Centre de la sécurité des télécommunications
Communications Security Establishment

NON CLASSIFIÉ

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Reconnaître les Courriels Malveillants

Avril 2022

ITSAP.00.100 V.3

Des auteurs de menace en quête d'information s'en prennent fréquemment à des organisations et à leurs réseaux. Ils sont doués en technologies, connaissent les vulnérabilités et sont vigoureusement agiles; s'ils s'introduisent dans un système, ils peuvent accéder rapidement aux données et aux renseignements personnels qu'ils contiennent. Si vous avez accès aux renseignements sensibles de l'organisation pour laquelle vous travaillez, méfiez-vous des courriels malveillants qui sont envoyés par les auteurs de menace pour infecter des dispositifs et des systèmes et accéder à l'information qu'ils contiennent. En vous familiarisant avec les courriels malveillants et les attaques par hameçonnage, vous pourrez aider à protéger l'information de votre organisation.

Attaques par hameçonnage

L'hameçonnage est l'envoi de communications qui semblent légitimes, mais qui sont frauduleuses. Les courriels d'hameçonnage contiennent souvent des pièces jointes malveillantes ou des liens qui mènent vers des sites Web malveillants. Les auteurs de menace ont recours à l'hameçonnage pour vous inciter, par la ruse, à dévoiler de l'information sensible, comme des numéros de cartes de crédit, des numéros d'assurance sociale ou des justificatifs d'identité bancaires.

Les attaques par hameçonnage peuvent être menées par courriel, par texto ou par appel téléphonique, mais le présent document se penche sur les courriels malveillants.

Les courriels d'hameçonnage sont parfois génériques, mais les auteurs de menace peuvent prendre le temps de confectionner des courriels plus convaincants ou ayant l'air plus légitimes :

- **Harponnage** : Un auteur de menace envoie un courriel à des cibles précises, comme une personne, un groupe ou une entreprise. Le courriel de harponnage est conçu en fonction des caractéristiques et des intérêts professionnels ou personnels du destinataire. L'auteur de menace s'inspire souvent de l'information publique qui se trouve dans les comptes de médias sociaux de la cible. Le courriel de harponnage demande plus de travail, mais son destinataire est plus susceptible d'y répondre, d'ouvrir ses pièces jointes ou de cliquer sur les liens qu'il contient.

- **Chasse à la baleine :** Un auteur de menace envoie des courriels à des personnes connues ou à des cadres supérieurs d'une entreprise. Il compose des courriels ciblés et convaincants qui contiennent des renseignements protégés sur les destinataires ou l'entreprise pour laquelle ils travaillent. L'auteur de menace peut s'inspirer de l'information publique qui se trouve dans le site Web de l'entreprise ou ses comptes de médias sociaux.

Une méthode d'attaque efficace

Les attaques par hameçonnage sont efficaces, car leurs auteurs sont très doués pour fabriquer des courriels qui ont l'air légitimes. Les courriels contiennent le logo de l'entreprise ciblée ou de l'information sur la marque de commerce. La ligne d'objet est opportune et le message est pertinent.

Comme nous sommes de nature confiante (et que nous recevons d'innombrables courriels chaque jour), nous pouvons facilement croire le contenu des courriels et ouvrir leurs pièces jointes ou cliquer sur les liens qu'ils contiennent. Ce qu'il faut savoir, c'est que les pièces jointes peuvent contenir un logiciel malveillant et les liens, mener à des sites Web malveillants. Même si un courriel vient d'une connaissance, pensez-y toujours à deux fois avant de cliquer sur un lien ou d'ouvrir une pièce jointe.

Personne n'est à l'abri

Tout le monde peut être visé par des courriels d'hameçonnage ou de harponnage, mais les personnes suivantes sont des cibles plus fréquentes :

- les cadres supérieurs et leurs adjoints
- le personnel des bureaux d'assistance
- les administrateurs de système
- les utilisateurs ayant accès à de l'information sensible
- les utilisateurs ayant des accès à distance
- les utilisateurs qui doivent interagir avec le public dans le cadre de leurs fonctions

Prenez garde à l'hameçonnage par code QR, une attaque consistant à insérer dans un courriel un code-barres 2D (ou code QR pour *Quick Response*) qui redirige l'utilisateur vers un site Web d'hameçonnage une fois le code QR numérisé. Vérifiez l'adresse URL du site Web pour vous assurer qu'il s'agit du site légitime.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-100-2021F-PDF
ISBN 978-0-660-38744-4

Reconnaître les courriels malveillants

Il peut être difficile de reconnaître les courriels malveillants, mais voici quelques trucs pour déterminer si les courriels sont légitimes ou faux :

- Vérifiez l'adresse de courriel de l'expéditeur et confirmez la légitimité de ses noms d'utilisateur et de domaine. Une adresse suspecte pourrait ressembler à l'adresse suivante : **"John Doe <johndoe.%nklo17er@gkmail.com>"**.
- Assurez-vous de connaître l'expéditeur et demandez-vous si le ton du courriel correspond à celui de la personne que vous connaissez.
- Cherchez des erreurs grammaticales ou des fautes de frappe dans le corps du message. Les entreprises veulent conserver leur grand professionnalisme et les courriels qu'elles envoient ne contiennent généralement pas ce genre d'erreurs et de fautes.
- Évaluez le ton du courriel et l'offre qu'il contient. Si le courriel est menaçant ou s'il contient une offre trop alléchante, il s'agit probablement d'un courriel d'hameçonnage.
- Portez attention à ce qui est demandé. La plupart des entreprises ne demanderont pas de fournir de l'information sensible ou des renseignements personnels par courriel.

Prendre les mesures adéquates avec les courriels malveillants

Soyez prudent lorsque vous recevez des courriels suspects. Avant d'ouvrir un courriel qui vous semble suspect, communiquez avec l'expéditeur par un autre moyen (p.ex. le téléphone) pour confirmer la provenance du courriel en question.

Ne cliquez sur aucune pièce jointe ni aucun lien ou code QR fourni dans les courriels. Si on vous demande, dans un courriel, de vous connecter à un compte de façon spontanée, ne cliquez pas sur le lien fourni. N'ouvrez pas les pièces jointes et évitez de numériser les codes QR. Rendez-vous plutôt sur le site Web en question en entrant l'adresse URL dans votre navigateur Web ou en cherchant le site dans un moteur de recherche.

Signalez les courriels suspects. Si vous recevez un courriel suspect ou soupçonnez des activités malveillantes sur un dispositif ou un compte professionnel, communiquez avec les équipes de TI et de sécurité de votre organisation. Suivez les directives et n'envoyez pas le courriel à vos collègues. Vous pouvez aussi signaler les courriels d'hameçonnage au Centre canadien pour la cybersécurité (**cyber.gc.ca**) ou au Centre antifraude du Canada (**antifraudcentre-centreantifraude.ca**).

Si vous recevez un message désobligeant, menaçant ou peut-être de nature criminelle, communiquez avec votre service de police local. Conservez le message, car les autorités pourraient vous en demander une copie aux fins d'enquête. **Ne faites pas suivre le message**.

Ouvrir un courriel malveillant

Si vous recevez un courriel malveillant et faites par inadvertance une manœuvre fâcheuse (p. ex. ouvrir une pièce jointe), restez calme et prenez les mesures suivantes :

- Arrêtez d'utiliser le dispositif.
- Désactivez la connexion Wi-Fi ou déconnectez les câbles de réseau pour couper la connexion à Internet.
- Éteignez votre dispositif.
- S'il s'agit d'un dispositif de travail, communiquez avec votre service de sécurité des TI. Les responsables pourront désactiver les comptes et toute autre function.
- Changez vos mots et vos phrases de passe ou vos NIP en utilisant un autre dispositif.
- Effectuez l'analyse de votre dispositif avec un antimaliciel, si possible.
- Rétablissez la connexion réseau uniquement lorsque vous croyez que votre système est nettoyé.
- Installez toutes les mises à jour et les correctifs de sécurité offerts.
- Surveillez vos comptes de près et soyez à l'affût de toute activité suspecte.

Autres publications

Pour en apprendre davantage sur les attaques par hameçonnage ou d'autres sujets liés à la cybersécurité, veuillez consulter notre site Web.

Vous y trouverez d'autres guides et ressources, dont les publications connexes suivantes:

- Êtes-vous victime de piratage? (ITSAP.00.015)
- Protéger l'organisme contre les maliciels (ITSAP.00.057)
- Ne mordez pas à l'hameçon: Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Protection d'un organisme contre les macros malveillantes (ITSAP.00.200)
- Conseils de cybersécurité pour le télétravail (ITSAP.10.116)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Directive de mise en œuvre – protection du domaine de courrier (ITSP.40.0645 v1.1)
- Facteurs relatifs à la sécurité à considérer pour les codes QR (ITASP.00.141)

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.