

Exercice sur table :

Déjouer les attaques par hameçonnage et fraude au président

Présentation

Les attaques par hameçonnage ont pour but de manipuler le personnel pour compromettre la sécurité, en jouant sur des ressorts psychologiques tels que la peur, la serviabilité ou le respect de l'autorité. Cette activité porte sur une forme particulière d'hameçonnage, ultra-ciblée, appelée « fraude au président » (également connue sous le nom de « whaling »). Lors de cette attaque, des cybercriminels usurpent l'identité de dirigeants haut placés, tels que le PDG ou le directeur financier, afin d'exploiter le biais d'autorité et de provoquer une réaction émotionnelle immédiate face à l'urgence.

Aujourd'hui, des individus malveillants s'appuient massivement sur l'intelligence artificielle (IA) générative pour créer des e-mails d'hameçonnage dépourvus de fautes de syntaxe et comportant des logos d'entreprise parfaitement identiques aux vrais. Même si les participant(e)s doivent toujours faire attention aux fautes d'orthographe évidentes ou aux incohérences liées à l'identité de l'organisation, cette session doit leur démontrer que s'appuyer sur ces seuls indices ne suffit plus pour détecter une tentative d'hameçonnage.

Rôles

Animateur :

il contrôle le rythme de l'exercice, guide les discussions et veille à la participation de toutes et tous.

Participant(e)s :

ils discutent ouvertement de leur raisonnement et réagissent aux scénarios en suivant les règles de l'exercice.

Introduction

Présentez le scénario suivant aux participant(e)s : Summit View Logistics étend ses activités en Europe. Le PDG, Marc Foret, est en déplacement en France toute la semaine afin de conclure la location d'un grand entrepôt. Chaque membre de l'organisation est au courant que cet accord constitue une priorité majeure. La directrice financière, Hélène Goujon, effectue actuellement un vol retour de dix heures vers le siège social et n'est pas joignable. C'est dans ce contexte que Thierry Chanoix, responsable des comptes fournisseurs, reçoit un courriel pour le moins suspect...

Partie 1 : Annotation des indices

 **Durée :** 15 minutes

Matériel :

- Minuteur ou chronomètre
- Copies du scénario
- Stylos ou crayons

Instructions :

- Divisez la salle en petits groupes.
- Distribuez à chaque groupe une copie imprimée de l'e-mail ainsi que des stylos ou crayons.
- Demandez aux groupes de souligner les éléments conçus pour crédibiliser le message. Par exemple : une signature d'e-mail parfaitement imitée, la mention de projets internes réels ou un ton managérial convaincant.
- Demandez ensuite aux groupes **d'entourer** les signaux d'alerte. Par exemple : une urgence extrême, une demande de stricte confidentialité ou des instructions visant à contourner les procédures de paiement habituelles.
- Accordez aux groupes 15 minutes pour lire l'e-mail, échanger en groupe et marquer les indices.

Partie 2 : Discussion

 **Durée :** 10 minutes

Questions :

- Quels sont les éléments qui crédibilisent le piège, et qu'est-ce qui a failli vous faire mordre à l'hameçon ?
- Quels signaux d'alerte précis vous ont permis de débusquer l'arnaque ?
- Comment ces ressorts psychologiques visent-ils à influencer vos émotions ou vos réactions ?

Réponses/pistes possibles :

- Détails crédibles : Les auteurs d'attaques par hameçonnage récupèrent des informations sur LinkedIn ou sur les sites officiels des entreprises, afin d'utiliser de véritables noms de projets pour rendre leurs e-mails crédibles.
- Signaux d'alerte : L'e-mail d'hameçonnage demande à l'employé de contourner les procédures habituelles. L'expéditeur exige que l'employé garde l'information secrète vis-à-vis de son responsable direct.
- Point essentiel à retenir : Les éléments qui semblent authentiques ne sont qu'un écran de fumée. Le véritable danger provient des leviers de manipulation utilisés (urgence, confidentialité, entorse aux règles).

Conclusion

 **Durée :** 5 minutes

Concluez l'exercice en reliant directement ces concepts à la réalité de votre organisation. Expliquez que repérer un signal d'alerte n'est que la première étape de la défense ; la seconde consiste à réagir correctement en suivant les procédures de l'organisation.

Profitez de ce moment pour répondre aux questions concernant le signalement interne de ce type d'arnaque ainsi que les outils, canaux et ressources disponibles pour signaler ces incidents.

Pièce jointe – Copie du scénario

 Nouveau message

 Boîte de réception

 Brouillons

 Envoyés

 Suivis

 Courriers indésirables

 Corbeille

 Archive

 Tous les e-mails

 Archive

 Courrier indésirable

 Supprimer

 Plus

 Répondre

 Transférer

De : Marc Foret <m.foret@summitview-logistics-interne.com>

À : Thierry Chanoix

Objet : **URGENT : Dépôt de garantie pour l'entrepôt de Paris**

Bonjour Thierry,

Je suis actuellement avec les courtiers à Paris. Nous sommes prêts à signer le bail de l'entrepôt dont nous avons parlé lors de la réunion générale de lundi.

Nous avons un gros problème. Une autre entreprise vient tout juste de faire une offre pour cette installation. Le courtier a indiqué que si nous ne versions pas le dépôt de garantie de 50 000 € dans l'heure qui vient, il attribuerait le bail à l'autre entreprise.

Hélène Goujon est actuellement en vol et je ne peux pas attendre son accord. De plus, le courtier n'est pas encore enregistré dans notre portail fournisseurs, et la procédure administrative prendrait trop de temps.

J'ai besoin que vous effectuiez immédiatement un virement bancaire direct vers les coordonnées jointes ci-dessous. Restez discret jusqu'à ce qu'Hélène ait atterri afin d'éviter toute inquiétude en interne sur un échec éventuel de l'accord. Prévenez-moi dès que le virement aura été confirmé.

Cordialement,

Marc

 Pièce jointe : Coordonnées_virement_bancaire.pdf

Détails crédibles : localisation de l'expéditeur (Paris) ; mention d'un projet réel (location de l'entrepôt / réunion générale) ; connaissance du nom et de la situation de la directrice financière (Hélène est en vol).
Signaux d'alerte : urgence extrême (« dans l'heure » / « attribuer le bail à l'autre entreprise ») ; contournement des procédures (fournisseur pas enregistré sur le portail) ; isolement (« restez discret »).