

Vous offrez aux hackers des données invisibles sans le savoir



Vous offrez aux hackers des données invisibles sans le savoir

Empreintes digitales, données GPS des photos, réponses aux questions prétendues «secrètes»...: des données sensibles se cachent sur ce que vous publiez sur les réseaux sociaux, même si l'essentiel du risque se concentre sur des informations livrées plus directement encore...

Le « V » de la victoire pourrait être celui des hackers. Un chercheur japonais avertissait début janvier contre le danger contenu dans ce signe parfois associé aux selfies: en montrant vos doigts, vous courez le risque de vous faire voler vos empreintes digitales, prévient Isao Echizu.

Alors que les «données sont le pétrole du 21ème siècle », comme on l'entend à l'envi, nous avons une fâcheuse tendance à livrer les nôtres, intentionnellement, sur les réseaux sociaux, en négligeant bien souvent les règles de confidentialité ou l'utilisation commerciale qui est leur est destinée. Mais la vigilance se complique quand on n'a même pas conscience qu'une donnée en est une...

Attention aux données invisibles... Permettez-moi d'emprunter vos empreintes

Avec la haute résolution des photos prises par les smartphones, une opération – assez complexe, toutefois, et loin d'être à la portée de tout le monde – peut permettre de récupérer les empreintes. « Or à l'inverse des mots de passe, les empreintes, une fois volées, ne pourront jamais être changées », rappelle à *20 Minutes* Jérôme Billois, expert cybersécurité au cabinet Wavestone.

Il note que si l'avertissement du professeur japonais a fait le tour du monde, « on connaissait le risque depuis 2014 »: un hacker avait montré lors d'une conférence qu'il était parvenu à cloner les empreintes digitales de la ministre allemande de la Défense. Depuis, les empreintes digitales sont de plus en plus utilisées, pour déverrouiller smartphones, objets connectés ou pour réaliser certains paiements.

Des photos très bavardes

Autre donnée invisible, la géolocalisation associée aux photos, la grande majorité étant prise aujourd'hui par des smartphones équipés d'une puce GPS (qui ne sert pas qu'à vous guider sur la route jusqu'à Palavas-Les-Flots). Aux images numériques sont associées tout un ensemble de métadonnées, qui «peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale», comme le précise We Fight Censorship, qui indique la marche à suivre pour nettoyer ces métadonnées.«Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage», lit-on encore.

En septembre dernier, deux étudiants de Harvard ont pu démasquer 229 dealers grâce aux coordonnées géographiques contenues dans les métadonnées associées à des photos qu'ils avaient prises et postées en ligne.

En huit tweets, tout est dit

Sur Twitter, si la géolocalisation des tweets est désactivée par défaut, beaucoup l'activent. En mai dernier, des experts du MIT et d'Oxford démontraient que huit tweets (d'utilisateurs pour lesquels la géolocalisation est activée) suffisaient à localiser quelqu'un de façon très précise. « Il est extrêmement simple pour des personnes avec très peu de connaissance technique de trouver où vous travaillez ou vivez », expliquaient-ils, à l'issue d'une expérience concluante.

Le secret imaginaire des questions secrètes

Il y a enfin ces infos que nous livrons publiquement sur les réseaux sociaux alors qu'elles contiennent parfois les réponses aux questions censées être «secrètes». «Les questions secrètes sont le talon d'Achille des réseaux sociaux, souligne Jérôme Billois. Elles vous permettent d'accéder à vos comptes en cas d'oubli de mot de passe et ce sont toujours les mêmes: Quel est le prénom de votre mère? Quel est votre plat préféré? Or toutes ces infos peuvent être retrouvées facilement sur les réseaux sociaux.»

... et surtout aux données plus évidentes, qui permettent de personnaliser le phishing

Pour les scénarios ci-dessus, qui peuvent avoir le mérite d'attirer l'attention, la probabilité d'utilisation malveillante est pourtant « faible », assure Jérôme Billois. Parallèlement, «nous passons notre temps à livrer des informations hypersensibles», et de façon bien plus directe. Or l'occupation principale des cybercriminels reste les mails de phishing, et ces données les aident à les personnaliser.

«Si le mail est pointu, que c'est votre « bonne » banque qui vous dit qu'elle a remarqué votre passage à telle heure la veille, et que toutes ces infos sont correctes parce que vous avez partagé ces données sur les réseaux sociaux, il y a toutes les chances pour que vous cliquiez sur le lien malveillant.»...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous accompagner dans vos démarches de mise en conformité avec la réglementation Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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 DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous



Réagissez à cet article

Original de l'article mis en page : Sans le savoir, vous offrez aux hackers des données invisibles