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

HAMEÇONNAGE ET USURPATION D'IDENTITÉ

Les attaques de phishing utilisent des emails ou des sites Web malveillants pour infecter votre ordinateur avec des logiciels malveillants et des virus afin de collecter des informations personnelles et financières. Les cybercriminels tentent d'inciter les utilisateurs à cliquer sur un lien ou à ouvrir une pièce jointe qui infecte leurs ordinateurs, créant des vulnérabilités que les criminels peuvent utiliser pour attaquer. Les e-mails d'hameçonnage peuvent sembler provenir d'une véritable institution financière, d'un site de commerce électronique, d'une agence gouvernementale ou de tout autre service, entreprise ou particulier. L'email peut également demander des informations personnelles telles que des numéros de compte, des mots de passe ou des numéros de sécurité sociale. Lorsque les utilisateurs répondent avec les informations ou cliquent sur un lien, les attaquants l'utilisent pour accéder aux comptes des utilisateurs.

Les attaques d'usurpation d'identité utilisent des adresses e-mail, des noms d'expéditeurs, des numéros de téléphone ou des URL de sites Web déguisés en source de confiance. Les cybercriminels tentent de tromper les utilisateurs en modifiant une lettre, un symbole ou un chiffre dans le nom. Cette tactique est utilisée pour convaincre les utilisateurs qu'ils interagissent avec une source familière. Les cybercriminels veulent vous faire croire que ces communications falsifiées sont réelles pour vous amener à télécharger des logiciels malveillants, à envoyer de l'argent ou à divulguer des informations personnelles, financières ou d'autres informations sensibles.

COMMENT LES CRIMINELS VOUS ATTIRENT

Les messages suivants de la OnGuardOnline de la Commission fédérale du commerce ont des exemples de ce que les attaquants peuvent envoyer par e-mail ou SMS lors de l'hameçonnage d'informations sensibles :

- « Nous soupçonnons une transaction non autorisée sur votre compte. Pour vous assurer que votre compte n'est pas compromis, veuillez cliquer sur le lien ci-dessous et confirmer votre identité. »
- « Lors de notre vérification régulière des comptes, nous n'avons pas pu vérifier vos informations. Veuillez cliquer ici pour mettre à jour et vérifier vos informations. »
- « Nos dossiers indiquent que votre compte a été surfacturé. Vous devez nous appeler dans les 7 jours pour recevoir votre remboursement. »

Pour voir des exemples d'e-mails d'hameçonnage réels et les étapes à suivre si vous pensez avoir reçu un e-mail d'hameçonnage, veuillez visiter StopRansomware.gov.

CONSEILS SIMPLES

- **Jouez dur pour avoir des inconnus.** Les liens dans les emails et les publications en ligne sont souvent la façon dont les cybercriminels compromettent votre ordinateur. Si vous n'êtes pas sûr de l'expéditeur d'un e-mail, même si les détails semblent exacts, ne répondez pas et ne cliquez sur aucun lien ou pièce jointe trouvé dans cet e-mail. Méfiez-vous des salutations génériques telles que "Bonjour client de la banque", car elles sont souvent des

signes de tentatives de d'hameçonnage. Si vous êtes préoccupé par la légitimité d'un email, appelez directement l'entreprise.

- **Pense avant d'agir.** Méfiez-vous des communications qui vous implorent d'agir immédiatement. De nombreux emails d'hameçonnage tentent de créer un sentiment d'urgence, faisant craindre au destinataire que son compte ou ses informations soient en danger. Si vous recevez un email suspect qui semble provenir d'une personne que vous connaissez, contactez cette personne directement sur une plate-forme sécurisée distincte. Si l'e-mail provient d'une organisation mais semble toujours « hameçonneur », contactez-la via le service client pour vérifier la communication.
- **Protégez vos informations personnelles.** Si les personnes qui vous contactent ont des informations clés sur votre vie (votre fonction, plusieurs adresses e-mail, votre nom complet et bien plus que vous avez peut-être publiés en ligne quelque part), elles peuvent tenter une attaque de phishing directe contre vous. Les cybercriminels peuvent également utiliser l'ingénierie sociale avec ces détails pour essayer de vous manipuler afin de sauter les protocoles de sécurité normaux.
- **Méfiez-vous des hyperliens.** Évitez de cliquer sur les hyperliens dans les e-mails et survolez les liens pour vérifier l'authenticité. Assurez-vous également que les URL commencent par "https". Le "s" indique que le chiffrement est activé pour protéger les informations des utilisateurs.
- **Doublez votre protection de connexion.** Activez l'authentification multifactorielle (MFA) pour vous assurer que la seule personne ayant accès à votre compte est vous-même. Utilisez-le pour les emails, les opérations bancaires, les réseaux sociaux et tout autre service nécessitant une connexion. Si MFA est une option, activez-la à l'aide d'un appareil mobile de confiance, tel que votre smartphone, une application d'authentification ou un jeton sécurisé, un petit dispositif physique qui peut s'accrocher à votre trousseau de clés. Lisez le guide pratique de l'authentification multifacteur (MFA) pour plus d'informations.
- **Secouez votre protocole de mot de passe.** Selon les directives du Institut national des normes et de la technologie, vous devriez envisager d'utiliser le mot de passe ou la phrase secrète le plus long autorisé. Faites preuve de créativité et personnalisez votre mot de passe standard pour différents sites, ce qui peut empêcher les cybercriminels d'accéder à ces comptes et vous protéger en cas de violation. Utilisez des gestionnaires de mots de passe pour générer et mémoriser des mots de passe différents et complexes pour chacun de vos comptes. Lisez le Création d'une feuille de conseils sur le mot de passe pour plus d'information.
- **Installer et mettre à jour un logiciel antivirus.** Assurez-vous que tous vos ordinateurs, appareils Internet des objets, téléphones et tablettes sont équipés de logiciels antivirus, de pare-feu, de filtres de messagerie et de logiciels anti-espion régulièrement mis à jour.

COMMENT SIGNALER

Pour signaler des tentatives d'hameçonnage, d'usurpation d'identité ou signaler que vous avez été victime, consultez le www.ic3.gov pour déposer une plainte. Pour plus d'informations sur les moyens de protéger vos informations, visitez la page suivante StopRansomware.gov.

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

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 à CyberAwareness@cisa.dhs.gov ou consultez le www.cisa.gov/cybersecurity-awareness-month ou même le staysafeonline.org/cybersecurity-awareness-month/ pour en savoir plus.