



SÉCURITÉ DU NUMÉRIQUE L'HAMEÇONNAGE (OU PHISHING)

Cible : personnels des organismes privés et publics

1 Et si c'était vous ?



Ingénierie sociale

Alors que vous assurez la permanence pendant les fêtes de fin d'année, un individu vous contacte par téléphone. Il souhaite obtenir rapidement, pour motif professionnel, les codes d'accès de l'application financière en charge des paiements fournisseurs et des salaires. À force d'arguments et grâce à un ton assuré, il réussit à vous convaincre et, en l'absence de votre hiérarchie, vous cédez sous la pression et lui communiquez l'information convoitée.

S'il ne s'agit pas d'une attaque informatique directe mais d'une technique répandue d'ingénierie sociale, ce type d'information (code d'accès, coordonnées bancaires, données personnelles, etc.) peut être utilisé comme point d'entrée pour mener une attaque à l'encontre de votre organisme.



Attaque par la messagerie

Au retour d'une absence prolongée du bureau, vous trouvez votre messagerie électronique engorgée. Pressé, vous ignorez l'invitation à redémarrer votre ordinateur et empêchez par conséquent l'installation des mises à jour. En parcourant rapidement les objets de vos courriels, l'un d'eux semble traiter d'affaires en cours vous concernant directement et retient votre attention. Vous l'ouvrez et y découvrez un bref message vous enjoignant de consulter un site Internet qui vous est familier dans l'exercice quotidien de vos fonctions.

Vous venez d'être victime d'hameçonnage (ou phishing).

En contrevenant à un principe d'hygiène fondamental (mettre à jour ses logiciels) et en cliquant sur ce lien d'apparence légitime sans prêter attention à certains détails, vous avez permis à un attaquant d'installer un programme malveillant dans le système d'information de votre entreprise et vous lui avez donné accès non seulement à vos dossiers mais aussi à ceux de vos collègues.

2 Comment renforcer ma vigilance et bien me protéger ?



Qu'est-ce que l'hameçonnage ?

L'hameçonnage est une technique d'attaque prenant la forme d'un courriel qui vous est adressé et qui semble provenir d'un expéditeur de confiance. Ce courriel peut contenir un **fichier**, une **pièce jointe** ou un **lien de redirection vers un site frauduleux**, avec une incitation à cliquer sur ces éléments, ce qui permettra à l'attaquant de recueillir de l'information ou d'installer un programme malveillant dans le système d'information de votre organisme.



Adopter les bonnes pratiques au quotidien

- Méfiez-vous des courriels exigeant de vous une réponse ou une action immédiate et vous intimant de ne pas en informer votre hiérarchie ou vos collaborateurs.
- Soyez prudents vis-à-vis des courriels comportant des visuels a priori officiels mais dont la résolution est mauvaise.
- Ne cliquez jamais sur un lien ou une pièce jointe dont l'origine ou la nature vous semblent douteuses. **Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse dans la barre de recherche.**
- Soyez à l'affût des fautes d'orthographe ou de syntaxe dans l'adresse de l'expéditeur, l'objet du courriel ou le corps du texte.
- Ne répondez jamais à un courriel vous demandant des informations confidentielles (identifiants, coordonnées bancaires, etc.). **Au moindre doute, n'hésitez pas à contacter l'expéditeur** par un autre canal, par exemple téléphonique.
- Méfiez-vous des courriels d'expéditeur connu mais dont l'adresse électronique ou la nature du message sont inhabituelles ou catégorisés comme « spam / indésirable » par le logiciel de messagerie.
- Procédez régulièrement au redémarrage de votre poste, notamment lorsque le système vous y invite.

3

Je pense avoir été victime d'une attaque. Que faire ?



Qui prévenir ?

Si vous pensez avoir été victime d'une attaque informatique :

- prévenez immédiatement le support informatique de votre organisme et vos supérieurs hiérarchiques ;
- procédez sans délai au renouvellement de vos identifiants si vous les avez transmis lors de l'attaque.

4

Documents de référence

Guide des bonnes pratiques de l'informatique

http://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf



CONDUITE A TENIR LORS D'UN ÉVÉNEMENT BIOLOGIQUE OU CHIMIQUE

Fiche pratique à destination des responsables de sécurité et de sûreté des établissements recevant du public (ERP)

(Fiche actualisée en date du 7 mai 2019)

Cette fiche décrit les bons réflexes à adopter en cas de survenue d'un événement de type biologique ou chimique au sein d'un ERP afin de limiter au maximum le nombre de victimes et de préparer au mieux l'arrivée des services spécialisés. Elle ne vise pas à faire de chaque agent de sécurité un spécialiste des risques biologiques et chimiques. Elle vient en complément de la fiche de sensibilisation du grand public sur cette thématique déjà accessible sur le site du gouvernement : <https://www.gouvernement.fr/partage/10904-que-faire-en-cas-d-exposition-a-un-produit-toxique-ou-contaminant-reagir-attaque-chimique>

- Les criminels et les terroristes ont démontré leur capacité à fabriquer des explosifs ou des substances chimiques en utilisant des produits chimiques courants.
- La fabrication et la volonté des terroristes à utiliser des armes biologiques ou chimiques est aujourd'hui avérés. Plusieurs tentatives d'attentats ont été déjouées par les autorités ces dernières années :
- Été 2017** : arrestation d'individu préparant un attentat chimique en Australie ;
- Mars 2018** : tentative d'assassinat au novitchok au Royaume-Uni ;
- Mai 2018** : découverte de tutoriels de fabrication d'explosifs et de ricine (toxine) lors d'une perquisition en France ;
- Juin 2018** : découverte d'un laboratoire clandestin de production de ricine en Allemagne.
- Novembre 2018** : arrestation en Italie d'un suspect souhaitant commettre un attentat à la ricine.

En cas d'événement de nature biologique ou chimique, une bonne organisation préalable de vos établissements ainsi qu'une réaction adaptée de vos personnels peuvent sauver des vies.

1

Généralités sur la menace biologique et chimique



La menace biologique se caractérise par l'utilisation de deux types d'agents :

- les agents infectieux (virus, bactéries, champignons). Ils peuvent être :
 - **contagieux**. Quelques agents suffisent alors pour provoquer une épidémie si la maladie n'est pas détectée à temps ;
 - **peu ou pas contagieux (bacilles du charbon)**. Ces agents peuvent exceptionnellement se transmettre lorsqu'ils sont, par exemple, sous forme de poudre fine volatile. La dispersion initiale peut passer inaperçue. La maladie se déclare alors après une période d'incubation pouvant aller de un à dix jours, compliquant d'autant plus l'identification de son origine.
- les toxines sont des substances toxiques produites par des organismes vivants** (ricine par la graine de ricin, toxine botulique par le bacille *clostridium botulinum*). Elles peuvent être :
 - inhalées par les voies respiratoires, leur action nocive peut alors survenir en quelques minutes ;
 - ingérées par voie alimentaire ou hydrique, leur action peut survenir en quelques heures, voire davantage. La survie des personnes intoxiquées tient alors essentiellement à l'identification très rapide de l'agent et, souvent, à l'administration, en extrême urgence, du traitement adéquat.



La menace chimique est liée à l'utilisation de produits toxiques qui sont inhalés par les victimes (gaz ou aérosols de fines gouttelettes), **qui pénètrent à travers la peau ou qui sont ingérés** (aliments, boissons).

Si **leur action est généralement rapide** (quelques secondes à quelques minutes), ils peuvent toutefois entraîner des effets secondaires très graves qui n'apparaissent que plusieurs heures après l'agression (phosgène, chlore, etc.).

Certains de ces produits sont très répandus dans l'industrie (chlore, cyanures), d'autres sont uniquement fabriqués à des fins offensives (sarin, ypérite, etc.).

Si certains toxiques se dispersent assez rapidement (acide cyanhydrique, chlore), d'autres, moins volatiles, sont dits « persistants » et peuvent maintenir le danger pendant plusieurs heures, voire plusieurs jours. Ces derniers sont généralement « contaminants » : ils se déposent sur le corps, les vêtements, les objets et peuvent se transférer d'une personne à l'autre.



CONDUITE A TENIR LORS D'UN ÉVÉNEMENT BIOLOGIQUE OU CHIMIQUE

FICHE PRATIQUE À DESTINATION DES RESPONSABLES DE SÉCURITÉ

(Fiche actualisée en date du 7 mai 2019)

2

Un événement biologique ou chimique, qu'il soit intentionnel ou accidentel, peut être détecté par **l'observation concomitante de certains indices** (odeur inhabituelle, déversement d'une substance liquide, nuage de fumée, etc.) **et de symptômes identiques sur plusieurs personnes**. Sans disposer de matériel de détection spécifique, cette concomitance d'indices et de symptômes doit alerter et pousser les agents de sécurité d'un ERP à réagir afin de limiter au maximum le nombre de victimes. **Le tableau ci-dessous récapitule :**

- **les principaux symptômes aisément détectables** chez une personne soumise à l'action d'un agent biologique ou d'une substance chimique ;
- **les principales actions à réaliser** afin limiter le nombre de victimes et préparer l'arrivée des services de secours spécialisés.

ÉLÉMENTS D'ALERTE

LES SYMPTÔMES : OBSERVÉS SUR PLUSIEURS PERSONNES À LA FOIS, ILS DOIVENT VOUS ALERTER

- Angoisse, agitation
- Chute brutale
- Tremblements, convulsions, crampes
- Suffocation
- Difficulté pour respirer
- Toux
- Larmoiements, sueurs
- Douleur aux yeux
- Écoulement nasal et/ou salivaire
- Irritation, brûlure de la peau
- Sensation de brûlure, de douleur
- Sensation de poids sur la poitrine
- Sensation de brûlure dans la gorge
- Douleur abdominale
- Nausées, vomissements
- Diminution du diamètre de la pupille

PRINCIPALES ACTIONS À RÉALISER

ALERTER LES SECOURS

- Alerte, ou demandez à votre poste de sécurité d'alerter les services de secours (18, 15 ou 112).
- Donner, si possible, un bilan d'ambiance à votre service de sécurité et décrivez-lui succinctement la situation (contexte et symptômes observés, gravité et ampleur de ces symptômes, nombre et état des victimes).

PROTÉGER / RASSURER LE PUBLIC

- Faites évacuer le public de la zone soumise à un risque et guidez le vers un point de regroupement identifié, si possible aéré.
- Evitez que d'autres personnes non exposées ne viennent dans la zone concernée.
- Demandez aux personnes de limiter les contacts entre elles, de ne pas boire, manger ou fumer.
- Tentez de limiter les phénomènes de panique en rassurant les victimes et les personnes dans l'attente des secours.

PRÉPARER L'ARRIVÉE DES SECOURS

- Coupez les systèmes de ventilation et de climatisation propres au bâtiment touché afin de limiter la diffusion d'air vicié.
- Encouragez les victimes à rester sur place, au point de regroupement.
- Faites retirer les vêtements (manteau, blouson, pantalon, etc.) présentant des tâches de contamination (liquide/poudre).
- Si vous pensez être contaminé, signalez-vous aux services d'incendie et de secours ou au service d'urgence et réanimation (SMUR).