APAJH Fédération

Guide Pratique

Reconnaitre une attaque cyber

APAJH Fédération

✱ ✱ ✱ Usurpation d'identité

> *J'ai reçu un appel téléphonique d'un prestataire me demandant un accès à distance au SharePoint d'un service interne…*

Attaquant

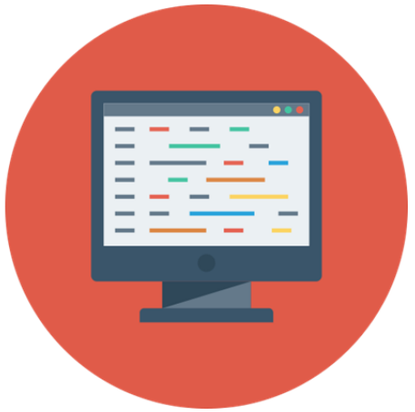
Collaborateur APAJH

Je reçois un appel téléphonique…

Bonjour,

Nos bases de données ont été corrompues, et nous aurions besoin d'un accès aux données sur le projet P. Pourriez-vous nous fournir un accès au *SharePoint* sur l'adresse suivante ?
prestataire@presta.com

Je fournis au prestataire un accès au SharePoint



Les données ont été compromises… Que s'est-il passé ?

Un individu s'est fait passer pour un prestataire et contacte un collaborateur. Il utilise des techniques de manipulation pour obtenir des informations confidentielles sauvegardés dans le *SharePoint* de la Fédération.

Soyez toujours attentifs!

Une personne malveillante peut se faire passer pour un employé, un fournisseur ou un partenaire commercial afin de vous **soutirer des informations confidentielles**!

✱ ✱ ✱ Usurpation d'identité

Cette fraude se déroule généralement par mail ou par téléphone (appel ou SMS), mais les pirates sont inventifs et développent chaque jour de nouvelles méthodes d'attaque…

Quels sont les signes d'une usurpation d'identité ?

J'analyse la source du message

- L'adresse e-mail est inhabituelle / ne correspond pas au nom de l'expéditeur.
- L'adresse e-mail provient d'un domaine extérieur à la Fédération (par exemple, ne se termine pas en *apajh.asso.fr*)
- Le numéro de téléphone est inconnu.

J'analyse le contenu du message

- Le message est grammaticalement incorrect.
- L'émetteur demande des informations inhabituelles (documents confidentiels, mot de passe, envoi par une méthode non utilisée à la Fédération …).
- L'émetteur demande secrètement des informations, ou de manière urgente.

Si le message ou l'appel correspond à plusieurs de ces critères, il peut s'agir d'une tentative d'usurpation d'identité!

Par téléphone, je propose à la personne de la rappeler plus tard. Cela me donne le temps de vérifier la légitimité de sa demande.

Les méthodes et les conséquences de cette attaque

1 Ingénierie sociale

Un individu se fait passer pour un employé ou un fournisseur et contacte les services internes de la Fédération afin d'obtenir des informations confidentielles en exploitant la confiance de la victime.

2 Vol d'identité en interne

Un employé malveillant utilise les informations d'identification d'un collègue pour accéder à des données sensibles et commettre des actes répréhensibles en son nom.

3 Faux sites web

Des cybercriminels créent de faux sites web similaires à ceux de l'entreprise pour tromper les employés et obtenir leurs informations d'identification.

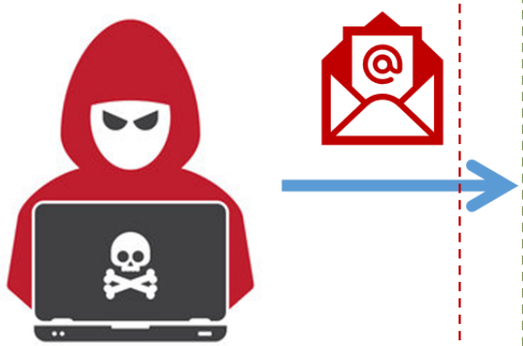
Comment réagir ?

En cas de doute, j'appelle directement l'émetteur au téléphone pour confirmer sa demande, et je signale tout message suspect au support informatique (*support@apajh.asso.fr Ou support@humane-si.fr*).

✱ ✱ ✱ Le Hameçonnage (« Phishing »)

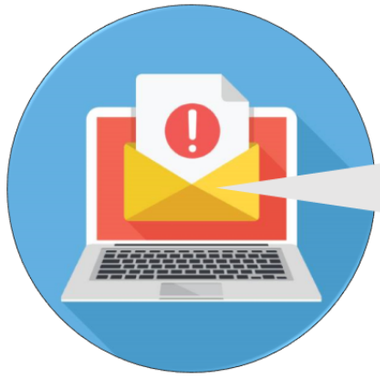
> *Je viens de recevoir un mail me demandant de changer mon mot de passe avant demain soir, sous peine de voir mon compte bloqué… Je dois me dépêcher!*

Attaquant



Collaborateur APAJH

Je viens de recevoir un mail du support !

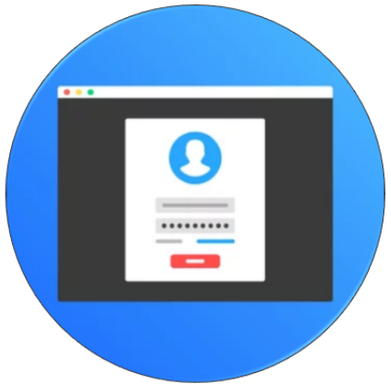


De: support@apaih.asso.fr
À: moi@apajh.asso.fr
Objet: Renouvellement obligatoire
politique_de_securite.exe

Pour rester en conformité avec la nouvelle politique de sécurité de la DSI (disponible en pièce-jointe), tous les collaborateurs sont priés de bien vouloir changer leur mot de passe avant demain soir sur la plateforme:
https://www.apajh.org/mot-de-passe
Passé ce délai, les comptes seront bloqués par le support.

Cordialement,
La Direction des Systèmes d'Information

Je m'authentifie et modifie mon mot de passe. J'en profite pour consulter la nouvelle politique de sécurité.



Mon ordinateur est bloqué … Que s'est-il passé ?

Le mail contient un lien trompeur et un fichier frauduleux! J'ai transmis mes identifiants à un pirate, et j'ai installé son virus sur mon ordinateur en consultant le document.

Définition

Le hameçonnage est une technique d'attaque pouvant se baser sur l'usurpation d'identité. L'attaquant envoie un mail contenant une **pièce jointe infectée** ou un **lien frauduleux** visant à dérober des informations confidentielles.

✱ ✱ ✱ Le Hameçonnage (« Phishing »)

> *Les attaques de phishing se déroulent aussi par SMS, et les pirates peuvent vous inciter à cliquer sur des liens infectés en vous promettant une récompense à la clé.*

Quelles sont les conséquences ?

En téléchargeant la pièce jointe ou en cliquant sur le lien sans procéder à aucune vérification, je prends le risque de :

Divulguer mes informations personnelles, ou celles d'une personne accompagnée

Divulguer mes mots de passe et mes identifiants de connexion

Exposer la Fédération à une cyber-attaque

Comment reconnaitre un mail frauduleux ?

J'analyse la source et le contenu du message en utilisant la même méthode que pour reconnaître une usurpation d'identité.

La pièce-jointe:

Je me méfie des pièces jointes que je n'attend pas

Je ne télécharge jamais les fichiers en .exe, .pif, .bat et .com

Les liens:

Je passe ma souris sur le lien sans cliquer pour voir l'URL qui se cache derrière

Je ne clique pas si l'URL n'a pas le « s » de « https:// »

Comment réagir ?

En cas de doute je ne clique sur aucun lien ni pièce jointe et je signale tout message suspect au support informatique (*support@apajh.asso.fr Ou support@humane-si.fr*).

✱ ✱ ✱ Les logiciels malveillants

> *Lorsque je suis victime d'hameçonnage, je peux télécharger plusieurs types de logiciels malveillants à mon insu. Quels sont-ils et quelles sont les différences ?*

Virus

Programme malveillant pouvant altérer ou endommager les fichiers d'un ordinateur. Les virus ont la capacité de **se propager entre plusieurs ordinateurs** connectés, tout en transmettant vos informations aux pirates.

Rançongiciel (« *Ransomware* »)

Logiciel malveillant **prenant en otage des données** en les chiffrant. Les pirates utilisant cette attaque réclament une rançon en échange du déchiffrement des données, ou menacent de les détruire.

Logiciel espion (« *Spyware* »)

Programme installé à l'insu de l'utilisateur, et qui **collecte des données** comme les sites visités, les documents consultés et les frappes clavier de l'utilisateur, et qui les transmet à la personne à l'origine de l'attaque.

Cheval de Troie (« *Trojan Horse* »)

Programme malveillant **« déguisé » en programme légitime**. L'utilisateur l'installe lui-même sans se rendre compte de la supercherie. Un cheval de Troie peut cacher n'importe quel type de programme malicieux, il faut donc être extrêmement vigilant en téléchargeant des fichiers et programmes sur internet.

Comment réagir ?

Si je pense avoir téléchargé un logiciel malveillant, je contacte immédiatement le support informatique (*support@apajh.asso.fr Ou support@humane-si.fr*).