Ne mordez pas à l'hameçon : reconnaître et prévenir les attaques par hameçonnage

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Août 2022 | ITSAP.00.101

L'hameçonnage est une attaque dans le cadre de laquelle un fraudeur vous appelle, vous envoie un texto ou un courriel, ou utilise les médias sociaux pour vous inciter à cliquer sur un lien malveillant, à télécharger un logiciel ou à divulguer de l'information sensible. Les tentatives d'hameçonnage prennent souvent la forme d'un envoi massif de messages généraux en apparence légitimes et en provenance d'une source de confiance comme une institution financière ou un fournisseur de services de messagerie .

Harponnage: Attaque personnalisée qui vous cible directement. Le message peut contenir des détails vous concernant, comme vos champs d'intérêt, vos récentes activités en ligne ou de récents achats.

Chasse à la baleine (*Whaling*): Attaque personnalisée qui vise les cadres supérieurs. Un fraudeur choisit ces cibles pour tirer avantage de leur niveau d'autorité et d'un possible accès à l'information la plus sensible.

Hameçonnage par message texte: Attaque par hameçonnage menée au moyen de messages texte (textos). Un fraudeur peut se faire passer pour quelqu'un que vous connaissez ou le représentant d'un service que vous utilisez, comme un fournisseur de services Internet ou cellulaires, afin de vous demander ou de vous offrir une mise à jour ou un paiement.

Hameçonnage par code QR (*Quishing*): Attaque par hameçonnage ayant recours à des codes QR *(Quick Response)* qu'un fraudeur envoie généralement par courriel. La victime lit le code QR, ce qui la redirige vers un site Web malveillant. L'hameçonnage par code QR peut contourner le mécanisme de sécurité mis en place pour analyser les pièces jointes et les liens malveillants.

Hameçonnage vocal (*Vishing*): Fraudes et arnaques par téléphone qui visent à inciter les gens à divulguer des renseignements sensibles. Un fraudeur peut utiliser un système de voix sur protocole IP *(VoIP pour Voice Over Internet Protocol)* pour changer l'identification de l'appelant afin de vous faire croire qu'il s'agit d'un appel légitime.

Les fraudeurs tentent d'obtenir :

Vos Mots de Passe

À Quoi Ressemble une Attaque par Hameçonnage?

Étape 1: L'appât

Le fraudeur personnalise le message de manière à ce qu'il semble provenir d'une institution financière ou d'un service bancaire légitime. Des techniques de mystification sont employées, puis le message est envoyé à plusieurs destinataires dans l'espoir que certains d'entre eux mordent à l'appât et tombent dans le piège.

Dans le cas d'une attaque par hameçonnage ou d'une chasse à la baleine, le fraudeur collecte d'abord les détails sur la personne ou l'entreprise visée. Il pourrait, par exemple, recueillir l'information tirée des profils de médias sociaux, des sites Web de l'entreprise et de l'activité en ligne pour créer un message personnalisé.

En ce qui concerne les attaques par hameçonnage vocal, le fraudeur pourrait utiliser un composeur automatique pour acheminer le message frauduleux à plusieurs victimes.

Étape 2: L'hameçon

La victime croit que le message a été envoyé par une source fiable et qu'il contient de l'information qui nécessite une prise de mesures immédiate, comme régler un problème avec son compte.

Si la victime clique sur le lien dans le message, elle sera redirigée à son insu vers la fausse version d'un site Web réel, qui a été créée par le fraudeur. La victime fournit de l'information sensible, comme ses justificatifs d'ouverture de session, et celle-ci est ensuite transmise au fraudeur. Si la victime ouvre une pièce jointe infectée, du code malveillant peut s'exécuter et infecter son dispositif.

Dans le cas d'une attaque par hameçonnage vocal, si la victime répond et appuie sur la touche correspondant à l'une des options suggérées, elle entre directement en communication avec le fraudeur.

Étape 3: L'attaque

Vol des justificatifs d'identité – Le fraudeur peut maintenant accéder au compte de la victime et, par exemple, envoyer d'autres courriels d'hameçonnage aux contacts de cette dernière. Si la victime est un professionnel des TI avec des accès privilégiés, le fraudeur peut avoir accès aux données sensibles ou aux systèmes essentiels de l'organisation.

Installation du maliciel – Le fraudeur peut utiliser le maliciel pour obtenir le contrôle du dispositif de la victime, voler ses données ou verrouiller l'accès à ses fichiers jusqu'à ce qu'une rançon soit versée (comme c'est le cas lors d'une attaque par rançongiciel). Les rançongiciels sont devenus l'un des cybercrimes les plus courants au fil des 15 dernières années.

Dans la société numérique d'aujourd'hui, les attaques par hameçonnage sont si fréquentes que personne n'y est immunisé. L'hameçonnage est la technique que les cybercriminels utilisent le plus souvent pour s'infiltrer dans vos réseaux afin d'installer des maliciels ou des rançongiciels, ou de voler vos données.

Les fraudeurs tirent avantage des périodes de crise, des conflits ou d'événements mondiaux, comme une pandémie ou un désordre civil, pour lancer des attaques par hameçonnage contre des institutions financières, des entités gouvernementales et des secteurs des infrastructures essentielles. Les partis politiques, les politiciens et les citoyens sont souvent la cible d'activités d'hameçonnage dans les mois précédant une élection.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Ne mordez pas à l'hameçon : reconnaître et prévenir les attaques par hameçonnage

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Août 2022 | ITSAP.00.101

Protégez votre information et votre infrastructure:

- Avant de cliquer sur les liens, assurez-vous qu'ils sont légitimes. Passez sur le lien pour voir si l'expéditeur et le site Web correspondent bien à l'information attendue
- Évitez d'envoyer de l'information sensible par courriel ou par texto
- Sauvegardez l'information de manière à toujours en avoir une copie
- Appliquez les mises à jour logicielles et les correctifs
- Filtrez les pourriels (courriels indésirables envoyés en bloc)
- Bloquez les addresses IP, les noms de domaines et les types de fichiers que l'on sait malveillants
- Appelez l'expéditeur pour vérifier sa légitimité (par exemple, si vous recevez un appel d'un conseiller de votre institution financière, raccrochez et rappelez-le)
- Utilisez un logiciel anti-hameçonnage conforme au protocole DMARC (*Domain-based Message Authentication, Reporting and Conformance)*
- Limitez la quantité d'information personnelle que vous divulguez en ligne (par exemple, les numéros de téléphone et de postes des employés)
- Mettez en place des protocoles et des procédures que vos employés pourront adopter pour vérifier les communications suspectes à l'interne. Ces procédures devraient fournir au personnel un moyen facile de signaler les attaques par hameçonnage
- Mettez à jour le plan d'intervention en cas d'incident de votre organisation de manière à ce qu'il fasse mention de la façon d'intervenir si vous faites l'objet d'une attaque par hameçonnage
- Faites appel à l'authentification multifacteur

36% **NOMBRE DE VIOLATIONS DE DONNÉES EN 2021 DÉCOULANT D'ATTAQUES PAR HAMEÇONNAGE***

*Data Breach Investigations Report 2021 de Verizon

Pour obtenir des conseils et des ressources, vous pouvez consulter les publications suivantes sur notre site Web:

- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Protéger l'organisme contre les maliciels (ITSAP.00.057)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Reconnaître les courriels malveillants (ITSAP.00.100)
- Directive de mise en œuvre – protection du domaine de courrier (ITSP.40.065 v1.1)
- Facteurs relatifs à la sécurité à considérer pour les codes QR (ITSAP.00.141)

Faites preuve de vigilance lors de communications non sollicitées:

- pièces jointes
- liens masqués
- sites web frauduleux
- codes QR malveillants
- pages d'ouverture de session
- demandes urgentes
- invites demandant la saisie d'information personnelle
- Interlocuteur qui prétend être un représentant du gouvernement ou d'une institution financière

La formation et la sensibilisation peuvent faire toute la différence:

Les utilisateurs de votre organisation devraient savoir à quel point il est important de protéger leur information personnelle et celle de l'organisation. Ceux qui ne savent pas reconnaître les signes précurseurs d'une attaque par piratage psychologique pourraient divulguer de l'information ou infecter involontairement les dispositifs du réseau. Miser sur la sensibilisation et la formation des employés sur les questions de respect de la vie privée (traitement de l'information personnelle) et de cybersécurité permet de réduire le risque d'une attaque par hameçonnage fructueuse. Procéder à des simulations d'hameçonnage internes aidera également vos employés à mieux comprendre comment détecter et prévenir les attaques par hameçonnage dans un environnement sécurisé.

Il pourrait y avoir **anguille sous roche** si:

- vous ne reconnaissez pas le nom, l'adresse courriel ou le numéro de téléphone de l'expéditeur (ce qui est fréquent dans le cas de l'hameçonnage)
- vous remarquez plusieurs fautes d'orthographe et de grammaire
- l'expéditeur vous demande de fournir de l'information personnelle ou confidentielle, ou d'ouvrir une session par l'entremise du lien fourni
- la demande de l'expéditeur est urgente et vous devez respecter une échéance
- l'offre semble trop belle pour être vraie
- l'interlocuteur parle d'un ton robotique ou son débit est inhabituel
- l'appel est de piètre qualité

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada