# Hackers ou comment s’en protéger


**Le piratage est devenu une industrie à part entière. Pour ce prémunir devant ces « professionnels » et éviter le pire, il faut avant tout travailler sur l’anticipation, car la sécurité se passe tout d’abord en amont afin de garder une marche d’avance sur les hackers… C’est ce que nous allons voir dans ce deuxième chapitre consacré au piratage informatique.**

Voir également : Hackers, les maîtres du monde

**Pascal Wolff –** *Le Cardiologue n° 447 – juillet-août 2022*

La numérisation des données s’est considérablement développée ces dernières années, et les interconnexions entre  les différentes parties (professionnels, patients, téléconsultations, entreprises de données, etc.) ont bondi de manière exponentielle. Les attaques virtuelles ont bien évidemment suivis cette évolution qui n’en est qu’à ses débuts.

Jusqu'à présent, et sans en prendre une réelle conscience, les hackers faisaient le buzz dans le vol des données. Et ce n'est pas les grandes entreprises, mondialement connues, qui étaient les plus protégées. Facebook par exemple, s'est fait subtiliser une base de données de 533 millions d'utilisateurs en 2019. À l'époque, l'entreprise avait affirmé avoir résolu le problème. Seulement, nouvelle fuite en 2021… Les utilisateurs n'ont jamais été prévenus *(voir encadré ci-dessous et visitez le site* havebeenpwned.com*)*. Les vols massifs ont également eu lieu dans de nombreux hôpitaux. Cependant, aucune attaque n'a, à ce jour, visé à la désorganiser le système de soins français, même si la moitié des incidents déclarés ont bel est bien… désorganisé les structures.

Que cherchent ces voleurs de données ? C'est tout d'abord le business avec ses profits qui ont développés cette guerilla informatique, même si l'on n'oublie pas que des équipes gouvernementales (de tout pays) ont des spécialistes très aiguisés en la matière.

Les angles d'attaque des hackers sont orientés vers les entrées que nous leurs « offrons », à savoir les failles organisationnelles, physiques techniques et humaines.

## LES ANGLES D'ATTAQUE

### L'hameçonnage. Le grand classique

L'hameçonnage, ou pishing, consiste à envoyer des e-mails dans le but d'obtenir des informations personnelles. Cette technique implique soit une pièce jointe chargeant un logiciel malveillant sur votre ordinateur dès que vous l'ouvrez, soit en utilisant un lien pointant vers un (faux) site web vous incitant à télécharger des logiciels malveillants (voir Le Cardiologue 446) ou à transmettre des renseignements personnels (numéro de carte bleue, mots de passe…).

Vérifiez tout d'abord la connexion du site qui doit être en https. Si le chiffrement des données transmises est une bonne chose grâce à ce « s » de http, cela signifie juste que les informations échangées entre votre navigateur et le site visité ne

sont pas accessibles à des tiers, mais ne veut pas dire que le site est sûr, le certificat délivré ne dit rien du site lui-même. Une page d'hameçonnage peut tout à fait avoir ce certificat et chiffrer le trafic qui circule entre vous et lui.

### L'harponnage. L'usurpateur

Le harponnage, ou spear phishing, est un type de hameçonnage utilisant les adresses-mails pour cibler les individus et les entreprises. C'est à partir de messages personnels et pertinents que le harponnage peut être difficile à identifier. L'un des moyens les plus utilisés est l'usurpation d'une adresse électronique d'une personne que vous connaissez. « Hello, regarde la photo jointe et dis-moi ce que tu en penses… » suffit passer du côté obscur, tout comme une soit-disante commande de 352,00 euros dont l'opérateur a perdu votre adresse, ou votre banque qui vous envoie un message pour vérifier la mise à jour de votre profil. Généralement, le courriel usurpe l'identité d'une personne morale (établissement bancaire, service public…) ou d'une personne physique (travail, famille, ami…) dans le but d'ouvrir une pièce jointe ou de cliquer sur un lien qui vous dirige vers un site malveillant. Une fois la « proie » cernée, l'attaquant prend le contrôle du système d'information. On parle ici « d'infiltration ».

Il est facile aujourd'hui de copier un site « officiel » et de le rendre ainsi utilisable à des fins d'escroquerie. Nombreux sont les sites affichant une colonne à droite « Accès client » visant à vous faire remplir vos nom d'utilisateur et mot de passe.
Si vous avez un doute, rendez-vous directement sur le site en question avec votre propre adresse. Vous pouvez également survolez les liens avec votre curseur. Si vous voyez par exemple http//l.mail.hsbc.fr pour un message reçu de la banque hsbc, vous ne pouvez que passer votre chemin et pourtant le mail est envoyé de l'adresse contact@mail.hsbc.fr qui vous paraît pourtant véritable. Il faut faire preuve d'esprit critique en déchiffrant l'URL.

## L'ANTICIPATION, LA RÈGLE D'OR DE LA PRÉVENTION

Si la cybercriminalité a touché essentiellement les grands groupes, les cabinets médicaux, et donc les médecins, ne sont plus épargnés par ce phénomène. Les attaques se sont multipliées dans les petites structures car celles-ci ne sécurisent pas efficacement leurs données sensibles. Le Cnom a confirmé que les médecins sont particulèrement concernés, la protection des données s'articulant avec le secret professionnel. Un guide a d'ailleurs été rédigé entre le Cnom et la Cnil afin de vérifier la mise en conformité avec le RGPD.

La base de la prévention est tout d'abord matérielle avec la sécurisation du système informatique (serveur professionnel externe, wifi sécurisé, sauvegardes interne Raid et externe, mots de passe régulièrement renouvelé, verrouillage en système de veille, antivirus mis à jour, VPN).

Ensuite, toute personne ayant accès aux données du cabinet doit être conscient des risques et leur comportement doit être l'allier d'une extrême vigilance… n'hésitez pas à faire une formation à ce sujet. Insérer une clause dans les contrats sur le respect du secret et de la confidentialité. L'anonymisation des données, les envois sécurisés via messagerie cryptée, suppression des messageries gmail, des réceptions de fichier via Wetransfer, vérification hebdomadaire de vos adresses-mail (voir encadré)… tout ceci doit faire partie du comportement de chacun afin de limiter au maximum les attaques.

Enfin, travaillez en amont en pensant que si vous arrivez un matin et que votre informatique est bloquée à cause d'une attaque, quels sont vos angles de recours (et de secours).

## Comment savoir si vos adresses mails n'ont pas été piratées

**Le site haveibeenpwned.com (littéralement « je me suis fait avoir ») qui est la référence ou l'Institut Hass-Platner Institut à Berlin (HPI ). Vous pouvez ainsi voir si votre e-mail ou votre numéro de portable ont fuité ou ont été volés dans des bases de données.**

### Que faire en cas de piratage ?

Vous devez impérativement et sans délai modifier votre mot de passe, voire de supprimer votre compte si les attaques ont été multiples. Mais de manière générale, tous vos mots de passe doivent être changé régulièrement, et – cela va de soi –chaque compte ne doit pas avoir le même mot de passe.

# LES DIX RÈGLES D'OR DE LA PRÉVENTION

## LEURS APPLICATIONS SONT ESSENTIELLES !

 **Les usages informatiques à caractère personnel de ceux à caractère professionnel doivent être strictement séparés.** Cela concerne les courriels, les comptes d'échange de fichiers, les clés USB ou tout support informatique (disques durs…).
 **Les mises à jours doivent être faits régulièrement (personnels et professionnels).** Faites en sorte d'automatiser les mises à jour sur vos machines. Si elles ne peuvent pas l'être, vérifier les ponctuellement ou acceptez les immédiatement si des messages vous les propose.
 **Vos accès aux différents services doivent être protégés par des mots de passe complexes.** Ils doivent être sans informations personnelles, uniques et bien sûr à ne divulguer en aucune manière. La règle principale : un mot de passe par support.
Si vous pouvez le faire, protégez vos accès par une authentification à double-facteur (ou vérification en deux étapes) lorsque c'est possible. Par exemple, le site sur lequel vous vous connectez vous envoie un code à usage unique sur votre smartphone.
 **Surveillez vos équipements lors de vos déplacements.** Cette surveillance vous protégera des manipulations à votre insu.
 **Lorsque vous devez vous absenter, protégez votre espace de travail et donc vos données.** Mettez un code de sécurité sur vos machines si c'est possible. Placez en lieu sûr tout matériel connecté (disques durs, clés usb…) et si possible coupez votre internet.
 **Votre identité numérique doit être divulguée avec parcimonie sur internet et les réseaux sociaux.** Si vous devez par exemple donner votre adresse mail une seule fois ou si vous n'êtes pas sûr d'un site, créez une adresse fictive et temporaire sur un hébergeur dédié tel YOPmail (Your Own Protection mail) qui est un serveur de messagerie électronique temporaire et gratuite.

 **Protégez vos messageries professionnelle et personnelle.** Avant d'ouvrir une pièce jointe, soyez sûr à 100 % de votre émetteur et ne cliquez pas sur les liens qui vous semblent douteux.
 **Protégez-vous des réseaux extérieurs non maîtrisés** pour connecter vos équipements (réseaux ou bornes de recharge USB publics, prêt d'un ordinateur…).
 **La visioconférence est devenu une mane pour les hackers.** Passez par des sociétés reconnues. La confidentialité des conversations n'est pas assurée sur les réseaux publics.
 **Évitez de prendre votre smartphone lors de réunions sensibles.** Il peut être très facilement utilisé pour enregistrer vos conversations, y compris à votre insu.



# Vérifiez vos adresses mails !

**Il n'y a pas que votre ordinateur qui peut être piraté. Vos adresses mails on pu être subtilisées dans d'autres bases de données (Santé, Gafam, réseaux sociaux…). Pour le savoir et éviter une usurpation de votre identité, de l'hameçonnage ou autre méfait, vérifiez auprès du site haveibeenpwned s'il y a eu violation de vos adresses. Si tel est le cas, le site vous indique sur quels sites vos données ont été volées… et changez vos mots de passe.**

# la CNIL et vos données

**Le médecin libéral doit donc protéger ses données personnelles et médicales. Pour ce faire, il doit passer par des protocoles précis : hébergement certifié données de Santé avec demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).**

**La CNIL a récemment sanctionné deux médecins libéraux pour ne pas avoir suffisamment protégé les données de leurs patients, des milliers**

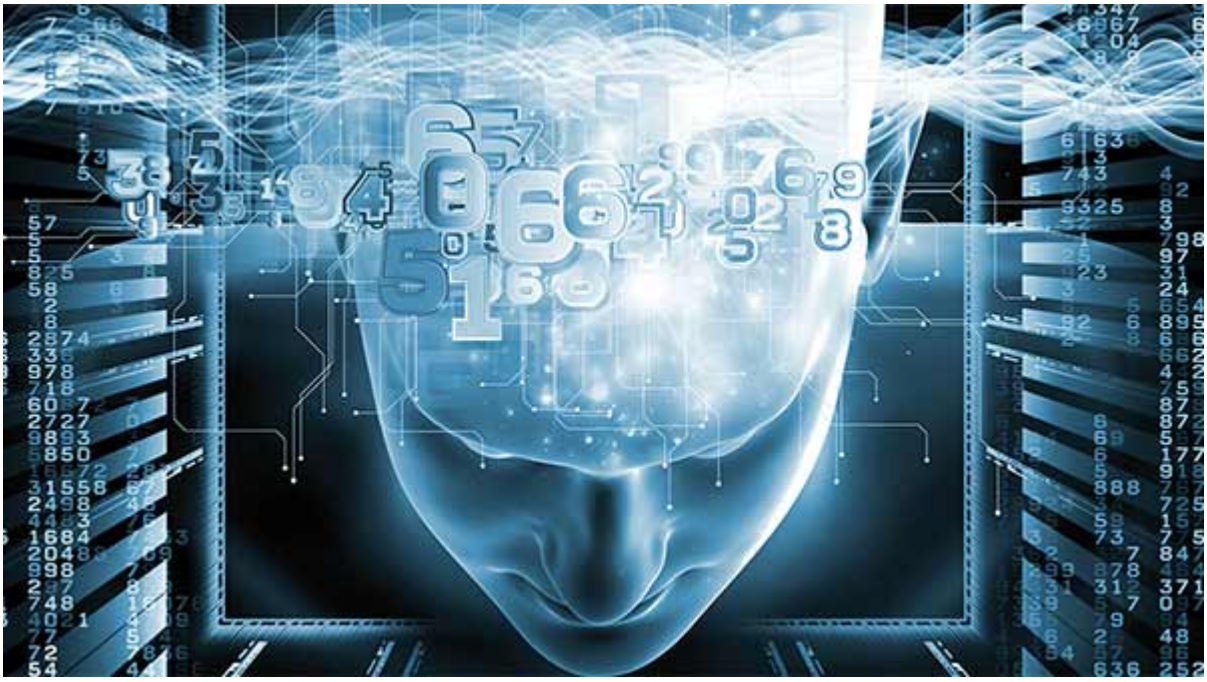
**d’images médicales hébergées sur des serveurs étaient en accès libre. Toutes ces données pouvaient donc être consultées et téléchargées, et étaient, selon les délibérations de la CNIL, « *suivies notamment des nom, prénoms, date de naissance et date de consultation des patients* ». Le problème venait simplement d’un mauvais paramétrage de leur box internet et du logiciel d’imagerie qui laissait en libre accès les images non chiffrées.**

# A lire également

Cybersécurité – banalisation sur toile

Intelligence artificielle – la santé au cœur du futur

L’intelligence artificielle – Introduction à la Santé

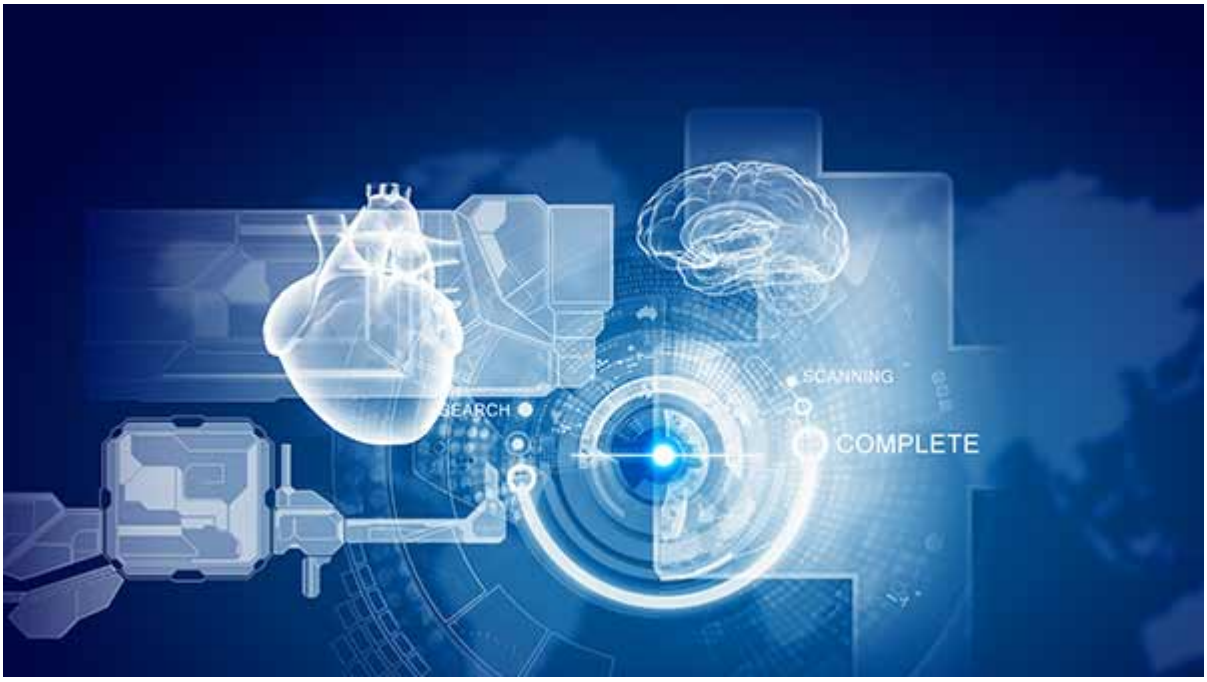


Les préoccupations liées à l’intelligence artificielle


Les 50 ans d’internet

Les virus

De l’impression 3D à la bio-impression




Retour vers le futur – les prédictions médicale dans les années 1950

## LES NFT, C'EST QUOI EXACTEMENT ?

Les jetons non fongibles (NFT) sont des certificats de propriété stockés sur une blockchain. Ces jetons numériques permettent de certifier l'authenticité d'un objet qui lui est associé en achetant un code (ou un certificat)

Contrairement à la monnaie telle qu'on la connaît (ou aux cryptomonnaies), chaque NFT est unique ou non fongible, c'est-à-dire qu'il ne peut être échangé contre quelque chose de valeur égale.

Le marché de l'art est en pleine révolution grâce aux NFT. Mike Winkelmann (Beeple) a vendu une photo numérique pour plus de 69 millions de dollars chez Christie's. Et pourtant, cette photo est consultable et téléchargeable sur internet, contrairement à un tableau « réel ». Alors, pourquoi acheter une telle œuvre de cette manière ? Et bien tout simplement parce que celle-ci a été vendue avec son NFT qui la rend unique et traçable. Ce certificat signe bien sûr l'œuvre de l'artiste et indique qui l'a vendue, qui l'a achetée et pour quelle somme et à quelle date. Cette œuvre « numérique » peut donc être cédée en enchère… et si la valeur de la cryptomonnaie qui a permis d'acquérir le certificat NFT augmente, la valeur de cette œuvre augmentera  pour le possesseur du NFT.