NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

Les précautions contre les attaques des cybercriminels…



Correspondance de Californie : Les cybercriminels exploitent la pandémie de COVID-19 pour perpétrer des fraudes

Alors que de plus en plus de personnes travaillent à domicile, les cybercriminels exploitent la pandémie de COVID-19 pour cibler les organisations et les individus avec des escroqueries sophistiquées. Le FBI a récemment annoncé une augmentation des stratagèmes de fraude1 liés à la pandémie de COVID-19.2 Les organisations peuvent se retrouver plus vulnérables en raison de leur main-d'œuvre éloignée et de leur personnel limité. Il est important de rester vigilant pour vous protéger contre les risques de fraude accrus résultant des impacts du virus.

Le phishing et les attaques de logiciels malveillants sont en augmentation. Les chercheurs du Barracuda Network ont signalé une augmentation de 667% des attaques de phishing liées à COVID-19 depuisa fin février.2 et les détails du compte bancaire. À l'aide de logiciels malveillants, les fraudeurs peuvent rapidement accéder à votre ordinateur pour surveiller et enregistrer vos frappes ou injecter des ransomwares. Les cybercriminels utilisent des informations dans l'actualité sur COVID-19 pour concevoir leurs attaques, par exemple en ciblant les travailleurs à distance avec des e-mails les informant d'un test COVID-19 positif au sein de leur organisation.

Les ransomwares deviennent de plus en plus populaires car les cybercriminels recherchent des paiements de rançon plus importants sachant que de nombreuses

entreprises sont vulnérables lorsqu'elles opèrent en ces temps difficiles. Dans une attaque de ransomware, les fraudeurs tiennent votre ordinateur ou votre réseau en otage, bloquant l'accès à vos données et fichiers importants jusqu'à ce que vous payiez une grosse somme d'argent. Tous les secteurs sont exposés à un risque accru de ransomware, mais les soins de santé et les agences gouvernementales peuvent être plus à risque car les cybercriminels savent à quel point ces services sont critiques en ce moment.

La fraude par imposteur, également connue sous le nom de compromis sur le courrier électronique d'entreprise (BEC), constitue une menace importante pour votre entreprise. BEC est l'endroit où un fraudeur usurpe l'identité d'un fournisseur, d'un dirigeant d'entreprise ou d'un autre partenaire commercial de confiance – vous incitant finalement à effectuer le paiement. Les organisations qui ne sont pas en mesure de se conformer systématiquement aux contrôles et procédures d'exploitation standard en raison de pénuries de personnel et d'une main-d'œuvre de plus en plus éloignée peuvent être particulièrement vulnérables à BEC. Les employés doivent être à l'affût des escroqueries de fournitures médicales et des sites de dons frauduleux qui peuvent usurper l'identité d'une entreprise, d'un organisme de bienfaisance ou d'un organisme gouvernemental pour les convaincre de faire des achats ou des dons sur des sites Web usurpés ou de faire affaire avec un vendeur bidon.

Enfin, la prise de contrôle de compte est une autre menace de fraude grave qui est en augmentation en raison de l'augmentation récente des attaques de phishing et de la distribution de logiciels malveillants. Avec la prise de contrôle de compte, les voleurs ont accès à des transactions non autorisées, y compris le transfert de fonds, la création et l'ajout de faux employés à la paie et le vol d'informations sensibles sur les clients. Les organisations particulièrement à risque sont celles qui ne disposent peut-être pas d'un solide programme de travail à domicile et de contrôles de sécurité bien établis.

Prenez les précautions suivantes pour protéger les actifs de votre organisation

Méfiez-vous de l'augmentation des attaques de phishing.Il est particulièrement important pendant ces périodes d'éviter de cliquer sur des liens ou d'ouvrir des pièces jointes d'expéditeurs suspects ou inconnus, et d'être prudent lorsque vous visitez des sites Web non fiables, qui peuvent être contaminés par des logiciels malveillants. Gardez votre logiciel antivirus et anti-spyware et vos pare-feu mis à

jour régulièrement. Si possible, utilisez des appareils séparés pour vos activités professionnelles et personnelles afin de limiter votre exposition aux attaques de phishing.

Renforcez et suivez vos contrôles internes pour les paiements.

Au fur et à mesure que votre entreprise passe à une main-d'œuvre distante, les moyens d'atténuer les vulnérabilités incluent: l'utilisation de la double garde pour tous les paiements en ligne (ACH, virement bancaire, change) et les services d'administration, rapprochant les comptes quotidiennement pour détecter les activités suspectes et verrouillant le stock de chèques et les tampons de signature dans un endroit sécurisé.

Vérifiez vos informations de paiement

Vérifiez toujours les demandes de paiement et les modifications des instructions de paiement. Assurez-vous que les demandes de modification des détails de paiement, telles que les informations de compte ou de facture, sont authentiques. Vérifiez la demande en utilisant une méthode de contact différente. Par exemple, si le fournisseur vous contacte par e-mail, confirmez les informations par téléphone. Assurez-vous d'utiliser les informations que vous avez pour le contact dans le dossier, pas les informations de contact contenues dans la demande que vous avez reçue. Assurez-vous que vos employés ont accès aux numéros de téléphone des fournisseurs de confiance enregistrés, en particulier lorsqu'ils travaillent à distance, pour faciliter les rappels afin de confirmer les paiements. Soyez extrêmement prudent afin de repérer les escroqueries de fournitures médicales et les sites de dons frauduleux – faites vos recherches pour vous assurer que vous travaillez avec un fournisseur ou une organisation légitime.

Protégez l'accès à vos informations d'identification et méfiez-vous des invites de jeton inattendues.

Ne donnez jamais de mots de passe, d'ID, de codes de jeton ou d'autres informations d'identification d'autorisation. Faites attention aux invites de jeton inattendues. Ignorez les fenêtres contextuelles (pop-up) qui recherchent vos informations d'identification de connexion aux services bancaires en ligne. Méfiez-vous des appels non sollicités, y compris de votre banque, pour vous aider à résoudre les problèmes de connexion que vous n'avez pas signalés.

Ne vous connectez pas à votre compte à partir d'un lien dans un message suspect

Accédez toujours aux sites Web en utilisant un moteur de recherche réputé ou en saisissant l'URL complète dans votre navigateur. N'utilisez pas les mêmes mots de passe sur plusieurs sites Web.

Améliorez votre programme de sécurité d'accès à distance

Les travailleurs à distance peuvent présenter des risques de cybersécurité plus importants en raison des paramètres de sécurité Internet à la maison. Les employés peuvent exposer les appareils de l'entreprise à des risques supplémentaires lorsqu'ils quittent la sûreté et la sécurité du lieu de travail. Collaborez avec votre équipe informatique pour réévaluer votre programme de travail à domicile et collaborez avec les employés pour garantir la sécurité de leurs connexions Internet à domicile.

Les attaques frauduleuses sont inévitables pour la plupart des entreprises, et les cybercriminels exploitent la pandémie COVID-19 pour perpétuer encore plus d'escroqueries.

Assurez-vous d'éduquer vos employés et partenaires sur les risques de fraude accrus résultant de COVID-19 et sur la façon de rester vigilant contre les attaques frauduleuses.

Le FBI voit une augmentation des fraudes liées à la pandémie de coronavirus (COVID-19)

source : FBi

De notre correspondante au Royaume Uni : Liliy Sagherian