AGENCE DU NUMÉRIQUE EN SANTÉ

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

Note d'information sur les supports de sensibilisation à la cybersécurité (fiches, guides, webinaires, …)

CERT Santé

Statut : Validé | *Classification : Publique* | *Version : 1.0*

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

SOMMAIRE

1 A PROPOS DE CETTE NOTE

Cette note fait un premier état des lieux des supports de sensibilisation/formation à la cybersécurité disponibles pour les structures de santé (fiches, guides, webinaires …).

Les outils de sensibilisation recensés sont adaptés au secteur de la santé ou génériques en fonction d'une cible de population donnée ou de contenu.

Au regard de la diversité des contenus recensés, il semble opportun de proposer aux acteurs du secteur un point d'entrée unique, au travers par exemple du portail du CERT sectoriel ou de la plateforme de formation https://esante-formation.fr/ .

2 CERT SANTE

Le CERT Santé propose des contenus riches au sujet de la cybersécurité dans le secteur de la santé au lien suivant : https://www.cyberveille-sante.gouv.fr/accueil.

Les contenus sont destinés aux utilisateurs du numérique dans les structures, aux directions, aux responsables informatiques ainsi qu'aux opérationnels de la sécurité.

A. Fiches sur les menaces cyber et guides de bonnes pratiques de sécurité

Les fiches rédigées par type de menace cyber regroupent des actions urgentes à réaliser en cas d'incident mais aussi des recommandations de mesures proactives afin de protéger les systèmes d'information (SI) vis-à-vis de ces menaces.

Les sujets abordés sont multiples, et plutôt techniques (comme par exemple la prévention contre les maliciels, l'hameçonnage, les attaques par déni de services).

Les guides sont, quant à eux, destinés à renforcer la sécurité des SI afin d'augmenter sa résilience face à tout type de menace. Le périmètre de ces guides est large puisqu'on y trouve notamment des recommandations en matière de sensibilisation à la sécurité des mots passe, mais aussi de gestion des habilitations en encore un guide des mécanismes de protection de l'intégrité des données stockées.

B. Webinaires sur la cybersécurité et le CERT Santé

Les webinaires permettent d'aborder, sous un format plus interactif et vivant, l'état de la menace cyber, les principales mesures de prévention, mais aussi de présenter les activités du CERT Santé, et en particulier les actions d'appui à la réponse aux incidents à la prévention.

Les derniers webinaires sont accessibles à partir de https://esante.gouv.fr/ans/webinaire/ .

C. Vidéos de sensibilisation à la cybersécurité

Ces vidéos d'information et de formation abordent différents thèmes tels que la PGSSI-S et la sécurité opérationnelle (signaler un incident, présentation du portail cyberveille-santé, gestion des mots de passe, gestion des messages malveillants, etc…).

Elles sont accessibles à partir de https://esante-formation.fr/ .

3 GCS E-SANTE – GRADES PAYS DE LA LOIRE

Plusieurs GRADeS mènent des actions de sensibilisation à la cybersécurité. Le GCS E-Santé Pays de La Loire a une expérience particulière dans ce domaine et propose différents supports de sensibilisation à la sécurité des SI, en particulier pour les personnels des structures de santé.

A. Fiches sur les menaces cyber

Elles sont téléchargeables selon différents formats au lien suivant : https://www.esante-paysdelaloire.fr/media-files/3774/affiches-ssi-web.pdf .

B. Escape Game de sensibilisation aux risques numériques

Fruit d'un partenariat entre quatre structures régionales et un industriel, le GCS e-santé Pays de la Loire propose un Escape Game où les personnes formées s'impliquent et deviennent actives dans l'apprentissage. La diffusion de l'outil s'effectue au travers d'une formation à la mise en œuvre et à l'animation des sessions de jeu.

Pour plus d'information : https://www.esante-paysdelaloire.fr/nos-services/securite-numerique-en-sante-99-114.html

4 GIP CYBERMALVEILLANCE

Le portail cybermalveillance (https://www.cybermalveillance.gouv.fr/) est dédié aux particuliers, entreprises, associations, collectivités et administrations victimes de cybermalveillance. Les contenus sont destinés aux utilisateurs du numérique ainsi qu'aux responsables informatiques.

A. Fiches sur les menaces cyber et guides de bonnes pratiques de sécurité

Les fiches ont pour but de permettre la compréhension des cybermenaces et d'avoir les clés pour réagir à celles-ci (comme par exemple la fiche « La fraude à la carte bancaire » ou bien encore « Le phishing », mais aussi « la défiguration d'un site internet » par exemple).

Quant aux guides, ils exposent des bonnes pratiques à adopter afin de renforcer la protection cyber en amont de toute attaque. Ils couvrent différentes thématiques : les bonnes pratiques relatives à toutes les menaces, ou bien précisément relatives aux données, aux emails, aux ordinateurs, aux sites web, aux tablettes ou encore aux téléphones.

B. Aide au diagnostique de l'acte de malveillance et identification d'un prestataire de confiance

Ce dispositif permet de conseiller et orienter les victimes de cybermalveillance en réalisant un diagnostic du problème rencontré et en apportant des conseils adaptés pour y remédier. Il permet également à la personne qui réalise le diagnostic d'être orientée vers un professionnel de proximité référencé par le dispositif.

5 CNIL

La CNIL propose des contenus spécifiques à la protection des données personnelles. Ces informations sont disponibles au lien suivant : https://www.cnil.fr/. Elles sont destinées aux utilisateurs du numérique ainsi qu'aux responsables informatiques. Elles concernent en particulier les responsables de traitement quel que soit le contexte de manipulation des données.

A. Fiches sur les menaces et guides de bonnes pratiques de protection des données

La CNIL propose un grand nombre de fiches explicatives concernant différents sujets : la réglementation concernant la protection des données à caractère personnel, la mise en conformité RGPD et les pouvoirs de la CNIL, mais aussi la protection des données à caractère personnel dans des contextes particuliers (telle que le travail, la santé, l'open data, etc), ou encore l'application des principes de protection dans l'usage de technologies particulières (comme par exemple l'intelligence artificielle, la cybersécurité, ou les cookies et autres traceurs).

B. Formation certifiante

Un MOOC est disponible sur le site de la CNIL. Destinée à un public large, cette formation d'environ 20 heures permet d'aborder l'ensemble des points couverts par la réglementation de protection des données personnelles. Elle est disponible au lien suivant : https://atelier-rgpd.cnil.fr/

6 ANSSI

L'ANSSI propose un contenu spécialisé dans la cybersécurité accessible au lien suivant : https://www.ssi.gouv.fr/ . Les contenus sont destinés aux utilisateurs du numérique, aux responsables informatiques et en particulier aux opérationnels de la sécurité.

A. Fiches sur les menaces cyber et guides de bonnes pratiques de sécurité

Le site de l'ANSSI propose trois espaces : l'un est dédié aux administrations, l'autre aux entreprises et le dernier aux particuliers.

Pour chaque espace, des fiches de « Précautions élémentaires » sont disponibles. On trouve également des Guides de bonnes pratiques, plutôt à destination d'un public expert la cybersécurité (opérationnels), et qui abordent diverses thématiques (cryptographie, poste de travail & serveurs, réseaux, applications web, etc.).

B. Formation certifiante

L'ANSSI propose de suivre un MOOC de découverte des thématiques de la cybersécurité. Cette formation dure entre 24 et 32 heures et est destinée à un public large. Elle est disponible au lien suivant : https://www.secnumacademie.gouv.fr/