Agir contre le hameçonnage

Qu'est-ce que l'hameçonnage ?

L'hameçonnage (phishing) consiste à inciter les individus à divulguer des informations confidentielles (ex : identifiants, mots de passe, données personnelles, etc.) en utilisant des communications trompeuses, telles que des e-mails, des SMS, etc., prétendant provenir d'organisations légitimes.

Comment reconnaître une tentative d'hameçonnage ?

Les signes de phishing peuvent varier, cependant, certains indicateurs sont fréquemment observés, tels que :

- Réception de **messages non sollicités** provenant d'expéditeurs ou d'entreprises inconnus.
- **Sollicitations pressantes** pour des données personnelles ou confidentielles.
- Inclusion de **liens suspects** dans les emails ou les messages.
- Présence **d'erreurs grammaticales ou d'orthographe** dans les communications.

Actions préventives contre l'hameçonnage

Pour prévenir l'hameçonnage, certaines mesures doivent être adoptées :

- Organiser des **sessions de formation à la cybersécurité**, en mettant l'accent sur les types d'hameçonnage, les critères de contrôle dans les communications et les risques associés.
- Diffuser des **supports informatifs** détaillant les directives à adopter en cas d'une attaque d'hameçonnage.
- **Encourager les collaborateurs à signaler** toute activité d'hameçonnage suspecte.
- **Déployer des solutions de filtrage mails** pour prévenir les attaques d'hameçonnage.

Réagir face à une attaque d'hameçonnage

Face à une attaque de phishing, il est nécessaire de réagir rapidement :

Isoler et contenir :

- Isoler immédiatement l'appareil ou le compte affecté en le déconnectant du réseau ou en le désactivant si nécessaire.
- Informer les autres membres de l'équipe de ne pas ouvrir ou cliquer sur des liens provenant de l'appareil ou du compte compromis.

Analyser les dommages potentiels :

- Examiner les activités suspectes ou les changements survenus sur l'appareil ou le système compromis.
- Déclencher une levée de doutes afin de rechercher toute trace de compromission sur le poste ou le compte ciblé.

Modifier les identifiants :

- Changer immédiatement les mots de passe de tous les comptes compromis.

Informer l'équipe de sécurité informatique :

- Signaler l'incident au service de sécurité informatique de l'entreprise ou à l'administrateur réseau pour une enquête approfondie.
- Fournir des détails sur le mail de phishing (ex : son contenu, l'expéditeur, les liens ou pièces jointes suspects, etc.).

Rétablir les données et les systèmes :

- Restaurer les sauvegardes ou les versions précédentes des fichiers affectés si nécessaire.

Ressources mises à disposition

- Que faire en cas de phishing de **cybermalveillance.gouv.fr** (Site Web)
- Agir contre une campagne d'hameçonnage du **CERT Santé** (PDF)
- Attaque par hameçonnage de l'**ANSSI** (Site Web)
- 5 réflexes à avoir lors de la réception d'un courriel de l'**ANSSI** (Site Web)