Les médecins et pharmaciens demandent au prochain gouvernement d'investir dans la **cybersécurité**

Notre grande enquête cybersécurité dans les soins de santé révèle que la majorité des médecins et pharmaciens (84%) estime que le soutien des professionnels et des institutions de santé en matière de cybersécurité doit être une priorité du prochain gouvernement. Ils réclament une augmentation du budget cybersécurité alloué aux hôpitaux et des primes cybersécurité pour les praticiens non-hospitaliers.

VINCENT CLAES

Un participant sur cinq (19%) à notre grande enquête cybersécurité a été victime d'un cybercrime durant les six dernières années. Les francophones sont plus nombreux que les néerlandophones à le déclarer (24% vs 12%).

Quelles sont (dans l'ordre décroissant) les attaques auxquelles ces médecins généralistes, spécialistes et pharmaciens ont dû faire face?

- Phishing: tentative de vol de données ou d'accès aux comptes bancaires via un email, un sms ou un appel téléphonique: 55%
- Hacking: accès non-autorisé au système informatique : 54%
- Sabotage informatique: destruction, blocage, effacement des données informatiques: 45%
- Rançonnage: demande d'une rançon pour pouvoir récupérer des données qui ont été bloquées par un rançongiciel: 45%
- Cyberharcèlement: harcèlement en ligne via email ou messages: 21%.

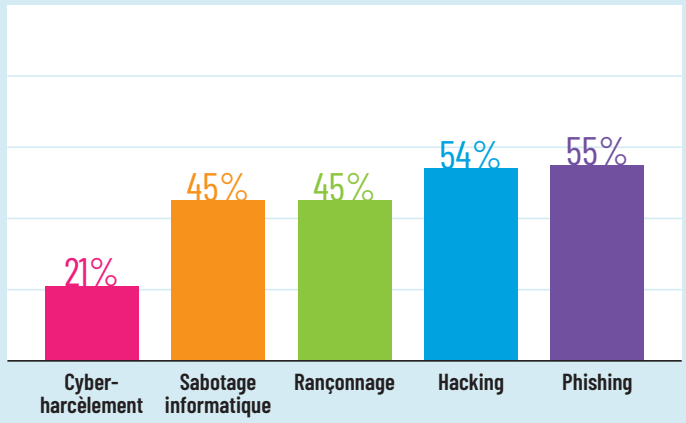
La sécurité informatique de leur activité professionnelle est une préoccupation permanente pour la moitié d'entre eux. Un tiers estime néanmoins que «c'est un problème pour leur service IT et leur informaticien», pas pour eux. Les pharmaciens sont davantage de cet avis que les médecins (49% vs 18%).

Augmenter le budget pour la cybersécurité

Huit répondants sur dix estiment que le soutien des professionnels de santé en matière de cybersécurité doit être une priorité pour le prochain gouvernement, qui doit élaborer un plan d'actions concrètes, et que les autorités fédérales doivent augmenter le budget consacré à la cybersécurité dans les hôpitaux.

Rappelons qu'en 2023, le gouvernement fédéral avait prévu un budget de 15 millions d'euros pour l'ensemble des hôpitaux. Ce qui est peu par rapport aux 130 millions d'euros que le CFEH conseille d'investir de façon structurelle. Fin avril, Frank Vandenbroucke a débloqué un budget non structurel de 39,5 millions d'euros pour que les hôpitaux puissent se munir d'une meilleure cybersécurité. «*Les hôpitaux sont de plus en plus les cibles de cyberattaques, comme cela a encore été démontré au cours de l'année écoulée. Les investissements dans la cybersécurité pour protéger au mieux les données des patients et assurer la disponibilité des soins sont essentiels*», a déclaré le ministre de la Santé.

Les médecins et pharmaciens qui ont été victimes ces 10 dernières années de cybercrime ont été confrontés à des actes de :



- **cyberharcèlement :** harcèlement en ligne via email ou messages
- **sabotage informatique :** destruction, blocage, effacement des données informatiques
- **rançonnage :** demande d'une rançon pour pouvoir récupérer des données qui ont été bloquées par un rançongiciel
- **hacking :** accès non-autorisé au système informatique
- **phishing :** tentative de vol de données ou d'accès aux comptes bancaires via un email, un sms ou un appel téléphonique

PAS DE PLAN DE GESTION DE CRISE

Les médecins et pharmaciens sont-ils prêts à gérer une cyberattaque?
Sur papier, cela ne semble pas être le cas. Ils sont peu nombreux (moins de 15%) à avoir élaboré des plans de gestion de crise, de communication, de reprise et de continuation de l'activité. Reconnaissons que ce sont généralement les grosses structures qui ont les moyens d'élaborer préventivement ces processus structurés.

61% des participants à notre enquête savent qui ils peuvent contacter au sein de leur structure professionnelle (hôpital, cabinet de groupe, officine…) s'ils sont victimes d'une cyberattaque. La majorité de ces derniers dispose des coordonnées (téléphone, email) de cette personne.

Par contre, les médecins et pharmaciens sont moins capables d'identifier le responsable du plan de continuité informatique en cas d'attaque ou d'incendie. Seuls 45% des néerlandophones et 27% des francophones savent qui exerce cette fonction.

JSS6881F

MIEUX PROTÉGER LES PROFESSIONNELS DE LA SANTÉ DES COMMENTAIRES MALVEILLANTS

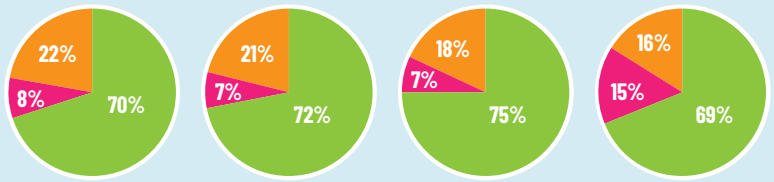
75% des participants à notre enquête demandent que les autorités prennent une réglementation spécifique pour protéger les professionnels de la santé des commentaires malveillants postés sur les réseaux sociaux et sites de référencement des prestataires de soins. Les spécialistes hospitaliers - plus exposés à des commentaires sur les réseaux sociaux - sont plus nombreux à réclamer cette mesure (77%) que les généralistes (73%) ou les pharmaciens (68%).
Dans nos colonnes, plusieurs médecins avaient déjà fait part de leur exaspération face à des avis négatifs à leur encontre publiés sur des sites internet.

La majorité des médecins et pharmaciens (79%) trouve que les autorités fédérales doivent allouer une prime cybersécurité aux praticiens non-hospitaliers (médecins généralistes (70%), spécialistes extra-hospitaliers (75%) et pharmaciens (72%) pour mieux protéger les données de santé. Les francophones et les spécialistes en formation sont plus demandeurs de cette aide que les néerlandophones (83% Vs 73%), de même que pour l'augmentation du budget fédéral cybersécurité (89% Vs 64%).

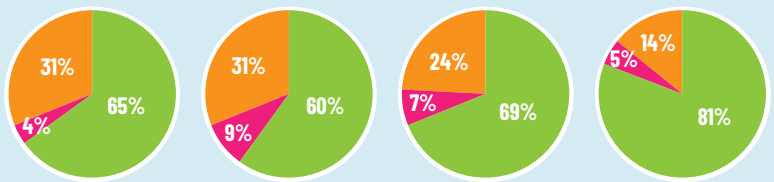
On ne s'étonnera pas d'apprendre qu'un répondant sur deux considère que le médecin ou le pharmacien ne peut pas être tenu responsable d'une faille de sécurité concernant les données de leurs patients. Les pharmaciens sont un peu plus nombreux que les généralistes (56% vs 46%) a être opposés à cette responsabilisation. Globalement, 30% des répondants sont tout de même prêts à endosser cette responsabilité.

Les autorités fédérales doivent-elles: Oui Non Sans réponse

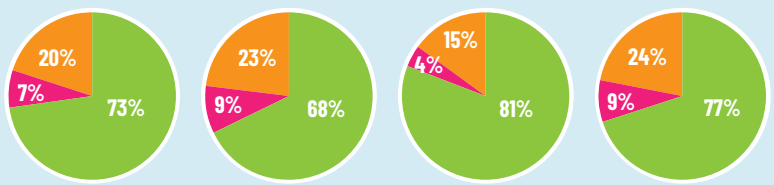
Allouer une prime cybersécurité aux praticiens non hospitaliers ?



Augmenter le budget cybersécurité des hôpitaux ?

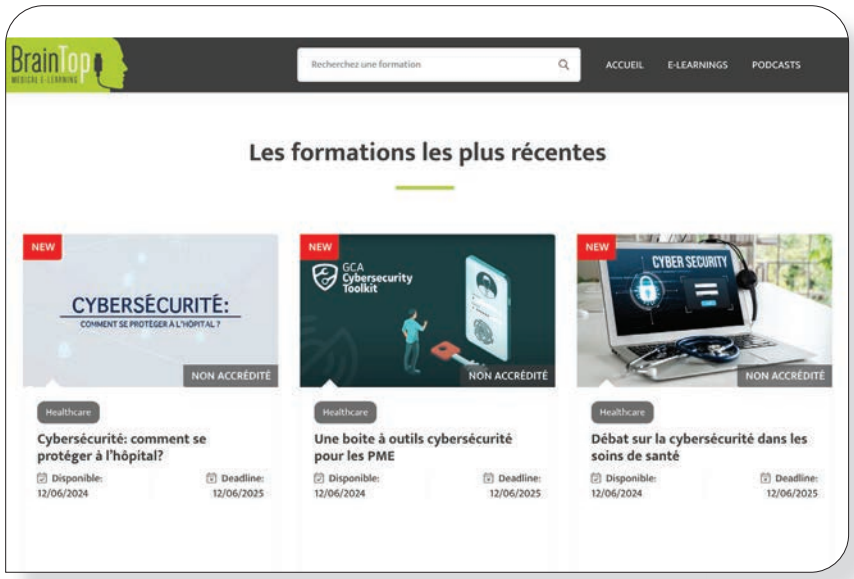


Prendre une réglementation spécifique pour protéger les professionnels de la santé des commentaires malveillants postés sur les réseaux sociaux et les sites de référencement ?

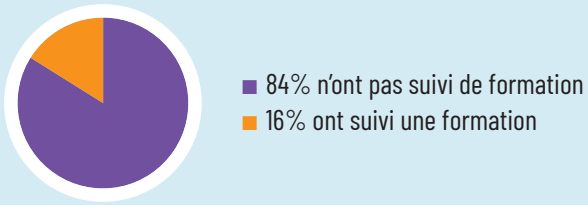


Une volonté manifeste de se former à la cybersécurité

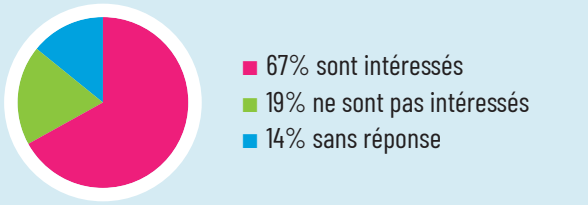
67% des répondants à notre enquête veulent se former à la cybersécurité. Afin de répondre à cette attente, nous proposons sur notre site BrainTop des vidéos d'information et de formation sur la cybersécurité.



Combien de médecins et pharmaciens ont-ils suivi une formation en cybersécurité ces 5 dernières années ?



Combien de médecins et pharmaciens aimeraient suivre une formation en cybersécurité ?



Les médecins et pharmaciens se forment-ils spécifiquement pour prévenir les risques de cybercriminalité? Actuellement, c'est encore rare. Huit répondants sur dix ne l'ont pas fait durant les cinq dernières années. Ce n'est pas une preuve de désintérêt puisque 67% des répondants se déclarent être prêts à suivre une formation. Un engouement qui démontre tout l'intérêt de notre initiative visant à publier des vidéos et des articles de formation et d'information sur la cybersécurité sur notre site BrainTop et sur les sites de nos médias.

Notre rédaction a réalisé quatre vidéos vous permettant d'en savoir plus sur la protection numérique:

- **Cybersécurité: comment se protéger à l'hôpital?**

Une interview de Sabrina Cristofano, présidente du Groupe cybersécurité de Gibbis et Chief Information Security Officer et Data Protection Officer au CHU Brugmann

- **Cybersécurité: comment obtenir un prêt pour mieux protéger sastructure de soins?**

Une interview de Lara Collard, Investment Manager chez Wallonie Santé

- **Cybersécurité: comment réagir face à une cyberattaque**?

Une interview de Didier Delval, CEO du CHwapi

- Un **débat-vidéo sur la cybersécurité dans les soins de santé** réunissant Dieter Goemaere (Gibbis), Peter Fontaine (Cliniques de l'Europe), Mathieu Lardinois (SkyForce) et Nina Hasratyan (Agence du Numérique).

Vous trouverez également sur notre site une présentation de la **Boîte à outils cybersécurité pour les petites et moyennes entreprises** réalisée par la Global Cyber Alliance (GCA) et l'Agence du Numérique.

Ces vidéos sont visibles sur notre plateforme BrainTop.

Découvrez nos formations
https://tinyurl.com/2me2bpw3

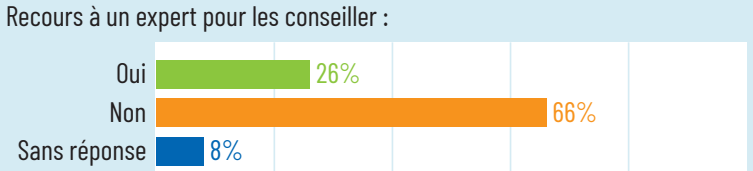
Avec le soutien de

Cyberwal by digital wallonia
Wallonie Relance
SKYFORCE CYBER SECURITY

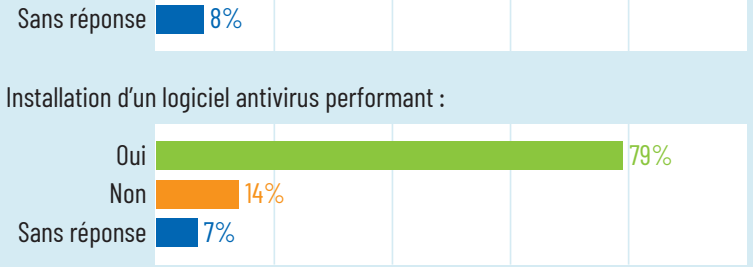
AUGMENTATION DE L'INVESTISSEMENT PERSONNEL

Quelles sont les mesures prises ces 5 dernières années par les médecins et pharmaciens pour se protéger contre les cyberattaques ?

Souscription d'une assurance spécifique cybersécurité :



Recours à un expert pour les conseiller :



Installation d'un logiciel antivirus performant :

Un répondant sur deux a investi durant les cinq dernières années dans des solutions informatiques et du matériel pour mieux protéger son activité contre les cyberattaques. Ces médecins et pharmaciens ont donc dû délier les cordons de leur bourse pour s'équiper. 83% des répondants ont augmenté en 2004 leur budget consacré à la cyberprotection de entre 0 et 50%; et 13% de 51% à 100%.

Quelles mesures prennent concrètement les médecins et les pharmaciens pour se protéger contre la cybercriminalité? Durant ces 5 dernières années, 79% des répondants ont installé un logiciel antivirus performant. Par contre, ils sont nettement moins nombreux (26% du côté FR et 41% du côté NL) à avoir demandé à un expert/une entreprise de les conseiller sur la manière de protéger le plus efficacement possible leur système informatique.

S'assurer spécifiquement contre les conséquences d'une cyberattaque ne fait pas encore partie des habitudes des médecins et des pharmaciens. Seuls 6% des répondants l'ont fait récemment.

Un tiers des participants à notre enquête (33% du côté NL et 42% du côté FR) utilise un réseau privé virtuel (VPN) pour communiquer. Près de huit répondants sur dix déclarent communiquer de façon électronique avec leurs patients. La moitié des néerlandophones le font via une messagerie sécurisée de santé pour un cinquième seulement des francophones.

MS15227BF

Mots de passe, sauvegarde et double authentification

Les professionnels de santé changent-ils régulièrement les mots de passe de leurs appareils informatiques professionnels (ordinateurs, applications ou sites web)? Notre enquête révèle que 61% des répondants ne le font pas systématiquement.

Lorsqu'ils le changent c'est (par ordre décroissant) parce qu'ils reçoivent une alerte de sécurité (23%) ou que le responsable informatique de l'institution le leur demande (20%).

Un tiers (28%) ne les changent jamais. Les généralistes semblent être moins prudents que les spécialistes et les pharmaciens puisque 44% d'entre eux ne changent jamais pour 28% des spécialistes et des pharmaciens. Ce n'est pas très étonnant puisqu'un tiers des pharmaciens et des spécialistes hospitaliers déclarent le faire à la demande du responsable informatique de leur institution.

Quid des mises à jour des programmes utilisés dans l'activité professionnelle? La majorité (72%) fait confiance à ses appareils qui font des mises à jour automatiques. Les alertes poussent 22% des répondants à mettre leurs programmes à jour. 5% le font quand ils y pensent et 1% ne le font jamais.
La majorité (63%) des sauvegardes des données sont réalisées de façon automatique. Les néerlandophones privilégient la sauvegarde automatique par rapport aux francophones (69% vs 57%). Un cinquième des répondants font encore de façon manuelle les sauvegardes à un rythme régulier.

Les généralistes préfèrent le cloud au disque local sécurisé pour stocker leurs données médicales (68% vs 19%). À l'inverse des spécialistes qui privilégient le serveur local sécurisé (43%) au cloud (19%).

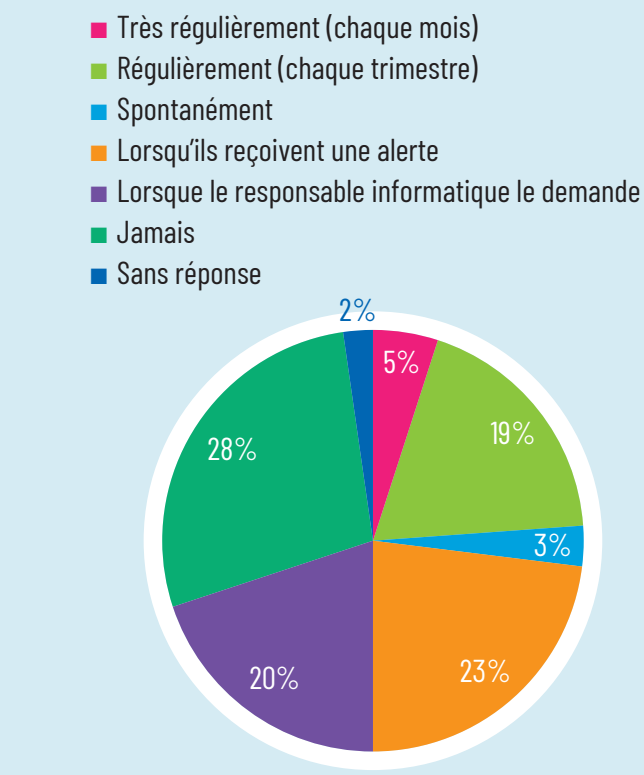
Il est toutefois étonnant de constater qu'un cinquième des répondants ne savent pas où leurs données sont stockées.

Une des manières de sécuriser les appareils électroniques est d'utiliser une double authentification. 52% des répondants néerlandophones ont déjà adopté cette pratique pour seulement 38% des francophones.

Ceux qui utilisent cette double authentification le font (par ordre décroissant) via une application spécifique, l'utilisation d'un code envoyé par SMS et la réception d'une notification.

Découvrez les réactions à notre enquête sur www.lespecialiste.be

Á quel rythme les médecins et pharmaciens changent-ils les mots de passe de leurs appareils informatiques professionnels ?



PLUS D'INFORMATIONS SUR LES DISPOSITIFS MÉDICAUX

Les pirates s'introduisent parfois dans les systèmes informatiques via des dispositifs médicaux. Pour huit répondants sur dix à notre enquête, les producteurs de dispositifs médicaux connectés doivent mieux communiquer sur les failles informatiques potentielles de leurs produits et doivent proposer une formation spécifique lors de la vente sur la cybersécurité de leurs dispositifs médicaux. Les médecins sont plus demandeurs de cette transparence et de cet accompagnement que les pharmaciens.

NIS2: UNE DIRECTIVE MÉCONNUE

La majorité des répondants (92%) à notre enquête n'ont jamais entendu parler des normes européennes liées à la directive NIS2 (sécurité de l'information) qui entreront en vigueur en octobre 2024 et concerneront les entreprises de plus de 50 employés ou réalisant un chiffre d'affaires annuel de plus de 10 millions d'euros. Seulement 6 répondants sur les 903 ont été impliqués dans des réunions de travail pour implémenter ces normes dans leur institution. Il est donc grand temps pour les structures de soins de sensibiliser les médecins aux implications du passage à NIS2.

MÉTHODOLOGIE

- Enquête en ligne réalisée via les médias *Le Spécialiste*, *Medi-Sphere* et *Pharma-Sphere*
- Période de l'enquête: janvier-avril 2024
- Nombre de répondants: 903 (59% hommes / 41% femmes)
  - Médecins généralistes: 38%
  - Spécialistes hospitaliers: 34%
  - Spécialistes extra-hospitaliers: 19%
  - Pharmaciens: 9%
- Distibution géographique du lieu d'exercice (cabinet ou officine): Flandre (40%), Bruxelles (11%) et Wallonie (49%).

MS152270F