MAIL SUSPECT

Étape 1 : Investiguer auprès de l'utilisateur

Lister les questions à poser à l'utilisateur lors de l'entretien :

- **Expéditeur : Quelle est l'adresse email de l'expéditeur ?**
- **Principes du phishing : Avez-vous remarqué quelque chose d'inhabituel dans l'email (grammaire, orthographe, urgences suspectes) ?**
- **Messages d'alertes : Avez-vous reçu des messages d'alerte ou de notification suspecte concernant cet email ?**
- **Récurrences : Avez-vous déjà reçu des emails similaires par le passé ?**
- **Étendues : Cet email a-t-il été envoyé à d'autres collègues ? Si oui, qui sont-ils ?**
- **Interactions : Avez-vous cliqué sur un lien ou ouvert une pièce jointe contenue dans l'email ?**

Étape 2 : Analyser les composants du mail

Décrivez la méthodologie :

1. **En-tête du mail :**
    - **Expéditeur : Vérifier l'adresse email de l'expéditeur pour détecter toute incohérence ou usurpation.**
    - **Destinataires : Identifier tous les destinataires pour vérifier s'il s'agit d'une attaque ciblée ou massive.**
    - **Chemin de transmission : Analyser le chemin suivi par l'email depuis l'expéditeur jusqu'au destinataire pour déceler toute anomalie.**
2. **Corps du mail :**
    - **Pièces jointes : Non**
    - **URL : "Télécharger application ma banque (découvrez les grandes fonctionnalités)", "Lien SecuriPass"**

Étape 3 : Qualification de la menace

Menace pour l'utilisateur :

- **Vol de données : Les informations personnelles et financières peuvent être dérobées, conduisant à une usurpation d'identité.**
- **Installation de malware : Le clic sur des liens malveillants peut installer des logiciels nuisibles sur l'ordinateur de l'utilisateur, compromettant sa sécurité et sa vie privée.**

Menace pour l'entreprise :

- **Fuite de données sensibles** : Les informations d'entreprise confidentielles peuvent être exposées, ce qui peut entraîner des pertes financières et une atteinte à la réputation.
- **Compromission des systèmes** : Les systèmes internes peuvent être infiltrés, permettant aux attaquants d'accéder à des réseaux et de causer des perturbations opérationnelles.

Étape 4 : Faut-il sensibiliser les utilisateurs ?

Oui, une sensibilisation est nécessaire pour prévenir de futures attaques similaires.

Pour sensibiliser au phishing, voici quelques mesures à proposer :

Formations régulières :

- Organiser des sessions de formation pour aider les employés à reconnaître les signes de phishing (faute d'orthographe, urgences artificielles, adresses email suspectes).
- Utiliser des simulations de phishing pour évaluer et améliorer la vigilance des employés.

Rappels de bonnes pratiques :

- Ne jamais cliquer sur des liens ou ouvrir des pièces jointes provenant d'expéditeurs inconnus.
- Vérifier l'authenticité des emails en contactant directement l'expéditeur via un numéro de téléphone officiel.
- Encourager l'utilisation de l'authentification à deux facteurs pour renforcer la sécurité des comptes.

Étape 5 : Qualifier le cas

Cet e-mail semble être une tentative de phishing. Il comporte des fautes d'orthographe et des espaces inutiles. De plus, les banques ne menacent pas de geler les comptes ou de les mettre sous tutelle pour ne pas avoir adhéré ou mis à jour un SécuriPass.