Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREFET DE LA CHARENTE

Angoulême, le 31 OCT. 2017

Cabinet du Préfet
Service interministériel de défense et de protection civiles
Affaire suivie par Nicolas DUDICOURT
Tél : 05 45 69 60 02
Mél : nicolas.dudicourt@charente.gouv.fr
Ref : SIDPC/ND/N° 2017- 135

SIGNALÉ

Le Préfet

à

Mesdames et Messieurs les Maires

OBJET : Nouvelle posture Vigipirate – *Transition 2017-2018*

Pièces jointes :

1. Fiche « principales mesures de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme » (nouveauté) ;
2. Fiche « Recommandations pour la sécurisation des lieux de rassemblement ouverts au public » (actualisation) ;
3. Fiche « Produits chimiques : signalement de tout vol ou utilisation suspecte » (nouveauté);
4. Fiche « Sécurité du numérique : l'hameçonnage (ou *phishing*) » (nouveauté).

La posture VIGIPIRATE *Transition 2017-2018* s'applique **à partir du 2 novembre 2017** et prend en considération les risques spécifiques liés à l'ensemble des festivités de fin d'année (marchés de Noël, cérémonies religieuses, fréquentation accrue des espaces commerciaux) et aux vacances scolaires générant de nombreux flux de voyageurs, notamment dans les transports collectifs. Elle s'applique, sauf événement particulier, **jusqu'au 28 février 2018**.

Le contexte général actuel est marqué par une menace terroriste qui demeure à un niveau très élevé, par la sortie de l'état d'urgence et par l'adoption de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme.

Le **Premier ministre a ainsi décidé de maintenir l'ensemble du territoire national au niveau « Sécurité renforcée – Risque attentat »**.

1. Axes d'effort de la nouvelle posture VIGIPIRATE

Cette nouvelle posture met l'accent sur :

– la sécurité des grands espaces de commerce lors des soldes d'hiver, celle des lieux de rassemblement, marchés de Noël et lieux de culte marqués par une forte affluence pendant les fêtes de fin d'année ;

– la sécurité dans le domaine des transports publics de personnes, en particulier lors des départs et retours des vacances scolaires et universitaires ainsi que dans les établissements d'enseignement, les établissements de santé, médico-sociaux et sociaux ;

– la protection des systèmes d'information face aux risques d'attaques cybernétiques.

2. Mesures de protection

– Vous veillerez au maintien de l'application des mesures de protection figurant dans les extraits de la partie publique du plan VIGIPIRATE dans tous les bâtiments publics et les lieux de rassemblement du public sur votre commune (ERP ou manifestations).

Ces mesures de sécurité des rassemblements, rappelées ci-dessous, doivent en particulier être appliquées lors des périodes de forte affluence et être adaptées en fonction de la configuration des lieux :

- **la surveillance des entrées par des inspections visuelles des sacs et des bagages à main.** Une attention particulière devra être portée sur les bagages les plus volumineux ou pour les bagages des personnes ayant un comportement suspect. ***En cas de refus, je vous recommande d'interdire l'accès de cette personne à votre établissement et d'en aviser les forces de l'ordre ;***
- **le contrôle des objets entrants** (livraisons, courriers, etc.) **et des accès aux zones sensibles** telles que les stations-services, les zones de livraison, les consignes automatiques ou les réserves ;
- **la surveillance à l'intérieur et aux abords des installations et bâtiments concernés par des rondes régulières et le recours à la vidéosurveillance ;**
- **la limitation voire l'interdiction du stationnement aux abords des lieux de rassemblement de personnes ainsi qu'aux abords des installations et bâtiments concernés, notamment à proximité des entrées et des issues de secours ;**
- **le renforcement des dispositifs de protection passive sur les lieux et les artères les plus fréquentés compte tenu du risque lié aux attaques par véhicules-béliers ;**
- **la vérification du bon fonctionnement des systèmes de sécurité** (alarme, évacuation, vidéosurveillance) ;
- **la sensibilisation du personnel ou des intervenants aux règles de sécurité à respecter ;**
- **la sécurisation de la sortie du public des lieux de manifestations.**

– Je vous demande également de maintenir les **mesures de précaution concernant les agents intervenant en tenue**, notamment par le port du gilet pare-balles pour les policiers municipaux, et ainsi que les **personnes exerçant certaines professions** (personnalités politiques, journalistes, etc.).

– J'attire également votre attention sur l'application des **mesures de protection de vos systèmes d'information, de communication et de sécurité** au niveau des mots de passe (*vérification de la robustesse et changement régulier à prévoir*) ou contre les attaques ciblant les sites internet à des fins d'exfiltration de données personnelles sans oublier de sensibiliser les utilisateurs sur les mesures de protection contre les attaques par courriels piégés.

3. Sensibilisation du grand public

Dans un souci de pédagogie et de large diffusion des bonnes pratiques face à la menace terroriste, vous êtes encouragés à relayer le plus largement possible les outils de sensibilisation (notamment les fiches jointes à ce courrier) téléchargeables sur les sites http://www.gouvernement.fr/vigipirate et http://www.sgdsn.gouv.fr/vigipirate

4. Suivi

– Je vous remercie de porter à la connaissance des **forces de l'ordre** tout fait ou observation qui apparaît sensible au regard du contexte actuel ;

– Le service interministériel de défense et de protection civiles (S.I.D.P.C.) est à votre disposition pour vous apporter tout renseignement complémentaire. Je vous remercie de lui signaler, par messagerie électronique à l'adresse pref-sidpc16@charente.gouv.fr, toute difficulté éventuellement rencontrée dans la mise en œuvre de ces mesures.

Je sais pouvoir compter sur votre totale implication dans la mise en œuvre des mesures de vigilance et de protection sur le territoire de votre commune, en étroite collaboration avec les forces de l'ordre.

Pour le Préfet et par délégation,
Le Sous-préfet,
Secrétaire général,

Xavier CZERWINSKI

Principales mesures de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme

Le projet de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme a été adopté par l'Assemblée nationale et le Sénat respectivement les 11 et 18 octobre 2017. En application de l'article 10 de la Constitution, le président de la République dispose d'un délai de 15 jours, suivant la transmission au Gouvernement de la loi, pour la promulguer[7].

Les principales dispositions du texte, susceptibles d'avoir un impact sur l'application du plan VIGIPIRATE, sont les suivantes.

1 **L'établissement, par le préfet, pour une durée maximale d'un mois[8], de périmètres de protection** de nature à assurer la sécurité d'événements ou de lieux particulièrement exposés à la menace terroriste (nouvel article L. 226-1 du code de la sécurité intérieure). Les officiers de police judiciaire, les agents de police judiciaire et certains agents de police judiciaire adjoints pourront procéder, avec l'assistance éventuelle d'agents privés de sécurité ou d'agents de police municipale, à des palpations de sécurité ainsi qu'à l'inspection visuelle et à la fouille des bagages avec le consentement des personnes faisant l'objet de ces vérifications. Les personnes qui refusent de se soumettre, pour accéder ou circuler à l'intérieur de ce périmètre, aux palpations de sécurité, à l'inspection visuelle ou à la fouille de leurs bagages, ou à la visite de leur véhicule s'en voient interdire l'accès.

La prise en compte de cette nouvelle disposition dans le plan VIGIPIRATE se traduit par la création de deux nouvelles mesures : la mesure RSB 20-03 et la mesure BAT. 30-04.

2 **La fermeture administrative, par le préfet et pour une durée maximale de 6 mois, des lieux de culte** qui, par les propos qui y sont tenus, les idées ou théories qui y sont diffusées ou les activités qui s'y déroulent, provoquent à la commission d'actes de terrorisme en France ou à l'étranger, incitent à la violence ou font l'apologie de tels actes (nouvel article L. 227-1 du code de la sécurité intérieure).

La prise en compte de cette nouvelle disposition dans le plan VIGIPIRATE se traduit par la création d'une nouvelle mesure : la mesure RSB 10-04.

3 **L'extension des périmètres des contrôles d'identité (modification de l'article 78-2 du code de procédure pénale)** :

- aux abords des gares ferroviaires et routières ouvertes au trafic international pour une durée maximale de douze heures consécutives ;
- dans un rayon maximal de dix kilomètres autour des ports et aéroports constituant des points de passage frontaliers.

---

[7] La saisine du Conseil constitutionnel, dans ce délai, suspend le délai de promulgation.

[8] Sauf si la menace perdure.

La prise en compte de ces nouvelles dispositions dans le plan Vigipirate se traduit par la création de trois nouvelles mesures (FRT 10-02, AIR 30-05, MAR 30-05) et l'actualisation de deux mesures (TER 10-01, TER 20-04).

Avertissement

Les nouvelles dispositions mentionnées aux chapitres 1 et 2 sont d'application immédiate dès lors qu'elles ne nécessitent pas de dispositions réglementaires. Pour autant, leur mise en œuvre est subordonnée à la promulgation de la loi.

La nouvelle disposition visée au chapitre 3 nécessite au préalable la détermination des ports et aéroports constituant des points de passage frontaliers.

Les créations ou actualisations de mesures VIGIPIRATE mentionnées aux chapitres 1, 2 et 3 donneront lieu à une mise à jour du plan VIGIPIRATE et du catalogue de mesures associé.

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 novembre 2017)

Cette fiche traite de la protection des lieux de rassemblement ouverts au public (événements sportifs, festivals, marchés de Noël, braderies, etc.) et doit pouvoir servir de guide pratique aux organisateurs de ce genre de manifestations. Elle doit être largement diffusée. Certains des conseils délivrés ci-dessous peuvent ne pas être applicables à tous les sites. Ils doivent donc être adaptés en fonction de la configuration des lieux et du bon sens de circonstance.

1 Identifier les menaces et les vulnérabilités

Il faut d'abord évaluer la sensibilité du rassemblement en lien avec les autorités locales (préfet, maire, Police Nationale, Gendarmerie Nationale) :

- pourquoi ce rassemblement pourrait-il être ciblé par des terroristes ?
- en quoi est-il un symbole du mode de vie occidental et des valeurs de la République ?
- ce rassemblement a-t-il une couverture médiatique qui donnerait une forte visibilité à une action terroriste ?

Les différentes attaques possibles doivent être envisagées :

- jet ou dépôt d'un engin explosif à l'intérieur ou en périmétrie du site ;
- véhicule piégé en stationnement aux abords du site ;
- véhicule-bélier ;
- fusillade ou attaque suicide ;
- prise d'otage ;
- attaque à l'arme blanche.

2 Organiser la sécurité de l'événement

Il est primordial que les organisateurs de rassemblements se coordonnent avec le maire et le préfet, ainsi qu'avec les forces de police, de gendarmerie, les services de police municipale et d'incendie et de secours.

Par ailleurs, il peut être nécessaire de faire appel aux compétences de sociétés privées de sécurité pour renforcer la sécurité d'un tel événement.

2.1 - En périphérie du rassemblement

- **choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités.** Il est préférable de choisir le lieu du rassemblement de manière à limiter l'accès de véhicules (ne pas s'installer au débouché d'un axe important) ;
- **limiter ou interdire le stationnement** des véhicules aux abords immédiats du lieu du rassemblement ;
- **mettre en place une signalétique** afin d'orienter les piétons sur le lieu de l'événement et de détourner les flux de véhicules ;
- **cloisonner le flux des véhicules de l'espace de déambulation des piétons ;**
- **identifier le mobilier urbain** qui pourrait servir à dissimuler de l'explosif, le faire retirer par les autorités habilitées, en réduire l'utilisation ou mettre en place des rondes de vérification ;
- **solliciter les forces de l'ordre** ou la police municipale pour la réalisation de patrouilles, voire la mise en place de points de contrôle et de filtrage. Des agents des sociétés privées de sécurité peuvent concourir à cette mission ;
- **identifier les points de vulnérabilité hauts** (immeubles surplombant) et les sécuriser, éventuellement par une présence humaine ;
- si possible, mettre en place un système de vidéoprotection donnant, en priorité, sur les accès au site, en prenant en compte les dispositions du Code de la sécurité intérieure.

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 novembre 2017)

2.2 - Sur la périmétrie du rassemblement

- **aménager des points de contrôle ou de filtrage en nombre suffisant** aux entrées du site afin de fluidifier l'entrée du public. Leur efficacité repose sur la présence d'un superviseur, de moyens de communication et de procédures claires afin de diffuser l'alerte et de faciliter l'intervention des forces de sécurité intérieure en cas d'incident ;
- **maintenir le niveau de vigilance tout au long de l'événement mais également lors du moment sensible de sa dispersion** (le 22 mai 2017 à Manchester, au Royaume-Uni, un homme a fait détoner une charge explosive qu'il portait sur lui à la sortie de la salle de spectacle *Manchester Arena*), en rappelant régulièrement des messages de sensibilisation à destination du public (*via* la sonorisation de l'événement par exemple – « TOUS acteurs de la sécurité) » ;
- **installer une délimitation physique du périmètre extérieur** de l'événement au moyen de barrières reliées entre elles, de blocs en béton, de véhicules du comité d'organisation comme élément de barrage, etc. ;
- organiser un ou plusieurs cheminements jusqu'au point de contrôle en installant des barrières. Séparer, dans la mesure du possible, les flux entrants et les flux sortants ;
- **aménager les issues de secours en nombre suffisant** au regard de l'importance de l'événement afin de permettre une évacuation rapide du public en cas de danger à l'intérieur de la zone ;
- **organiser et contrôler les livraisons.** Prévoir des équipements mobiles permettant de bloquer physiquement les véhicules appelés à pénétrer dans le périmètre le temps de ce contrôle ;
- apposer les affiches de sensibilisation à destination du public aux points d'entrées notamment « Réagir en cas d'attaque terroriste ».

Les véhicules-béliers constituent un mode d'action terroriste de plus en plus utilisé : attentats de Nice et de Berlin en 2016, attaque contre une patrouille de militaires à Levallois-Perret et attentats en Catalogne en 2017.

Il est recommandé de mettre en place des moyens de circonstance permettant d'interdire l'accès au site ou de réduire la vitesse des véhicules à proximité des lieux de rassemblement. La mise en place de chicanes avec des obstacles successifs est également conseillée : plots en béton, bacs de fleurs de dimensions importantes, herses mobiles, barrières d'arrêt ou véhicules lourds (camions). Il est indispensable de tenir compte de la distance de pénétration potentielle d'un véhicule-bélier lors de la définition du périmètre extérieur d'un rassemblement (distance de sécurité entre les dispositifs de sécurité et la foule).

Exemple de revue de propagande de l'Etat Islamique qui préconise le recours à un véhicule-bélier.

2.3 - Au niveau des volumes intérieurs

- **désigner un responsable sûreté** qui sera l'interlocuteur unique des forces de l'ordre et des services d'incendie et de secours en cas d'intervention sur le site. Véritable coordinateur de la sûreté de l'événement, il doit connaître les bons réflexes à adopter. Il peut se rapprocher préalablement des forces de sécurité intérieure pour recueillir leurs conseils ;
- prévoir l'aménagement d'un **poste central de sûreté** au sein du site. Ce dernier doit être équipé 24H/24 par au moins un opérateur en mesure de visualiser les images du système de vidéo-protection mis en place ;
- **sécuriser la zone en période de fermeture du public** par la mise en œuvre d'un gardiennage humain ;
- **sensibiliser l'ensemble des collaborateurs au niveau de menace,** aux modes opératoires terroristes et à la détection de situations suspectes. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque.

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

PRODUITS CHIMIQUES :
SIGNALEMENT DE TOUT VOL OU UTILISATION SUSPECTE

Les derniers attentats ou actes de malveillance commis en Europe ont montré la capacité des criminels et terroristes à fabriquer des explosifs artisanaux ou des substances toxiques en utilisant des produits chimiques d'usage courant, souvent disponibles dans les magasins de bricolage, les jardineries, les grandes surfaces, etc.

Des tentatives d'attentats ont pu être déjouées grâce aux signalements de comportements ou d'achats suspects de produits chimiques (engrais, solutions de nettoyage de piscine, détachant, dissolvant, etc.).

- Novembre 2015 : **attentats de Paris** (stade de France, Bataclan) ;
- Mars 2016 : **attentats à l'aéroport de Bruxelles-Zaventen** et à la **station Maelbeek** (Belgique) ;
- Février 2017 : découverte d'un laboratoire de fabrication d'explosifs à **Montpellier** – attentat déjoué ;
- Avril 2017 : découverte d'un laboratoire de fabrication d'explosifs à **Marseille** – attentat déjoué ;
- Mai 2017 : **attentat de Manchester** (Royaume-Uni) ;
- Août 2017 : explosion d'un laboratoire de fabrication d'explosifs à **Alcanar** (Espagne) ;
- Eté 2017 : jets d'acide à **Londres** (Royaume-Uni) ;
- Août 2017: découverte d'un projet d'engin chimique à **Sidney** (Australie) ;
- Septembre 2017 : jet d'acide à **Marseille** ;
- Septembre 2017: découverte d'un **laboratoire clandestin** de fabrication d'explosifs à **Villejuif.**

Des recettes disponibles sur Internet

Un laboratoire de fabrication d'explosifs artisanaux

1 Comment détecter une utilisation suspecte de produits chimiques ?

En étant attentif à son environnement, chacun **peut détecter** la fabrication de substances permettant de commettre des attentats. Les éléments suivants, **constatés dans un lieu inapproprié, doivent vous alerter :**

- divers **produits chimiques** en quantité inhabituelle ;
- des **équipements** tels que des moyens de chauffage, des ustensiles de cuisine ou de la verrerie de laboratoire, des gants et lunettes de protection ;
- une **odeur** suspecte.

SUBSTANCES CHIMIQUES + MATÉRIELS INAPROPRIÉS (+ ODEURS) = SIGNALEMENT

2 Comment réagir et signaler ?

Si vous êtes témoin d'une utilisation suspecte de produits chimiques, **ne vous mettez pas en danger, restez discret et appelez sans délai les forces de sécurité intérieure** en composant le 17, 112 ou 114 (pour les personnes ayant des difficultés à entendre et à parler).

VIGIPIRATE

PRODUITS CHIMIQUES :
SIGNALEMENT DE TOUT VOL OU UTILISATION SUSPECTE

3 Quelles sont les obligations des professionnels qui commercialisent des produits chimiques ?

La réglementation française (*décret n°2017-1308 du 29 août 2017*) prévoit des mesures pour restreindre l'accès du grand public à des substances chimiques d'usage courant :

	Présence possible dans…	INTERDICTION de vendre aux particuliers (au delà d'une certaine concentration)	Autorisation de vendre aux particuliers avec obligation d'ENREGISTREMENT par le vendeur	
Peroxyde d'hydrogène (7722-84-1)	Produits de blanchissage, décolorants capillaires, désinfectants, agents nettoyants	> 35% p/p	de 12 < % p/p ≤ 35	**SIGNALEMENT au point de contact national (PIXAF) de tout vol, perte, disparition ou transaction suspecte**
Nitrométhane (75-52-5)	Carburants pour modèles réduits, solvants	> 40% p/p	de 30 < % p/p ≤ 40	
Acide nitrique (7697-37-2)	Décapants, traitement des métaux	> 10% p/p	de 3 < % p/p ≤ 10	
Chlorate de sodium (7775-09-9), **chlorate de potassium** (3811-04-9), **perchlorate de sodium** (7601-89-0) et **perchlorate de potassium** (77778-74-7)	Articles pyrotechniques	> 40% p/p		
Nitrate d'ammonium (6484-52-2)	Engrais, poche de froid			
Acétone (67-64-1)	Dissolvants, solvants			
Hexamine (100-97-0)	Additifs alimentaires, carburants solides pour réchauds de camping et pour moteurs à vapeur de modèles réduits			
Acide sulfurique (7664-93-9)	Déboucheurs de canalisation			
Nitrate de potassium (7757-79-1), **nitrate de sodium** (7631-99-4)	Engrais, conservateurs alimentaires			
Poudres d'aluminium (7429-90-5) et de **magnésium** (7439-95-4) **Nitrate de calcium** (10124-37-5) **Nitrate de magnésium hexahydraté** (13446-18-9)	Engrais			

Pour plus de détails, contacter le service central des armes (ministère de l'intérieur/SCA) :
sca-precurseurs-explosifs@interieur.gouv.fr

Quels critères permettent de détecter une transaction suspecte de produits chimiques à des fins malveillantes ?

Les critères suivants peuvent alerter un professionnel :

- absence d'explications cohérentes sur l'utilisation prévue des produits ;
- utilisation du produit inconnue de l'acheteur ;
- réticence à dévoiler l'utilisation du produit ;
- quantités, combinaisons ou concentrations inhabituelles de produits pour un usage domestique ;
- réticence de l'acheteur à donner les éléments nécessaires à l'enregistrement de la transaction ;
- paiement important en espèces ;
- tentative de communiquer le moins possible ;
- refus de tout produit de substitution ou de plus faible concentration.

Que faire en cas de vol, disparition ou transaction suspecte de produits chimiques réglementés ?

Les professionnels ont l'obligation de signaler tout vol, disparition ou transaction suspects au **point de contact national :**

Plateau d'Investigation eXplosifs et Armes à Feu de la Gendarmerie nationale
pixaf@gendarmerie.interieur.gouv.fr - 01 78 47 34 29 (24H/24H)

VOL ou DISPARITION ou TRANSACTION SUSPECTE = SIGNALEMENT

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

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.

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 à 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
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