
- Vérifiez l'identité de la personne qui fait la demande via plusieurs canaux.
- Restez au fait des derniers développements en matière de technologie de deepfake.

PHISHME
COFENSE
EMAIL SECURITY

COMMENT RESTER PROTÉGÉ ?

LORS DE L'UTILISATION DE CHATBOTS D'IA

Les chatbots d'intelligence artificielle (IA) sont pratiques, mais ils peuvent également présenter des risques pour la sécurité. Avec l'utilisation croissante des chatbots d'IA tels que ChatGPT, voici ce que vous devez faire pour protéger la confidentialité de vos données et éviter une violation.

1. COMPRENDRE LES RISQUES

- ***Attaques de phishing :*** Les bots malveillants se font passer pour des services légitimes dans le but de voler vos informations.
- ***Distribution de logiciels malveillants :*** Les bots d'IA peuvent être utilisés pour diffuser des logiciels nuisibles.
- ***Confidentialité des données :*** Les informations sensibles partagées avec des bots peuvent être interceptées ou utilisées à mauvais escient.

2. UTILISER DES SERVICES DE CONFIANCE

- ***Vérifiez la légitimité :*** N'utilisez que des chatbots d'entreprises réputées.
- ***Recherchez les sceaux de sécurité :*** Assurez-vous que le service dispose des certifications de sécurité appropriées.

3. SÉCURISER VOS INFORMATIONS PERSONNELLES

- ***Évitez de partager des données sensibles :*** Ne divulguez jamais d'informations personnelles, financières ou de connexion à des chatbots d'IA.
- ***Utilisez des mots de passe forts :*** Assurez-vous que vos mots de passe sont complexes et uniques.

4. METTRE À JOUR RÉGULIÈREMENT

- ***Maintenez le logiciel à jour :*** Assurez-vous que votre antivirus et autres logiciels de sécurité sont à jour.
- ***Vérifiez les mises à jour des bots :*** Utilisez des chatbots qui mettent régulièrement à jour leurs protocoles de sécurité.

5. SURVEILLER L'ACTIVITÉ

- ***Vérifiez régulièrement les relevés :*** Surveillez les relevés bancaires et de carte de crédit pour détecter les transactions non autorisées.
- ***Restez informé :*** Restez au faut des dernières nouveautés en matière de cybersécurité pour être au courant des nouvelles menaces.

6. SIGNALER LES ACTIVITÉS SUSPECTES

- ***Contactez l'assistance :*** Si vous suspectez un bot d'être malveillant, signalez-le immédiatement au fournisseur de services.
- ***Alertez les autorités :*** Informez les autorités locales ou nationales de cybersécurité de toute faille de sécurité.

PHISHME COFENSE
EMAIL SECURITY