AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Bonnes pratiques contre l'hameçonnage

Guide pratique technique PGSSI-S

Publication : décembre 2022 | *Classification : Publique* | *Version : v1.0*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1 OBJET DU GUIDE

Le présent guide a pour objet de proposer un ensemble de bonnes pratiques contre l'hameçonnage. Il s'adresse aux personnes responsables de l'exploitation et/ou de la sécurité des systèmes d'information des structures qui utilisent des systèmes d'information entrant dans le périmètre d'application fixé à l'article L1470-1 du code de la santé publique[1], à savoir des services numériques en santé, systèmes d'information (SI) ou services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités.

L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'utilisateur en se faisant passer pour un tiers légitime pour l'inciter à communiquer des données personnelles (identifiants de comptes, mots de passe…) et/ou bancaires. Il peut s'agir d'un faux courrier électronique, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

S'il réussit son opération, le cybercriminel pourra utiliser les données obtenues à des fins illégales telles que fraude, intrusions, spam…

Les mesures présentées dans ce guide sont principalement des mesures techniques qui peuvent être mises en œuvre au niveau des composants informatiques du système d'information, avec l'organisation requise pour les gérer.

Il est cependant essentiel de souligner que la mesure majeure pour prévenir ce type d'attaque reste la sensibilisation des utilisateurs, puisque ce sont les utilisateurs qui sont la cible immédiate de ces attaques, et que leur vigilance, si elle est effective, permet a priori de déjouer les tentatives d'hameçonnage. Une fiche de sensibilisation est disponible sur le portail https://www.cybermalveillance.gouv.fr.

Toutefois, chacun est susceptible d'un moment d'inattention, d'un clic trop rapide, ou d'être malgré tout trompé par un message d'hameçonnage très bien conçu, maquillé et se trouvant adapté au contexte personnel ou professionnel ainsi qu'à la psychologie de sa victime. Aussi des mesures techniques de filtrage doivent-elles être mises en place comme lignes de défenses complémentaires permettant d'éviter aux utilisateurs d'être dérangés par des messages d'hameçonnage qui constituent à la fois un risque et une nuisance pour le travail de l'utilisateur.

Ce sont ces différentes mesures qui sont proposées par le guide.

Elles sont organisées en trois sections :

- Les mesures de prévention ;
- Les mesures de détection ;
- Les mesures de réaction.

Suivant le principe de défense en profondeur, il est recommandé que des mesures de chacune de ces trois catégories soient mises en œuvre.

[1] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464

Pour chaque mesure ou groupe de mesures proposées, il est indiqué dans un cadre à gauche, reproduit ci-dessous pour exemple, de haut en bas :

1
C1
R2

- Le **niveau global de priorité de mise en œuvre** pour la recommandation : de 1 (le plus prioritaire) à 4, qui découle de la combinaison des deux indicateurs suivants ;
- L'estimation du **niveau relatif de complexité et/ou de coût de mise en œuvre** de la mesure : de C1 pour les complexités et/ou coûts les moins élevés parmi les mesures proposées, à C3 pour les complexités et/ou coûts les plus élevés :
  - C1 : paramétrage simple à effectuer ou non technique,
  - C2 : paramétrage nécessitant des compétences ou logiciel peu coûteux,
  - C3 : paramétrage complexe ou nécessitant des compétences avancées, ou matériel/logiciel spécifique et/ou potentiellement coûteux ;
- L'estimation du **niveau relatif de réduction du risque** apporté par la mise en œuvre de la mesure : de R1 pour les réductions les moins élevées du risque parmi les mesures proposées, à R3 pour les réductions les plus élevées du risque.

Chaque niveau est également associé à une couleur dans une échelle classique allant du vert (le plus souhaitable) au rouge (le moins souhaitable, mais souhaitable tout de même).

Note : le niveau de réduction du risque apporté par la mise en œuvre d'une mesure est estimé sur la base de son potentiel fonctionnel, mais également sur son degré de généralisation dans Internet dès lors qu'elle requiert de multiples acteurs pour être efficace. Par exemple, signer électroniquement un message peut être efficace dans l'absolu, mais ne sert pas à grand-chose si aucun des destinataires ne vérifie que les messages reçus sont signés et valides.

Il est souligné que toutes les mesures présentées sont recommandées et devraient être appliquées quand rien ne s'oppose à leur mise en œuvre. Le niveau global de priorité de mise en œuvre peut être utilisé pour établir un plan d'action de mise en œuvre graduelle des mesures, planifié en fonction des ressources de la structure.

En outre, le guide se limite aux mesures concernant spécifiquement l'hameçonnage. Il suppose que les mesures de base de bonne sécurisation des systèmes d'information sont appliquées. Par exemple, il n'évoque pas l'utilisation d'antivirus, mesure bien évidemment impérative mais sortant du strict cadre de ce guide.

Pour des informations pratiques plus larges de sécurisation des systèmes d'information de santé, le lecteur peut consulter le portail Cyberveille Santé https://www.cyberveille-sante.gouv.fr/ (Espace documentaire) ainsi que les différents guides proposés dans le cadre de la PGSSI-S sur la page dédiée d'esante.gouv.fr.

2 MESURES DE PREVENTION

2.1 Sensibilisation des personnels

1 C1 R3	► Diffuser largement la fiche sur l'hameçonnage disponible sur https://www.cybermalveillance.gouv.fr. ► Sensibiliser les utilisateurs concernant les comportements à adopter face aux messages frauduleux. Les modules d'apprentissage en ligne et les vidéos mis à disposition sur la plateforme de formation e-santé (https://esante-formation.fr) dans la section « Sécurité opérationnelle des SI », et en particulier les modules intitulés « Gérer ses mails en toute sécurité » et « Identifier les arnaques par email » peuvent contribuer à cette sensibilisation. ► Intégrer l'utilisation des sites web d'entrainement (ex : https://phishingquiz.withgoogle.com) dans la sensibilisation des utilisateurs.

3 C3 R3	► Mener régulièrement des exercices avec des fausses campagnes de phishing. Des outils tels que *Gophish* (outil libre) peuvent être mis en place à cette fin (voir https://getgophish.com).

2.2 Au niveau du service de réception des courriels externes

Le service de réception des courriels externes est celui désigné par l'enregistrement MX dans le DNS pour le ou les domaines utilisés.

1 C1 R3	► Analyser systématiquement les messages (contenu et pièces jointes) avec un logiciel permettant la détection des pourriels (« anti-spam »).

1 C1 R3	► Activer le contrôle SPF sur les courriels entrants (RFC 7208, voir https://fr.wikipedia.org/wiki/Sender_Policy_Framework).

2 C2 R3	► Activer le « Greylisting » (voir https://fr.wikipedia.org/wiki/Greylisting) sur les courriels entrants. Attention à bien identifier préalablement les adresses courriel techniques (*abuse@ , contacts DNS/opérateur…*) ou d'urgence pour lesquelles un délai de réception pourrait être gênant et dont les messages à leur adresse pourraient être exemptés de ce mécanisme. ► Compléter le « Greylisting » en activant le « Greytrapping » sur les courriels entrants. Le principe est de « faire fuiter » des adresses courriel dont la seule finalité est de piéger les envois des pourriels et autres courriels malveillant provenant d'émetteurs inconnus. Quand un émetteur inconnu a été placé temporairement en Greylist et qu'il envoie un courriel à une de ces adresses « pièges », il est automatiquement mis en liste noire pour un certain durée (typiquement 24h).

2 C2 R3	► Activer l'usage de listes noires DNS « DNSBL / DNS Black Listing » (voir https://fr.wikipedia.org/wiki/DNS_Black_Listing) et d'IP Blocklist (*ex :* *https://mailspike.org*) sur les courriels entrants. Si besoin, prendre en compte les domaines et/ou adresses IP éventuels desquels il est critique de pouvoir recevoir des messages malgré leur apparition potentielle dans ces listes. ► Mettre en place un contrôle vérifiant que le domaine dans l'adresse indiquée par le champ Reply-To du courriel, s'il est présent, est identique à celui du champ From.

2 C2 R3	► Mettre en place une vérification des URL dans le contenu des courriels : • En s'appuyant sur des listes noires (*ex : https://urlhaus.abuse.ch/api/*) ; • En vérifiant que le domaine qui apparait à la lecture est identique à celui du lien réel (attribut href du lien dans du code html) ; • En filtrant certains domaines non souhaitables, par exemple sur la base de pays ou d'autres extension à risque (*ex : ".xyz"*) et pour lesquels il n'y a a priori pas de raison de recevoir des courriels légitimes ayant ces origines.

2 C2 R3	► Configurer l'ajout d'une bannière spécifique en tête de tout message d'origine externe afin de rappeler à l'utilisateur d'être vigilant face à un éventuel courriel d'hameçonnage. Exemple de bannière : *Ce courriel est envoyé par un expéditeur extérieur à <nom de la structure>.* *Si vous n'êtes pas en mesure de garantir que son contenu est sûr et cohérent avec son origine, NE CLIQUEZ SUR AUCUN LIEN et N'OUVREZ AUCUNE PIECE-JOINTE. Celle-ci pourrait renfermer un contenu malveillant. De même si le message est en provenance d'un expéditeur inconnu ou qui devrait être un expéditeur interne. En cas de doute, transmettez le courriel suspect à l'adresse alerte.securite.informatique@domaine.de.la.structure* Le texte et la couleur de la bannière peuvent être modifiés de temps en temps afin de conserver la vigilance des utilisateurs.

3 C3 R3	► Adapter des règles de classification (« *scoring* ») par défaut pour pondérer les différents critères de détection mentionnés dans ce chapitre en fonction du contexte et décider de la stratégie d'acceptation ou de mise en quarantaine (voire du rejet) des messages analysés ; ► Suivre régulièrement les résultats du *scoring* et faire évoluer les règles en fonction des faux positifs et faux négatifs (retours obtenus dans le cadre des mesures de détection).

3 C2 R2	► Activer la vérification de signature DKIM sur les courriels entrants (RFC 6376, voir https://fr.wikipedia.org/wiki/DomainKeys_Identified_Mail). Il est important de noter que l'absence de signature valide attendue ne doit pas (toujours) être rédhibitoire : des serveurs de messagerie intermédiaires (notamment les serveurs de mailing list) sont susceptible de « casser » la signature. Mais une signature valide peut, par exemple, être imposée pour les origines connues et supposées toujours signer. Ce point est à prendre en compte sous forme de pondération dans le scoring global du message. ► Activer la gestion DMARC sur les courriels entrants (RFC 7489, voir https://fr.wikipedia.org/wiki/DMARC et https://dmarc.org/). Cette mesure nécessite l'activation préalable des vérifications SPF et DKIM pour les courriels entrants.

3 C3 R3	► En alternative au « Greylisting » (voir plus haut), utiliser un système de vérification anti-robot lors d'un premier courriel d'un expéditeur inconnu du récepteur, qui consiste par exemple à renvoyer un message contenant un lien web à activer pour que les messages issus de cette nouvelle adresse soient acceptés. Attention dans ce cas à bien consolider l'inventaire des besoins et leur suivi dans la durée, afin d'exempter de cette vérification certains émetteur ou adresses destination, si elle s'avère problématique, comme elle pourrait potentiellement l'être pour : • Des messages légitimement envoyés par des automates qui ne seront pas en mesure d'activer eux-mêmes le lien web initial, • Des adresses courriel techniques (*abuse@ , contacts DNS/opérateur…*) ou d'urgence pour lesquelles un délai de réception pourrait être gênant.

Recommandations générales :

- Privilégier la mise en quarantaine ou en dossier "spam" plutôt que la suppression pure et simple des messages suspects pour gérer le risque de faux positifs par un examen manuel de ces messages et permettre les investigations en cas d'incident.
- Une liste blanche ne doit être utilisée dans un filtre que selon le principe « tout est interdit sauf ce qui est dans la liste blanche » et non pas « tout doit être vérifié sauf ce qui est dans la liste blanche ».
- Une liste blanche au niveau d'un filtre ne doit pas permettre d'éviter les autres filtres. Par exemple :
  - Ce n'est pas parce qu'un message provient d'un utilisateur interne qu'il peut être considéré comme exempt de virus ;
  - Ce n'est pas parce qu'un message provient apparemment d'un organisme partenaire que l'adresse de l'émetteur n'a pas été usurpé, voire que le serveur de messagerie de cet organisme n'a pas été piraté et utilisé par des cybercriminels à fin d'hameçonnage.

  Ainsi, une liste blanche ne doit jamais être utilisée selon le principe « tout ce qui est dans la liste blanche est directement autorisé sans passer par les autres vérifications ».

2.3 Au niveau du serveur de messagerie

1 C1 R3	► S'il existe des adresses courriel qui constituent des listes de diffusion vers un nombre important d'utilisateurs, en restreindre l'usage (par contrôle d'accès) à un nombre très limité d'utilisateurs. ► Interdire les courriels externes à destination de telles adresses de diffusion.

4 C3 R1	► Journaliser et centraliser des logs permettant une analyse forensique (*nom des pièces jointes, URL contenues, login/IP du poste client...*)

2.4 Au niveau des postes utilisateurs (accès internes ou nomades)

2 C2 R3	► Si le client de messagerie le permet, le paramétrer pour qu'il affiche les messages en texte simple (« plain text »). Ce paramétrage ne doit pas être modifiable par les utilisateurs (*paramétrage par GPO ou équivalent*). ► A défaut ou en complément, si le client de messagerie le permet, le paramétrer pour que les hyperliens présents dans les messages ne soient pas cliquables. Ce paramétrage ne doit pas être modifiable par les utilisateurs (*paramétrage par GPO ou équivalent*).

3 C3 R3	► Si les postes nomades peuvent accéder directement à Internet sans passer par un proxy web sortant de la structure, mettre en œuvre une solution Endpoint sur ces postes qui permette le filtrage d'URL afin qu'ils disposent d'un filtrage identique à celui appliqué aux flux Internet des postes internes. ► Si aucun proxy web sortant n'est mis en œuvre pour la structure, mettre en œuvre une solution Endpoint sur l'ensemble des postes pour permettre, entre autres, le filtrage d'URL.

2.5 Au niveau du webmail (accès depuis Internet)

2 C2 R3	► Si le webmail le permet, le paramétrer pour qu'il affiche les messages en texte simple (« plain text »). Ce paramétrage ne doit pas être modifiable par les utilisateurs (paramétrage par GPO ou équivalent). ► A défaut ou en complément, si le webmail le permet, le paramétrer pour que les hyperliens présents dans les messages ne soient pas cliquables. Ce paramétrage ne doit pas être modifiable par les utilisateurs (*paramétrage par GPO ou équivalent*).

2 C2 R3	► Privilégier l'authentification forte des utilisateurs (*par exemple : double facteurs tels que mot de passe + FIDO U2F ou mot de passe + Google Authenticator, certificat électronique protégé par mot de passe…*).

3 C3 R3	► Limiter les connexions depuis des adresses IP étrangères qui n'ont pas de raison d'être utilisées par les utilisateurs légitimes du service. Attention à bien prendre en compte les éventuels besoins de mobilité à l'étranger et autres situations spécifiques potentielles (*déplacements professionnels, astreintes, situations frontalières, usages de VPN…*) dans la décision de mise en œuvre de cette mesure et dans son paramétrage.

2.6 Au niveau du service d'émission des courriels

Les mesures qui suivent visent :

- À réduire le risque que des courriels légitimes émis par la structure soient classés comme pourriel par des services de messagerie destinataires ;
- À permettre aux services de messagerie tiers d'améliorer leur capacité à identifier les pourriels et courriels malveillants qui usurperaient l'identité de la structure.

Le niveau de réduction du risque permis par les mesures de ce chapitre est estimé dans ce sens.

1 C1 R3	► S'assurer que des enregistrements DNS permettant la résolution inverse (adresse IP vers nom DNS) de type PTR sont bien configurés pour les adresses IP publiques du service d'émission de courriel et pour celles du service de réception (MX) de courriel. L'absence de tels enregistrements peut causer le rejet des messages, voire l'inscription des adresses IP concernées dans des listes noires. ► Eviter d'émettre des messages qui indiquent dans les champs "From" et "Reply-To" des adresses de messagerie dans des domaines différents de celui de la structure.

1 C1 R3	► Utiliser régulièrement les services web disponibles pour analyser la sécurité de la configuration du système de messagerie (tel que visible depuis Internet), comme par exemple : • https://ssi.economie.gouv.fr/courriel • https://mxtoolbox.com/ • https://www.hardenize.com/

2 C2 R3	► Mettre en place un enregistrement DNS SPF qui liste les noms et/ou adresses IP publique de tous les serveurs légitimes à émettre des courriels pour la structure (RFC 7208, voir https://fr.wikipedia.org/wiki/Sender_Policy_Framework). Les services de messageries des tiers auront alors la possibilité de bloquer les tentatives d'envois par des serveurs illégitimes usurpant l'identité de votre structure. Attention à bien lister tous les serveurs légitimes émettant des courriel (ex : penser aux prestataires des campagnes d'e-mailing).

3 C2 R2	► Activer la signature DKIM des courriels sortants (RFC 6376, voir https://fr.wikipedia.org/wiki/DomainKeys_Identified_Mail)

3 C2 R2	► Définir et publier une politique DMARC pour les courriels sortants (RFC 7489, voir https://fr.wikipedia.org/wiki/DMARC et https://dmarc.org/). Il est important de faire évoluer la stratégie publiée relative aux messages non conformes reçus par les tiers, afin de valider le bon paramétrage du dispositif et la prise en compte adéquate dans SPF et DKIM des différents serveurs qui émettent légitimement des courriels pour le domaine. La stratégie initiale sera typiquement le reporting seul des anomalies, puis une fois une confiance suffisante acquise dans le bon fonctionnement du dispositif, une stratégie de mise en quarantaine. Après une nouvelle phase de validation supplémentaire, la stratégie de rejet pourra être adoptée et publiée si elle semble utile. Cette mesure nécessite l'activation préalable de SPF et DKIM pour les courriels sortants.

4 C3 R2	► Activer DNSSEC pour les domaines DNS utilisés par la structure afin de permettre un haut niveau de confiance dans les informations DNS diffusées. La fiabilité du service DNS est d'autant plus importante que de nombreux dispositifs de sécurité, dont SPF et DKIM, s'appuient sur les informations qu'il diffuse pour leurs prises de décision. (voir https://fr.wikipedia.org/wiki/Domain_Name_System_Security_Extensions et https://www.afnic.fr/fr/produits-et-services/services/dnssec-18.html).

2.7 Au niveau du proxy web sortant

1 C1 R3	► Bloquer les requêtes contenant des URL (pour les requêtes HTTP) ou vers des serveurs (pour les requêtes HTTPS) présents dans des listes noires (*ex : https://urlhaus.abuse.ch/api/*).

3 C2 R1	► Journaliser le paramètre "Referer" des requêtes web sortant vers Internet : il pourra éventuellement permettre d'identifier l'origine d'une connexion suspecte (provenant de l'utilisation de la messagerie).

3 MESURES DE DETECTION

3.1 Au niveau du service de réception des courriels externes

1 C1 R3	► Surveiller l'espace de quarantaine de la messagerie peut permettre d'identifier des campagnes de pourriels, voire d'hameçonnage, en cours.

3 C2 R2	► Surveiller l'apparition dans les listes noires publiques (DNSBL, IP blocklists) des domaines ou IP de correspondants légitimes habituels afin : • D'alerter les utilisateurs d'accroitre leur vigilance sur les messages de cette provenance ; • De surveiller plus activement les mises en quarantaine pour débloquer d'éventuels messages légitimes ayant cette provenance ; • D'être plus attentif à une éventuelle campagne d'attaques sectorielle.

3.2 Au niveau du serveur de messagerie

1 C1 R3	► Surveiller quotidiennement les flux anormaux de réception et d'envoi de courriels, par exemple le « top 20 » des courriels les plus diffusés en réception et en émission, les statistiques de supervision de la congestion de la file d'attente. *Une telle surveillance quotidienne d'un « top 20 » en réception des courriels sur l'ensemble d'un CHU et en émission de courriels depuis une seule boite mail du CHU a permis de détecter de nombreuses campagnes de phishing ainsi qu'une compromission de compte utilisateur.*

1 C1 R3	► Mettre en place une adresse courriel interne permettant aux utilisateurs de remonter les courriels suspects au responsable sécurité (avec l'entête et tous les éléments nécessaires), ou, à défaut, de notifier le responsable sécurité d'un tel événement. ► Mettre en place et relever les notifications sur l'adresse abuse@<domaine de la structure>. ► Si une politique DMARC est définie, également mettre en place une adresse courriel dédiée (ou utiliser abuse@ le cas échéant) et relever les rapports DMARC.

3.3 Au niveau des postes utilisateurs (accès internes ou nomades)

3 C2 R2	► Si disponible, mettre en place un module sur le client de messagerie qui permette à l'utilisateur de remonter simplement les courriels suspects au responsable sécurité (avec l'entête et tous les éléments nécessaires). ► Si possible, afin de faciliter cette opération pour utilisateur, mettre en place un bouton lui permettant de transférer automatiquement le message suspect vers la boite dédiée à cet usage.

3.4 Au niveau du webmail (accès depuis Internet)

2 C2 R3	► Surveiller les connexions d'adresses IP étrangères sur le webmail. ► Analyser les logs permettant d'identifier l'utilisateur éventuellement ciblé par ces connexions pour vérifier avec lui s'il n'a pas été victime d'un phishing.

3.5 Au niveau du service d'émission des courriels

1 C1 R3	► Vérifier régulièrement si l'IP du service d'émission de courriels (SMTP sortant) n'est pas black-listée en utilisant le protocole DNS (Black Listing) (*Voir par exemple https://www.dnsbl.info/dnsbl-database-check.php, http://www.mailspike.net/iplookup.html*) ► Consulter régulièrement les statistiques DMARC pour identifier les usurpations du nom de domaine ► Mettre en place une alerte et/ou surveiller l'espace de quarantaine des message sortants qui peut permettre d'identifier une compromission de compte ou de poste.

3.6 Au niveau du proxy web sortant

2 C2 R3	► Mettre en place une alerte et/ou surveiller les logs du proxy web sortant pour repérer des événements tels que, par exemple : • Blocage d'URL potentiellement dangereuse ; • Téléchargement suspect ; • URL complexe accédée sans aucun Referer.

4 MESURES DE REACTION

Les mesures proposées dans ce chapitre s'appliquent quand un message ou une campagne d'hameçonnage sont détectés, quand de tels messages sont remontés par les utilisateurs au service sécurité, ou encore quand il est suspecté que des comptes ou postes utilisateurs ont été compromis suite à la réception de tels messages.

Il est important de souligner que le niveau de priorité indiqué pour les mesures proposées est la priorité pour leur adoption dans la gestion de crise, et non pas la priorité de leur exécution en cas crise : cette priorité n'indique en rien l'ordre des actions à effectuer en cas d'incident.

Les mesures retenues sont typiquement intégrées sous forme de procédure à des Fiches Réflexes à appliquer en cas d'attaque par hameçonnage.

4.1 Organisation

1 C1 R3	► Alerter les équipes informatiques : messagerie, postes de travail, support utilisateur… ► Informer les utilisateurs de la campagne d'hameçonnage en cours et leur rappeler le comportement à suivre ; ► En cas d'incident « grave » de sécurité des systèmes d'information, déclarer l'incident au ministère de la santé sur le portail des signalements des événements sanitaires indésirables https://signalement.social-sante.gouv.fr ; ► Alerter les tiers éventuellement concernés.

3 C2 R2	► Contribuer à la lutte contre l'hameçonnage en signalant les attaques à la communauté d'Internet : • https://www.signal-spam.fr/ • https://phishtank.com/ • Si l'attaque utilise des adresses d'un domaine apparemment usurpé, en informer l'organisation concernée ou l'hébergeur du domaine (adresse abuse@ ou adresse de contact spécifique …)

4.2 Au niveau du service de réception des courriels externes

2 C2 R3	► Adapter les règles de classification (« *scoring* ») pour renforcer les critères correspondants aux messages en cause et s'assurer qu'ils soient mis en quarantaine, quitte à augmenter temporairement le taux de faux positifs ► Si les messages d'hameçonnage comportent des éléments très spécifiques (atypiques ou uniques), mettre en place des filtres correspondants pour une mise en quarantaine directe sur ces critères (dans les entêtes : adresse IP émettrice, User-Agent, From, Reply-To, autres entêtes spécifiques, URI ou mots clés dans le corps du message…)

4.3 Au niveau du serveur de messagerie

2 C2 R3	► Identifier les comptes de messagerie ayant reçu et ouvert les messages d'hameçonnage ; ► Désactiver les comptes potentiellement compromis puis changer leur mot de passe, ainsi que ceux des comptes des autres services externes s'il y a potentiellement une réutilisation de ces mots de passe ; ► Désactiver temporaire le webmail et les autres services externes s'il y a potentiellement une réutilisation des mots de passe tant que tous les comptes compromis ne sont pas identifiés et remis en état de sécurité ; ► Vérifier que la compromission se limite au compte de messagerie, qu'elle ne vient pas du poste de travail et qu'elle ne s'est pas étendue aux postes de travail ou aux autres ressources partageant éventuellement le même mot de passe ; ► Vérifier qu'aucune redirection (ou script de redirection) n'a été paramétrée.

3 C2 R2	► Utiliser une console d'administration de la messagerie, ou à défaut mettre en place des scripts, permettant de supprimer facilement l'ensemble des mails de phishing identiques sur l'ensemble des boîtes de messagerie de la structure.

4.4 Au niveau du service d'émission des courriels

1 C1 R3	► Bloquer l'émission de messages vers les adresses d'attaquants identifiées (adresses issues des champs From et Reply-To).

4.5 Au niveau proxy web sortant

1 C1 R3	► Bloquer les tentatives d'accès HTTPS et HTTP aux serveurs identifiés comme malveillants dans le cadre de l'attaque par hameçonnage sur la base de leur nom DNS ; ► S'il s'avère que l'attaque emploie des URL avec une adresse IP pour la partie « host » : • Bloquer les tentatives d'accès HTTPS et HTTP vers cette adresse, sous réserve qu'elle ne change pas fréquemment (cas d'un TTL court pour la résolution IP), • Voire bloquer temporairement toute tentative d'accès HTTPS et HTTP à une URL dont la partie « host » est formée par une adresse IP.

Annexe 1 : Glossaire

Sigle / Acronyme	Signification
ANS	Agence du Numérique en Santé
CHU	Centre Hospitalier Universitaire
DKIM	*DomainKeys Identified Mail*
DMARC	*Domain-based Message Authentication, Reporting and Conformance*
DNS	*Domain Name System*
DNSBL	*DNS Black Listing*
DNSSEC	*Domain Name System SECurity extensions*
FIDO	*Fast IDentity Online alliance*
GPO	*Group Policy Objects*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
IP	*Internet Protocol*
MX	*Mail eXchanger* (type d'enregistrement DNS)
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PTR	*domain name PoinTeR* (type d'enregistrement DNS)
RFC	*Request for comments*
SPF	*Sender Policy Framework*
U2F	*Universal Second Factor*
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*