La Fraude au faux président

QUELQUES CHIFFRES À CONNAÎTRE

En 2015, l'Observatoire national de la délinquance et des réponses pénales (ONDRP) a recensé 70 000 cyber-infractions. 90 % de ces atteintes relèvent des escroqueries et autres attaques financières.

En 6 ans, l'Office central pour la répression de la grande délinquance financière (OCRGDF) a recensé:

- 2550 faits d'escroqueries au faux virement,
- 1600 sociétés victimes pour un préjudice global de 550 M€.

Les tentatives représentent plus de 1 milliards €.

MODE OPÉRATOIRE DE CETTE ESCROQUERIE

- Utilisation de l'ingénierie sociale, méthode visant à obtenir des informations auprès d'individus, à leur insu.
- L'escroc se fait passer pour le président de l'établissement.
- Plusieurs échanges pour mettre la victime en confiance.
- Demande de réalisation d'un virement international par l'escroc, sous le signe de la confidentialité et de l'urgence.
- Exécution du virement par la victime sur un compte étranger.

COMMENT S'EN PRÉMUNIR

Pour diminuer l'exposition au risque, des mesures d'ordre organisationnel, technique et comportemental peuvent être mises en oeuvre.

Sur le plan organisationnel

- Sensibiliser régulièrement tout le personnel (y compris les stagiaires, les nouveaux arrivants, les saisonniers, les prestataires,…),
- Mettre en place des procédures de vérifications et de signatures multiples pour les paiements internationaux.
- Renforcer les contrôles sur les paiements internationaux à destination de certains pays (Chine, Pays de l'Est, Suisse, etc.)

Sur le plan technique

- Les fautes d'orthographe dans les mails et les erreurs dans les noms et fonctions du dirigeant doivent éveiller l'attention.
- Rompre la chaîne des mails pour diminuer le risque de se faire abuser (ne pas faire répondre à..). Ne pas hésiter à faire appel au responsable des SI le cas échéant.

Sur le plan comportemental

- Avoir un usage prudent des réseaux sociaux et ne pas y diffuser d'informations relatives à l'entreprise.
- Respecter les procédures mise en place malgré les pressions d'un interlocuteur sollicitant un paiement dans l'urgence.
- Rester attentif aux demandes inhabituelles de transmission de nouvelles coordonnées.

COMMENT RÉAGIR ?

Pour ce type d'escroquerie, la réactivité est déterminante pour optimiser les chances d'un retour rapide des fonds et une enquête pénale fructueuse. L'avocat de l'entreprise doit demander le blocage des fonds sans délai.

OÙ ET COMMENT DÉPOSER PLAINTE ?

Même s'il existe des services spécialisés comme par exemple la BEFTI à Paris, les services de la sous-direction de lutte contre la cybercriminalité (SDLC), ou encore le centre de lutte contre les criminalités numériques (C3N), le dépôt de plainte en commissariat ou en brigade de gendarmerie doit être privilégié.

Pour autant, dans les cas où le dépôt de plainte ne se justifie pas (certaines tentatives par exemple), il peut être utile de multiplier les signalements pour faire bloquer les sites frauduleux ou permettre aux enquêteurs de réaliser des recoupements.

S'INFORMER ET SIGNALER

Info-escroquerie

Ce site est fait pour vous renseigner sur les escroqueries, ou vous permettre de signaler:

- un site internet ou un courriel d'escroqueries,
- un vol de coordonnées bancaires ou une tentative de hameçonnage.

Ce service est disponible du lundi au vendredi, de 9h à 18h30, au numéro vert (appel gratuit) suivant: **0 805 805 817**.

Plateforme PHAROS

Constituant l'un des services de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), et composé de 23 gendarmes et policiers, PHAROS centralise les signalements de contenus et comportements illicites émis sur **internet-signalement.gouv.fr**.

En 2016, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) a reçu 170 721 signalements :

- *49% concernaient des escroqueries*,
- 11% des atteintes aux mineurs,
- 10% des discriminations,
- 7% des faits d'apologie et de provocation au terrorisme.

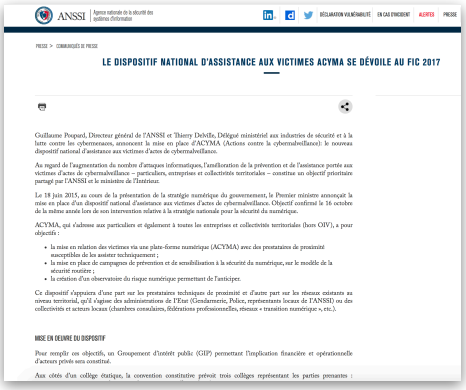
Phishing-initiative

Le hameçonnage (ou phishing) est une technique utilisée par des escrocs pour obtenir des renseignements personnels, et leur permettre de perpétrer une usurpation d'identité. Le **site phishing-initiative** vous permet de *rendre indisponible* tout site frauduleux, dans les principaux navigateurs web et en quelques clics (après validation).

ACYMA: Actions contre la cybermalveillance

Mise en œuvre par un Groupement d'intérêt public, ACYMA constitue le dispositif national d'assistance aux victimes de cybermalveillance qui se destine:

- Aux particuliers,
- Aux collectivités territoriales,
- Aux entreprises de toutes tailles (hors OIV).


ANSSI

LE DISPOSITIF NATIONAL D'ASSISTANCE AUX VICTIMES ACYMA SE DÉVOILE AU FIC 2017

Guillaume Poupard, Directeur général de l'ANSSI et Thierry Delville, Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, annoncent la mise en place d'ACYMA (Actions contre la cybermalveillance) : le nouveau dispositif national d'assistance aux victimes d'actes de cybermalveillance.

Au regard de l'augmentation du nombre d'attaques informatiques, l'amélioration de la prévention et de l'assistance portée aux victimes d'actes de cybermalveillance – particuliers, entreprises et collectivités territoriales – constitue un objectif prioritaire partagé par l'ANSSI et le ministère de l'Intérieur.

Le 18 juin 2015, au cours de la présentation de la stratégie numérique du gouvernement, le Premier ministre annonçait la mise en place d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance. Objectif confirmé le 16 octobre de la même année lors de son intervention relative à la stratégie nationale pour la sécurité du numérique.

ACYMA, qui s'adresse aux particuliers et également à toutes les entreprises et collectivités territoriales (hors OIV), a pour objectifs :

- la mise en relation des victimes via une plate-forme numérique (ACYMA) avec des prestataires de proximité susceptibles de les assister techniquement ;
- la mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique, sur le modèle de la sécurité routière ;
- la création d'un observatoire du risque numérique permettant de l'anticiper.

Ce dispositif s'appuiera d'une part sur les prestataires techniques de proximité et d'autre part sur les réseaux existants au niveau territorial, qu'il s'agisse des administrations de l'Etat (Gendarmerie, Police, représentants locaux de l'ANSSI) ou des collectivités et acteurs locaux (chambres consulaires, fédérations professionnelles, réseau « transition numérique », etc.).

MISE EN ŒUVRE DU DISPOSITIF

Pour remplir ces objectifs, un Groupement d'intérêt public (GIP) permettant l'implication financière et opérationnelle d'acteurs privés sera constitué.

Aux côtés d'un collège étatique, la convention constitutive prévoit trois collèges représentant les parties prenantes :

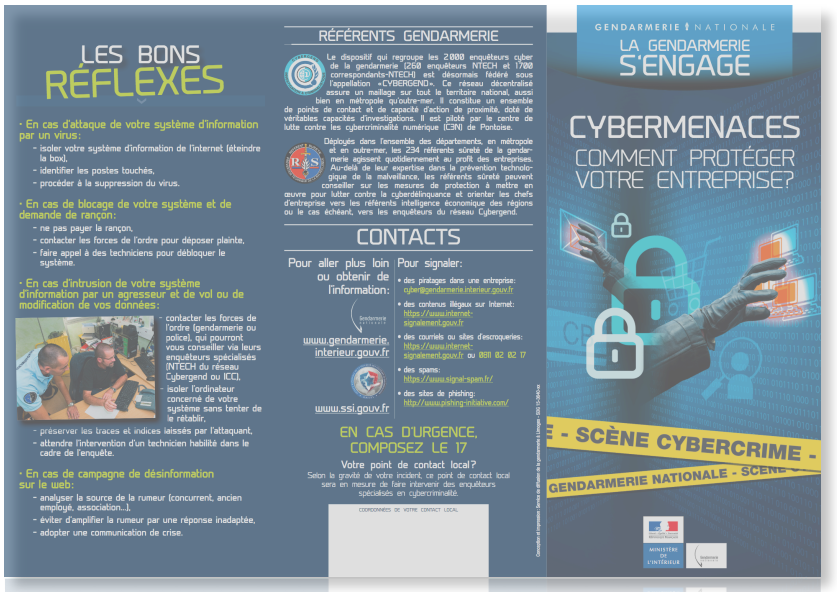
Les objectifs visés par cette plateforme sont:

- la mise en relation des victimes via une plate-forme numérique (ACYMA) avec des prestataires de proximité susceptibles de les assister techniquement,
- la mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique,
- la création d'un observatoire du risque numérique permettant de l'anticiper,

ACYMA sera lancée dans une phase pilote dans la région des Hauts de France, puis sera ouvert, à compter du mois d'octobre 2017, à l'ensemble de la France.

LE SAVIEZ-VOUS ?

Les cyberattaques ont connu une hausse de 38% au niveau mondial et de 51% en France en 2016. Chaque mois 5000 faits liés au technologies numériques sont recensés par les gendarmes.



VOUS AVEZ DIT CYBERGEND ?

Pour enquêter sur le cyberespace, rechercher, saisir et exploiter les preuves numériques, la gendarmerie s'appuie sur le dispositif Cybergend, piloté et animé par le Centre de lutte contre les criminalités numériques (C3N).

Pour signaler un piratage dans un entreprise, vous pouvez envoyer un courriel à: **cyber@gendarmerie.interieur.gouv.fr**

Une force significative

Ce réseau comprend actuellement:

- 3000 correspondants NTech (C-Ntech)
- 270 enquêteurs en technologies numériques (NTech).

POUR ALLER PLUS LOIN

- Suivre les conseils de la fédération bancaire française.
- Contacter une brigade de gendarmerie ou un commissariat de police.
- Télécharger le rapport de la délégation ministérielle en charge de la lutte contre les cybermenaces au ministère de l'intérieur.
- Télécharger la plaquette d'information sur les cybermenaces « Comment protéger votre entreprise ? ».
- Télécharger le magazine GEND'Info 392 sur la Cybercriminalité.