SÉCURITÉ DU NUMÉRIQUE
L'HAMEÇONNAGE (OU PHISHING)

VIGIPIRATE

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.

SÉCURITÉ DU NUMÉRIQUE
L'HAMEÇONNAGE (OU PHISHING)

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

SGDSN
SECRETARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette et impression : Pôle Conception graphique-Fabrication - DSAF/DPL - Octobre 2017.

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extremisme ou au terrorisme. L'objectif du signalement est de protéger ces personnes en les empêchant de commettre un acte criminel et de protéger la population de possibles comportements violents.

1 Pourquoi signaler un cas de radicalisation ?

La radicalisation **concerne tout type d'idéologie** qui peut conduire un individu à choisir l'action violente au nom de convictions auxquelles il adhère sans compromis possible. Cette action violente peut causer la mort d'autres membres de la société dont il rejette inconditionnellement les valeurs et le mode de vie.

Il s'agit d'un **processus de radicalisation** par paliers avec adhésion à une idéologie et rupture avec l'environnement habituel. La radicalisation apparaît comme un phénomène profondément lié à l'exploitation de conflits d'identité, de frustrations ou de fragilités. Certains groupes terroristes cherchent notamment à enrôler des individus en perte de repères et vulnérables.

La force d'une idéologie et son pouvoir d'attraction ne doivent pas être sous-estimés. Des individus ayant développé une haine de notre société peuvent adhérer pleinement à un discours qui donne sens à leurs frustrations ou sentiment d'humiliation.

La radicalisation est un phénomène complexe, amplifié par le développement des réseaux sociaux. La propagande véhiculée par des individus ou par des groupes touche des profils variés : délinquants, personnes vulnérables en quête d'identité, personnes ayant des troubles psychiatriques, etc.

Difficile à repérer et à traiter, la radicalisation est donc un enjeu majeur de sécurité nationale.

2 Identifier une situation de radicalisation

Identifier un processus de radicalisation ne se fait pas sur la base d'un seul indice. Pris isolément, un des comportements listés ci-dessous ne signifie pas qu'il y a radicalisation. C'est la combinaison de plusieurs comportements qui vous donne une forme de cohérence et qui doit provoquer votre étonnement.

COHÉRENCE → VIGILANCE → SIGNALEMENT

Les signaux de rupture :

- changements physiques et vestimentaires, alimentaires, de vocabulaire... inquiétants ;
- propos asociaux, apologie de la violence ;
- passage soudain à une pratique religieuse hyper ritualisée ;
- rejet de l'autorité et de la vie en collectivité ;
- rejet brutal des habitudes quotidiennes ;
- repli sur soi ;
- expression de haine de soi, rejet de sa propre personne, déplacement de la haine de soi sur d'autrui en raison d'une idéologie ;
- rejet de la société et de ses institutions (école, etc.) ;
- éloignement de la famille et des proches ;
- modification soudaine et inhabituelle des centres d'intérêt ;
- Etc.

VIGIPIRATE

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION

3 Initier une démarche de signalement

Il s'agit de **prévenir, voire d'éviter, le basculement vers un comportement violent,** ainsi que d'accompagner les jeunes et les familles par des cellules adaptées au sein des préfectures de leur département de résidence.

L'objectif du signalement est de **protéger l'intéressé en l'empêchant de commettre un acte criminel** (pour le sortir au plus tôt du chemin sur lequel il s'est engagé peut-être malgré lui) et de **protéger la population** de possibles comportements violents.

Prendre l'initiative d'appeler le numéro vert constitue un simple signalement. Il appartiendra aux spécialistes d'en évaluer le caractère sérieux et la gravité.

Dans quels cas pouvez-vous appeler ?

- ⊙ Pour signaler une situation inquiétante, qui paraît menacer un proche.
- ⊙ Si vous avez un doute ou des questions sur une situation.
- ⊙ Pour obtenir des renseignements sur la conduite à tenir.
- ⊙ Pour être écouté(e), conseillé(e) dans vos démarches.

Appeler le numéro vert : **0 800 005 696**
Les appels sont strictement confidentiels, votre identité ne sera pas dévoilée.
Ou remplissez le formulaire en ligne :
https://www.interieur.gouv.fr/Dispositif-de-lutte-contre-les-filieres-djihadistes/Assistance-aux-familles-et-prevention-de-la-radicalisation-violente/Votre-signalement
Ou contacter le commissariat de police ou la brigade de gendarmerie la plus proche.
Mais en cas d'urgence appelez immédiatement le 17.

4 Que se passe-t-il après un signalement ?

Si la situation est jugée préoccupante par les services de l'État, la personne faisant l'objet du signalement ainsi que sa famille **bénéficieront d'un accompagnement spécialisé et adapté à leur situation.**

Votre identité ne sera pas dévoilée, les signalements sont strictement confidentiels. Même si vous n'êtes pas sûr d'avoir reconnu des combinaisons de signes de comportement suspect, **vous pourriez sauver des vies.** il est donc préférable d'appeler rapidement le numéro vert. Des spécialistes se chargeront de qualifier la situation de préoccupante ou non.

Signaler une situation ne vous sera jamais reproché. il n'est jamais trop tard pour signaler une situation de radicalisation.

5 Signaler un contenu appelant à la haine ou faisant l'apologie du terrorisme sur Internet

Internet et les média sociaux ont favorisé la diffusion d'appels à la haine et de messages faisant l'apologie du terrorisme sur la toile.

La liberté d'expression est un élément fondamental de notre société. Elle ne constitue toutefois pas un « passe-droit » pour tout rédiger et publier sur Internet. En 2009, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation, également appelée PHAROS, a été mise en place par l'État pour signaler les comportements illicites sur internet.

Lorsque vous constatez des contenus appelant à la haine ou faisant l'apologie du terrorisme sur Internet, ne les partagez pas, ne les likez pas, ne les retweetez pas. Ayez le bon réflexe, signalez les sur :

https://www.internet-signalement.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrication, déploiements, image – DSAF/OPSG – Octobre 2020.