Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…)| Denis JACOPINI

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Denis JACOPINI

Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse…* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. **Dès lors, plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui vérouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien vérrouiller son ordinateur, etc…

Article original de Denis JACOPINI et Atlantico

Réagissez à cet article

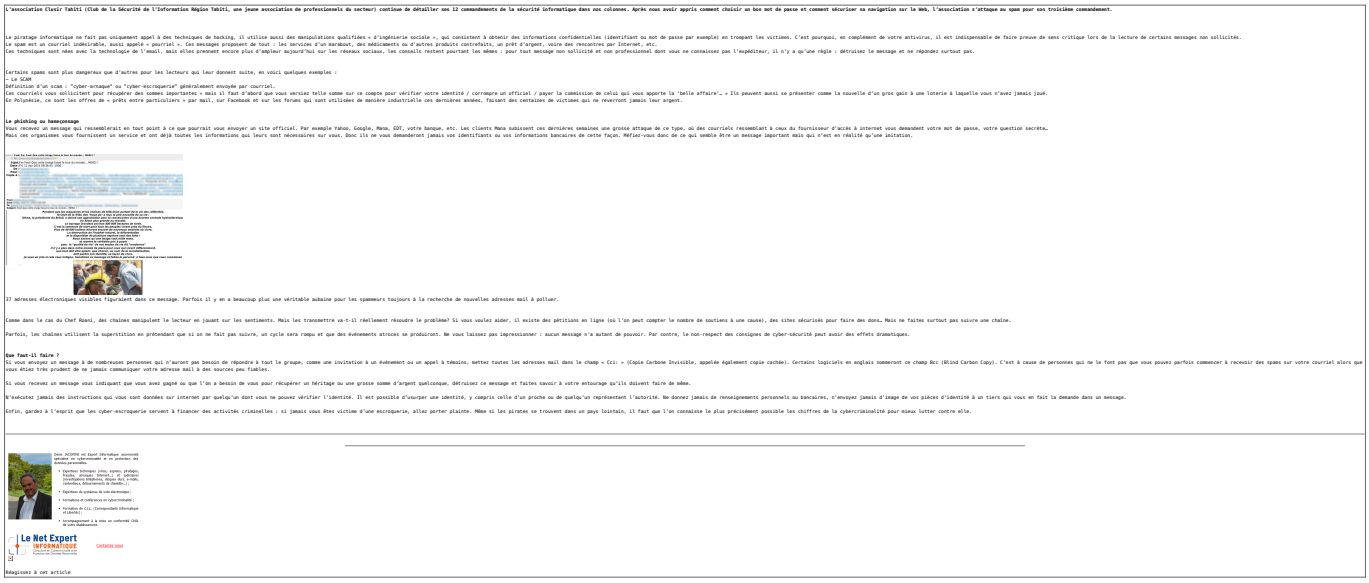
Original de l’article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Atlantico.fr

---

Ne relayez pas les spams, canulars, chaînes de lettres… | Denis JACOPINI

2

Ne relayez pas les spams, canulars, chaînes de lettres…



L'association Clusir Tahiti (Club de la Sécurité de l'Information Région Tahiti, une jeune association de professionnels du secteur) continue de détailler ses 12 commandements de la sécurité informatique dans nos colonnes. Après nous avoir appris comment choisir un bon mot de passe et comment sécuriser sa navigation sur le Web, l'association s'attaque au spam pour son troisième commandement.

Le piratage informatique ne fait pas uniquement appel à des techniques de hacking, il utilise aussi des manipulations qualifiées « d'ingénierie sociale », qui consistent à obtenir des informations confidentielles (identifiant ou mot de passe par exemple) en trompant les victimes. C'est pourquoi, en complément de votre antivirus, il est indispensable de faire preuve de sens critique lors de la lecture de certains messages non sollicités.
Le spam est un courriel indésirable, aussi appelé « pourriel ». Ces messages proposent de tout : les services d'un marabout, des médicaments ou d'autres produits contrefaits, un prêt d'argent, voire des rencontres par Internet, etc.
Ces techniques sont nées avec la technologie de l'email, mais elles prennent encore plus d'ampleur aujourd'hui sur les réseaux sociaux, les conseils restent pourtant les mêmes : pour tout message non sollicité et non professionnel dont vous ne connaissez pas l'expéditeur, il n'y a qu'une règle : détruisez le message et ne répondez surtout pas.

Certains spams sont plus dangereux que d'autres pour les lecteurs qui leur donnent suite, en voici quelques exemples :
– Le SCAM
Définition d'un scam : "cyber-arnaque" ou "cyber-escroquerie" généralement envoyée par courriel.
Ces courriels vous sollicitent pour récupérer des sommes importantes « mais il faut d'abord que vous versiez telle somme sur ce compte pour vérifier votre identité / corrompre un official / payer la commission de celui qui vous apporte la 'belle affaire'… » Ils peuvent aussi se présenter comme la nouvelle d'un gros gain à une loterie à laquelle vous n'avez jamais joué.
En Polynésie, ce sont les offres de « prêts entre particuliers » par mail, sur Facebook et sur les forums qui sont utilisées de manière industrielle ces dernières années, faisant des centaines de victimes qui ne reverront jamais leur argent.

Le phishing ou hameçonnage
Vous recevez un message qui ressemblerait en tout point à ce que pourrait vous envoyer un site officiel. Par exemple Yahoo, Google, Mana, EDT, votre banque, etc. Les clients Mana subissent ces dernières semaines une grosse attaque de ce type, où des courriels ressemblant à ceux du fournisseur d'accès à internet vous demandent votre mot de passe, votre question secrète…
Mais ces organismes vous fournissent un service et ont déjà toutes les informations qui leurs sont nécessaires sur vous. Donc ils ne vous demanderont jamais vos identifiants ou vos informations bancaires de cette façon. Méfiez-vous donc de ce qui semble être un message important mais qui n'est en réalité qu'une imitation.

17 adresses électroniques visibles figuraient dans ce message. Parfois il y en a beaucoup plus une véritable aubaine pour les spammeurs toujours à la recherche de nouvelles adresses mail à polluer.

Comme dans le cas du Chef Raoni, des chaines manipulent le lecteur en jouant sur les sentiments. Mais les transmettre va-t-il réellement résoudre le problème? Si vous voulez aider, il existe des pétitions en ligne (où l'on peut compter le nombre de soutiens à une cause), des sites sécurisés pour faire des dons… Mais ne faites surtout pas suivre une chaine.

Parfois, les chaines utilisent la superstition en prétendant que si on ne fait pas suivre, un cycle sera rompu et que des événements atroces se produiront. Ne vous laissez pas impressionner : aucun message n'a autant de pouvoir. Par contre, le non-respect des consignes de cyber-sécurité peut avoir des effets dramatiques.

Que faut-il faire ?
Si vous envoyez un message à de nombreuses personnes qui n'auront pas besoin de répondre à tout le groupe, comme une invitation à un événement ou un appel à témoins, mettez toutes les adresses mail dans le champ « Cci: » (Copie Carbone Invisible, appelée également copie cachée). Certains logiciels en anglais nommeront ce champ Bcc (Blind Carbon Copy). C'est à cause de personnes qui ne le font pas que vous pouvez parfois commencer à recevoir des spams sur votre courriel alors que vous étiez très prudent de ne jamais communiquer votre adresse mail à des sources peu fiables.

Si vous recevez un message vous indiquant que vous avez gagné ou que l'on a besoin de vous pour récupérer un héritage ou une grosse somme d'argent quelconque, détruisez ce message et faites savoir à votre entourage qu'ils doivent faire de même.

N'exécutez jamais des instructions qui vous sont données sur internet par quelqu'un dont vous ne pouvez vérifier l'identité. Il est possible d'usurper une identité, y compris celle d'un proche ou de quelqu'un représentant l'autorité. Ne donnez jamais de renseignements personnels ou bancaires, n'envoyez jamais d'image de vos pièces d'identité à un tiers qui vous en fait la demande dans un message.

Enfin, gardez à l'esprit que les cyber-escrocs ne servent à financer des activités criminelles : si jamais vous êtes victime d'une escroquerie, allez porter plainte. Même si les pirates se trouvent dans un pays lointain, il faut que l'on connaisse le plus précisément possible les chiffres de la cybercriminalité pour mieux lutter contre elle.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (vols, sabotages, piratages, fraudes, arnaques Internet…) et judiciaires (Police, Gendarmerie, Assurances, Particuliers, Sociétés, Avocats et Cabinets d'avocats…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Contactez-nous

Réagissez à cet article

Source : http://www.tahiti-infos.com/Clusir-Ne-relayez-pas-les-spams-canulars-chaines-de-lettres_a121624.html

---

Les bonnes pratiques pour lutter contre la cybercriminalité

Les bonnes pratiques pour lutter contre la cybercriminalité

Les entreprises modernes sont très vite confrontées aux dangers que représente un modèle commercial actif en permanence. Les clients ont de plus en plus recours à des outils en ligne pour accéder à des comptes, à des services ou à de l'expertise.

Quant aux employés, ils souhaitent pouvoir se connecter à distance et à tout moment aux réseaux de leur entreprise. D'où l'aspiration à un accès quotidien plus simple et plus pratique. Mais cette souplesse a aussi son revers. Les hackers, qui l'ont également bien compris, créent par conséquent des virus et des logiciels malveillants, dans l'unique intention de nuire. À la lumière des récentes révélations de l'organisme britannique Office for National Statistics selon lequel plus de 5,8 millions d'incidents de cybercriminalité ont eu lieu l'an dernier, il est crucial que les entreprises protègent les données de leur personnel et de leurs clients contre la cybercriminalité.
Dans ce contexte, quelles sont les principales activités de cybercriminalité dont les entreprises ont à se prémunir, et que faire pour les combattre ?

La manipulation sociale (Social engineering)
A l'ère du numérique, les pratiques de manipulation sociale sont devenues un problème préoccupant. Du fait que l'internet offre aux fraudeurs un voile d'anonymat, il est important que les sociétés qui détiennent des données clients sensibles soient au courant des pratiques les plus répandues parmi les hackers qui utilisent la manipulation sociale.
Le phishing aussi appelé hameçonnage, est peut-être la forme la plus connue de piratage de fraude par abus de confiance. Il recouvre les tentatives de fraudeurs qui généralement déploient de multiples moyens pour acquérir des données sensibles telles que les noms d'utilisateur, les mots de passe et les détails de paiement en se faisant passer pour une personne connue ou des organismes de confiance par courrier électronique ou une autre forme de communication numérique. Récemment, les cas de hameçonnage beaucoup plus ciblé, où les hackers se présentent comme des personnes de confiance, sont à la hausse. En cas de succès de l'attaque, les données des clients ou les documents sensibles d'une entreprise et donc sa réputation – sont en danger.
En effet, la recherche par Get Safe Online indique que la fraude liée au phishing a contribué aux organisations britanniques qui ont perdu plus de 1 milliard de livres sterling au cours de la dernière année en raison de la cybercriminalité.
Selon l'enquête, réalisée avec Opinion Way et dévoilée en exclusivité par Europe 1, 81% des sociétés française ont été ciblées par des pirates informatiques en 2015.
Le vishing et le smishing sont les variantes du phishing passant respectivement par les communications téléphoniques et SMS. Dans un cas comme dans l'autre, le principe est de récupérer les données sensibles de vos clients ou de votre entreprise. Compte tenu de l'impact dévastateur que peut avoir l'utilisation de la manipulation sociale par les cybercriminels sur les entreprises modernes, les dirigeants d'entreprise et les responsables informatiques doivent être très attentifs à ce type d'activités.

Menaces internes
A l'instar de la manipulation sociale qui peut porter préjudice aux entreprises de l'extérieur, il est légitime de se méfier également des menaces internes. Votre personnel peut disposer de privilèges d'accès aux données sensibles et en faire usage pour nuire à votre entreprise. Les employés mis à l'écart, les prestataires présents ou le personnel de maintenance sur site pourraient également représenter un danger pour votre société.
Les problèmes posés par les activités malveillantes des initiés ne sont pas toujours visibles immédiatement mais ils ne sauraient pour autant être ignorés. Prenons le cas d'un employé qui vient d'être licencié ou de perdre son poste dans une entreprise pour une autre raison. Il est possible que cette décision provoque chez lui de la colère et l'amène à vouloir exprimer son ressentiment envers son ancienne société. S'il possède toujours les droits d'accès au stockage partagé ou à des documents, il a la possibilité de modifier, supprimer ou falsifier les données ultrasensibles. De même, un prestataire exerçant sur le site et auquel un mot de passe temporaire a été attribué sans restrictions pour une courte durée peut représenter un danger. Qu'il s'agisse de corruption ou de communication de données financières, d'informations clients ou bien de droits d'authentification, les agissements de tels escrocs peuvent faire des ravages sur les entreprises de toutes tailles.
Cependant, comme c'est le cas avec les dangers de la manipulation sociale, le fait de connaître et de mesurer la menace potentielle des initiés malveillants peut permettre de faire un grand pas en avant dans la prévention des activités de cybercriminalité visant les entreprises. Les responsables informatiques et les dirigeants d'entreprises doivent rester vigilants en accordant aux utilisateurs des droits d'accès limités à leurs besoins et se méfier des récentes évolutions des techniques frauduleuses pour protéger leur entreprise contre les intentions malveillantes des cybercriminels.

Comment riposter
La lutte contre la cybercriminalité devrait dominer les débats et les plans stratégiques des dirigeants d'entreprise dans les années à venir. Pour optimiser leurs chances de l'emporter, les entreprises peuvent prendre plusieurs mesures.
1. Abandonnez la technique des mots de passe, trop simple, au profit d'un système d'authentification forte en entreprise : Les hackers qui dérobent le nom d'utilisateur et le mot de passe d'un employé peuvent la plupart du temps parcourir le réseau sans être repérés et charger des programmes malveillants ou bien voler ou enregistrer des données. Pour protéger les systèmes et les données, les entreprises ont besoin d'un système d'authentification forte qui ne repose pas exclusivement sur une information connue de l'utilisateur (mot de passe). Au moins un autre facteur d'authentification doit être utilisé, par exemple un élément que possède l'utilisateur (ex. un jeton d'ouverture de session informatique) et/ou qui le caractérise (ex. une solution d'identification biométrique ou comportementale). Il est également envisageable d'abandonner totalement les mots de passe et d'associer cartes, jetons ou biométrie.
2. Profitez de la commodité accrue d'un modèle d'authentification forte mobile : Les utilisateurs sont de plus en plus désireux d'une solution d'authentification plus rapide, plus transparente et plus pratique que celle offerte par les mots de passe à usage unique (OTP), les cartes d'affichage et autres dispositifs physiques. Désormais, les jetons mobiles peuvent figurer sur une même carte utilisée pour d'autres applications, ou être combinés sur un téléphone avec des dispositifs d'identification unique pour accéder à des applications cloud. Il suffit pour l'utilisateur de présenter sa carte ou son téléphone à une tablette, à un ordinateur portable ou à un autre périphérique pour s'authentifier sur un réseau, après quoi l'OTP devient inutilisable. Plus aucun jeton à mettre en place et à gérer. L'utilisateur final n'a qu'un seul dispositif à porter et n'a plus besoin de garder en mémoire ou de taper un mot de passe complexe.
3. Utilisez une stratégie de sécurité informatique par niveaux qui garantit des niveaux d'atténuation des risques appropriés : Pour une efficacité optimale, les entreprises ont intérêt à adopter une approche de la sécurité par niveaux, en commençant par authentifier l'utilisateur (employé, associé, client), puis en authentifiant le dispositif, en protégeant le navigateur et l'application, et enfin en authentifiant la transaction en recourant à l'intelligence basée sur les fichiers signatures si nécessaire. La mise en œuvre de ces niveaux nécessite une plateforme d'authentification polyvalente et intégrée dotée de moyens de détection des menaces en temps réel. Cette plateforme, associée à une solution antivirus, apporte le plus haut degré de sécurité possible face aux menaces actuelles.

_____

Chip Epps est Vice President, Product Marketing, IAM Solutions de HID Global
…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Les bonnes pratiques pour lutter contre la cybercriminalité Chip Epps, HID Global*

Ressources pour la collecte et la vérification d’informations à destination des journalistes

Ressources pour la collecte et la vérification d’informations à destination des journalistes

---

Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification

Présentation de Samuel Laurent, éditeur délégué du Monde, partenaire de First Draft
L'éditeur délégué du Monde présente à First Draft ses travaux en matière de lutte contre la désinformation en ligne et ses projets…[Lire la suite]

Lancement de CrossCheck : à l'approche des élections françaises, les rédactions s'associent pour lutter contre la désinformation
CrossCheck réunit les compétences des secteurs des médias et des technologies pour s'assurer que fausses déclarations soient rapidement détectées et corrigées…[Lire la suite]

Outils pour renforcer la confiance envers les journalistes
Fort de son expérience dans le paysage journalistique américain, Josh Stearns nous présente des outils pour que journalistes et rédactions regagnent la confiance de leur audience…[Lire la suite]
Outils et ressources : Hearken, Engaging News Project, Coral ProjectNews Voices Engaged Newsroom Toolkit

Guide pour la vérification visuelle des vidéos
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des vidéos des internautes…[Lire la suite]

Guide pour la vérification visuelle des photos
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des photos mises en ligne par des tiers…[Lire la suite]

Utiliser Google Earth pour vérifier des images comme un pro
Google Earth offre bien plus que des images satellites…[Lire la suite]

Réseaux sociaux et contenus viraux : comment les développeurs des rédactions peuvent-ils faciliter la démystification ?
Les nouveaux projets de vérification doivent tenir compte des leçons clés tirées des procédés de « fact-checking » (vérification par les faits) ayant faits leurs preuves, tout en les adaptant aux écosystèmes des réseaux sociaux…[Lire la suite]
Savoir où chercher : sources d'image pour la géolocalisation
Trouver d'autres photos ou vidéos d'un lieu peut être un des meilleurs moyens de vérifier le lieu où a été capturé un contenu. Voici où chercher…[Lire la suite]
10 façons de mieux couvrir le terrain pour les journalistes locaux
Combiner le reportage traditionnel sur le terrain et les possibilités offertes par les services numériques modernes peut faire la différence entre un bon et un très bon journaliste…[Lire la suite]
Respecter la source : l'importance du témoin dans la couverture de l'actualité en temps réel
Les témoins sont des personnages clés dans de nombreux événements majeurs se produisant aux quatre coins du monde…[Lire la suite]
Comment se protéger face aux contenus traumatisants ?
Sam Dubberley, cofondateur de Eyewitness Media Hub, détaille certains des résultats principaux d'une étude récente portant sur les traumatismes indirects dans les rédactions…[Lire la suite]

Réagissez à cet article

Original de l’article mis en page : First Draft News FR – Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification