« AUCUN RÉSEAU SOCIAL N'EST SÉCURISÉ À 100 % »

Comment se protéger sur internet ? Les conseils de Jean-Philippe Noat et Bruno Valentin d'Uriel Expert, une entreprise monégasque spécialisée dans la sécurité et l'investigation numérique, créée en 2005. **PAR RAPHAËL BRUN**

LA SÉCURITÉ TOTALE EXISTE SUR INTERNET ?

JEAN-PHILIPPE NOAT : « Non. On peut tendre vers une sécurité totale. Mais il y a toujours un risque résiduel qui continue à exister et qu'il est impossible d'éliminer. Entre un cloud public et un cloud privé, le niveau de sécurité n'est pas du tout le même. Google Drive, Dropbox et les autres clouds publics sont une porte ouverte pour la National Security Agency (NSA), l'organisme du département de la Défense des Etats-Unis. Même chose avec WeTransfer : qui vous garantit que les données transférées sont vraiment détruites ? Et puis, si tous ces services sont gratuits, c'est que les données collectées sont revendues ensuite. Car il faut bien que ces services se financent, d'une façon ou d'une autre ! Il faut bien se dire que derrière ces services gratuits, il y a toujours un modèle économique… »

« IL EST TOUT À FAIT POSSIBLE D'AVOIR ACCÈS À DES DOCUMENTS QUI ONT ÉTÉ EFFACÉS, QUE CE SOIT SUR FACEBOOK OU AILLEURS »

QUI SONT LES PIRATES ?

JEAN-PHILIPPE NOAT : « Il existe plusieurs profils de hackers. Les moins dangereux sont les scripts kiddies ou les lamerz, qui sont souvent de jeunes pirates qui s'amusent à modifier l'apparence d'un site internet. Il y a aussi des groupes organisés avec des revendications morales ou politiques : ce sont les hacktivistes. Les Anonymous reste le groupe d'hacktivistes le plus connu. On peut aussi citer les black hats, c'est-à-dire des pirates à la recherche de challenges pour se faire connaître. Sans oublier les pirates cupides qui cherchent à gagner de l'argent. Et puis il y a également des groupes mafieux, des gouvernements, des salariés, des stagiaires, des entreprises spécialisées en intelligence économique, des entreprises concurrentes, des pédophiles, des escrocs… »

BRUNO VALENTIN : « Depuis 2005, les motivations des pirates ont changé. Pour schématiser, on est passé du petit adolescent boutonneux qui bidouille devant son ordinateur dans sa chambre d'étudiant pour se faire connaitre et reconnaitre, à des attaques extrêmement discrètes. L'objectif, c'est de voler des informations sans que la personne ou l'entreprise volée ne s'en aperçoive. Il y a de plus en plus de cyberespionnage, notamment d'Etat à Etat. Les Chinois sont très forts d'ailleurs. Il ne faut pas oublier que même entre alliés, on s'espionne… On l'a vu récemment entre les Etats-Unis et la France. »

UN PROFIL VERROUILLÉ SUR FACEBOOK EST SÛR À 100 % ?

JEAN-PHILIPPE NOAT : « Non. Aucun réseau social n'est sécurisé à 100 %. Il suffit de créer un profil sur Facebook avec le nom d'une personne qui existe déjà, en copiant sa photo. Je prétends ensuite que mon compte Facebook a été piraté et je demande à être accepté comme ami. La personne va m'accepter et je verrai toutes ses publications. C'est aussi simple que ça. Et ça prend 5 minutes. »

BRUNO VALENTIN : « Il ne faut jamais oublier ceci : dès que l'on poste quelque-chose sur internet, ça appartient ensuite à internet. Dès que l'on publie un texte, une photo ou une vidéo sur internet, il faut considérer que ça devient public. Le droit à l'oubli numérique n'existe pas et n'existera pas. Donc publier sur internet des photos de soi peu flatteuses va vous suivre des années et peut poser pas mal de problème. Notamment lorsqu'on postule pour un emploi. Car les recruteurs regardent les informations vous concernant sur internet. »

PEUT-ON STOCKER EN TOTALE SÉCURITÉ DES DOCUMENTS ULTRA-CONFIDENTIELS SUR INTERNET ?

BRUNO VALENTIN : « Là encore, le risque nul n'existe pas. Les exemples ne manquent pas. On peut citer les photos très intimes de l'ex-championne française de natation, Laure Manaudou. Ou encore The Fappening, l'une des plus grosses fuites de photos concernant des célébrités nues, qui a eu lieu fin août 2014. Les photos et les vidéos diffusées ont été copiées et recopiées des centaines, voire des milliers de fois, partout dans le monde. Et on ne maîtrise plus rien. »

« DÈS QUE L'ON PUBLIE UN TEXTE, UNE PHOTO OU UNE VIDÉO SUR INTERNET, IL FAUT CONSIDÉRER QUE ÇA DEVIENT PUBLIC. LE DROIT À L'OUBLI NUMÉRIQUE N'EXISTE PAS ET N'EXISTERA PAS »

JEAN-PHILIPPE NOAT : « Tout ce qui est stocké sur Gmail, sur Google Drive ou sur Google Doc appartient à Google. C'est écrit. Il suffit de lire les conditions d'utilisation. Ce que presque personne ne fait… Les gens n'imaginent pas qu'avec internet, ils ouvrent la porte au monde entier à leur domicile »

FAUT-IL FUIR TOUS LES RÉSEAUX SOCIAUX ?

JEAN-PHILIPPE NOAT : « Surtout pas ! Car si vous n'êtes pas sur les réseaux sociaux, quelqu'un peut être présent à votre place et usurper votre identité. Il faut donc être sur les réseaux sociaux et contrôler au maximum ce qu'on diffuse. Sans oublier de vérifier que vos comptes Facebook ou Twitter par exemple ne diffusent pas de bêtises à votre insu. On est donc obligé d'être sur les réseaux sociaux, ce qui est une forme de diktat. »

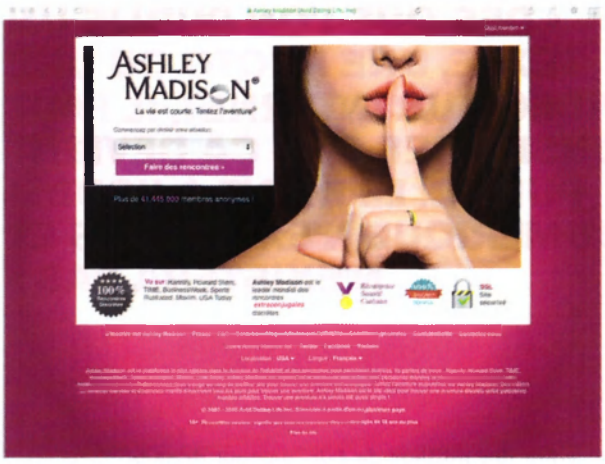
BRUNO VALENTIN : « On est désormais dans une société numérique dans laquelle il faut contrôler les informations publiées sur nous en ligne. Qu'on le veuille ou non. »

UNE FOIS QU'UN DOCUMENT EST EFFACÉ SUR INTERNET, ON PEUT ÊTRE TRANQUILLE ?

JEAN-PHILIPPE NOAT : « Absolument pas. Il est tout à fait possible d'avoir accès à des documents qui ont été effacés, que ce soit sur Facebook ou ailleurs. On peut non seulement consulter des photos ou des vidéos qui ont été effacées mais on peut aussi aller beaucoup plus loin. Et identifier, par exemple, qui est juif dans mon entourage. On peut aussi savoir si une personne en a vu une autre, où ça, à une date et à un horaire précis. »

QUE PEUT-ON STOCKER DANS UN CLOUD ?

JEAN-PHILIPPE NOAT : « Dans les clouds gratuits, comme Drop Box, iCloud, Box. com ou Google Drive, il n'y a bien évidemment aucune confidentialité. Un simple nom d'utilisateur et un mot de passe suffisent pour consulter ce qui est stocké dans ces clouds. Rien ne garantit non plus que ces clouds soient sécurisés de manière à empêcher toute intrusion physique. On ne sait pas non plus si les données ne sont pas copiées. Dans



« DANS L'AFFAIRE ASHLEY MADISON, IL Y AVAIT AUSSI QUELQUES ADRESSES EMAIL MONÉGASQUES ET DES ADRESSES IP BASÉES EN PRINCIPAUTÉ »

→ URIEL EXPERT FORME LA POLICE AMÉRICAINE

Le Monégasque Jean-Philippe Noat et son associé français, l'ancien policier Bruno Valentin, proposent des formations à l'étranger dans le cadre de leur entreprise Uriel Expert que Noat a lancé en 2005. Ces deux associés disposent de certifications que peu de professionnels ont en Europe. « *Tout cela nous donne une légitimité dans le monde entier* », explique Noat. Ce qui leur permet d'offrir leurs services à l'international, et notamment aux Etats-Unis. Un partenariat a été signé avec le leader de l'investigation numérique, Guidance Software, qui publie le logiciel EnCase. « *On est aussi certifié au niveau mondial pour l'investigation sur smartphones, donc on peut former et expliquer sur ces questions-là,* ajoute Noat. *L'un de nos partenaires israéliens recherchait des formateurs pour former la police américaine. On a postulé et on a été choisi. On est parti une semaine, à Vancouver au Canada former la police canadienne au mois de mai dernier et la semaine du 28 septembre nous sommes à Oroville, près de Sacramento, en Californie.* » Ensuite, les deux associés sont partis faire de la formation à Paris, à la Défense. Puis chez les forces de l'ordre spécialisées françaises pour la téléphonie mobile et sur Linux. Uriel Expert espère dépasser les 200 000 euros de chiffre d'affaires cette année. « *Mais on investit chaque année 50 000 euros pour rester constamment à la page* », souligne Bruno Valentin. **R.B.**

les clouds privés, par exemple celui d'une entreprise, la sécurité est beaucoup plus élevée, puisque tout se passe en interne, sur les serveurs de cette entreprise. »

VAUT-IL MIEUX STOCKER CES DONNÉES CONFIDENTIELLES À MONACO OU AILLEURS ?

JEAN-PHILIPPE NOAT : « Que l'on soit une entreprise ou un particulier, dans la mesure où on réside à Monaco, il vaut mieux tout stocker en Principauté. Car cela évite les problèmes éventuels liés aux frontières. Si une entreprise monégasque se fait pirater à l'autre bout du monde, ou dans un cloud quelconque, on peut se demander quelle loi va s'appliquer ? Car si les serveurs sur lesquels sont stockées les données sont répartis dans plusieurs pays, quelle est la loi qui s'applique ? Les entreprises monégasques peuvent aujourd'hui créer leur propre cloud chiffré et sécurisé en Principauté, en faisant appel à l'hébergeur qu'elles souhaitent, que ce soit Monaco Telecom, Télis ou d'autres. Ce qui leur permet de contrôler en direct tout risque d'intrusion physique chez eux. Et de sécuriser leur infrastructure comme ils le souhaitent. »

D'OÙ VIENNENT LES FUITES ?

JEAN-PHILIPPE NOAT : « Les fuites dans les entreprises viennent souvent de l'intérieur. Il peut tout simplement s'agir d'un clic malheureux d'un salarié. Jusqu'à présent, beaucoup misaient sur des firewall, c'est-à-dire des murs de feu, pour s'isoler et empêcher toute intrusion. Sauf que si rien ne peut entrer, tout peut sortir… Car il est impossible d'empêcher les salariés d'utiliser internet. Or, un simple clic dans un email douteux et le mal est fait. Et les données peuvent être récupérées. Qui n'a pas cliqué sur une pièce jointe ou sur un lien ? C'est d'ailleurs comme ça que le système informatique du ministère des Finances français a été attaqué en décembre 2011. Donc même si on ne pourra jamais empêcher un salarié de cliquer dans un mail, il faut absolument travailler sur l'éducation et l'information de chacun. Il faut sensibiliser et former. Car le maillon faible est souvent humain. On peut mettre des moustiquaires partout, si un salarié ouvre la porte de l'intérieur, ça ne sert plus à rien. »

BRUNO VALENTIN : « On est un peu plus préservé si on travaille sur un Mac. Car les concepteurs de virus veulent toucher un maximum d'ordinateurs dans le monde. Or, le parc mondial d'ordinateurs est constitué à plus de 90 % par des PC, pas par des Mac. Mais comme le parc de Mac augmente, on commence à voir arriver quelques virus sur ces machines. Autre possibilité de fuite : les clés USB qui passent d'ordinateur en ordinateur et qui peuvent véhiculer des virus. Autre problème : lorsqu'une entreprise change ses ordinateurs et que les machines partent en recyclage. N'importe qui peut alors récupérer les informations contenues sur les disques durs. Reformater les disques durs ne suffit pas : on conseille de garder les disques durs dans l'entreprise et d'envoyer le reste des machines en recyclage. Ou de les détruire. »

© Photo Monaco Hebdo.

« Les gens n'imaginent pas qu'avec internet, ils ouvrent la porte au monde entier à leur domicile. » Jean-Philippe Noat (ici à gauche) et Bruno Valentin. Uriel Expert.

LES ANTI-VIRUS SONT FIABLES ?

JEAN-PHILIPPE NOAT : « Aujourd'hui, les anti-virus détectent entre 10 et 20 % des virus connus. Donc 80 % des menaces restent invisibles et hors de contrôle. Les particuliers sont souvent peu ou pas informés sur ces questions de sécurité. Il faut donc les sensibiliser davantage. De plus, ils sont aussi victimes du marketing et de la publicité qui leur laissent souvent entendre que tout est sûr et parfaitement sécurisé. Ce qui est faux. »

VOUS N'ÊTES PAS UN PEU PARANO, À VOIR LE MAL PARTOUT ?

JEAN-PHILIPPE NOAT : « Pas du tout. Il suffit de suivre l'actualité pour se rendre compte que la cybercriminalité augmente. Tous les jours, il y des fuites de données sur internet. Le site de rencontre Ashley Madison est un exemple récent. En seulement 15 jours, les hackers ont réussi à entrer dans le site et à pirater la base de données. Informations personnelles, données bancaires, préférences sexuelles… Sur les 27 millions de mots de passe récupérés par les pirates, ils ont réussi à en déchiffrer 14 millions. Et je peux vous dire que chez Ashley Madison, il y avait aussi quelques adresses email monégasques et des adresses IP basées en Principauté. Parmi les mots de passe le plus utilisé : « 123456 » par plus de 120 000 utilisateurs. Beaucoup d'autres avaient mis le nom de leur femme… En tout cas, le PDG fondateur d'Ashley Madison a été viré. Après cette énorme affaire, tous les sites de rencontres sont inquiets. Car avant de s'inscrire, les gens vont désormais hésiter un peu plus qu'avant. Il faut en tout cas absolument éviter d'enregistrer son numéro de carte bleue sur un site internet marchand. En parallèle, il faut suivre de près ses relevés de comptes bancaires et signaler rapidement à sa banque toute opération litigieuse ou frauduleuse. En cas de piratage, les banques remboursent en général sans trop de problème. »

« AUJOURD'HUI, TOUT LE MONDE EST SUR LES AUTOROUTES DE L'INFORMATION. MAIS PRESQUE PERSONNE N'A LE PERMIS… »

BRUNO VALENTIN : « Il faut toujours éviter de se connecter sur le site de sa banque depuis un cybercafé. Et on évite aussi d'utiliser les réseaux de WiFi publics, que ce soit dans les gares, dans le métro ou ailleurs. Car sur ces hotspots WiFi, on peut non seulement savoir ce que vous faites, mais on peut en plus capturer vos mots de passe. Les WiFi publics ne sont pas fiables. Finalement, aujourd'hui, tout le monde est sur les autoroutes de l'information. Mais presque personne n'a le permis… »

BRUN@monacohebdo.mc
@RaphBrun