

Un guide pour la protection de la confidentialité en ligne des journalistes

@rib News, 09/05/2017 La confidentialité en ligne pour les journalistes Introduction De nombreux journalistes, toutes générations confondues, ont probablement remarqué que les allusions au Watergate pleuvent dans tous les sens ces derniers temps. Des livres comme 1984 de George Orwell sont de retour dans les vitrines des librairies, et une ambiance menaçante envers la liberté de parole et la liberté de la presse se répand doucement, comme un nuage noir sur l'horizon.

Quand un président américain en faction accuse l'ancien président de surveillance ; quand il empêche l'accès des journalistes et médias américains à un accès qui a toujours été autorisé, et considéré comme acquis aux contacts de la presse qu'il tient ; quand il attaque constamment les médias, les accusant d'être l'ennemi numéro 1 du pays, il est surprenant de voir remonter à la surface des souvenirs du président Nixon, à chaque nouveau tweet larmoyant qui attaque le SNL. Même John McCain, sénateur républicain, exprime des inquiétudes au sujet de l'avenir de la démocratie. Et McCain n'est pas le seul. De nombreux journalistes qui j'ai parlé récemment m'ont fait part de leur inquiétude sur l'avenir de la liberté de la presse. Dans une époque où il est possible de dire que Donald Trump contrarie la NSA sans passer pour un menteur, tout est possible. Quand on ajoute à cela les événements récents relatifs à la CIA, qui nous ont appris que presque tous les systèmes de cryptages peuvent être compromis avec de la persévérance, on commence à envisager un monde complètement dystopique, où l'on ne serait jamais à l'aise, même allongé sur son canapé à regarder la télévision. La bonne nouvelle, c'est qu'il est possible de rendre la tâche difficile à ceux qui souhaiteraient intercepter vos emails, vos SMS ou vos appels. Vous pouvez prendre des mesures pour compliquer la vie de ceux qui souhaitent découvrir vos sources et les informations qu'elles vous fournissent. Évidemment, les mesures que vous prenez pour protéger votre confidentialité, votre anonymat de vos sources et la sécurité de vos données doivent être proportionnelles à la possibilité qu'une telle menace survienne, que ce soit du piratage ou de l'espionnage. « Les promesses que je ne divulguerai pas l'identité de ma source et ne donnerai pas mes notes » sont inutiles si vous ne prenez pas les mesures nécessaires pour protéger vos informations numériques », nous dit Barton Gellman du Washington Post, dont la source Edward Snowden, ancien sous-traitant de la NSA, l'a aidé à découvrir la portée des opérations de la NSA et du GC&CS anglais avec la journaliste Tony Loci. Loci elle-même, qui couvrait le système judiciaire américain pour AP, Le Washington Post et USA Today, et qui a été convoquée par la cour pour avoir refusé de dévoiler ses sources, serait d'accord avec cette déclaration. Alors, qu'est-ce qu'il est nécessaire de faire pour s'assurer que les sources et les données des journalistes soient à l'abri et bien protégées ? Grosso modo, les astuces peuvent être classées dans les catégories suivantes : Isoler vos appareils et/ou leur environnement - par exemple, l'isolation physique d'un ordinateur dans le bureau, de vérifier des fichiers, ou l'utilisation de téléphones portables. Sécuriser les applications et fonctions des appareils - ce qu'on appelle réduire la surface d'attaque, c'est-à-dire limiter les applications installées, n'installer que depuis des sources fiables, choisir des applis qui nécessitent peu d'autorisations, maintenir le système à jour, et effectuer de nombreux contrôles de sécurité (basés sur le dernier livre blanc des meilleures pratiques) sur l'appareil. Agir avec précaution, dans le monde réel comme dans le monde numérique - il s'agit de bon sens que de bons logiciels ; par exemple, n'écrivez jamais le nom de votre source, surtout pas sur une appli, ni un document stocké dans votre ordinateur, et certainement pas non plus sur le cloud. Lire l'intégralité de cet e-book

À

À

(adsbygoogle = window.adsbygoogle || []).push({});