SÉBASTIEN DUPONT

VOUS ÊTES FOUS D'ALLER SUR INTERNET !

Usurpation d'identité, piratage, sécurité...

UN EXPERT VOUS DIT TOUT CE QUE VOUS DEVEZ SAVOIR

Flammarion

VOUS ÊTES FOUS D'ALLER SUR INTERNET

Ordinateurs, tablettes et Smartphones ont radicalement changé nos modes de vie. Ultra connectés, nous sommes devenus, sans nous en apercevoir, dépendants et fragiles. Nous ignorons tout de la réalité des risques numériques. Personne ne nous a prévenus de la nature du danger. Nous ne savons pas que nous sommes menacés quand on effectue un achat sur Internet, quand on consulte une banque en ligne ou même quand on cherche l'âme sœur sur un site de rencontres.

Vous êtes fous d'aller sur Internet ! tire la sonnette d'alarme et passe en revue tout ce qu'il faut savoir en matière de sécurité numérique (piratage de données, divulgation de la vie privée, harcèlement, vol d'identité, etc.), à travers près de cent pièges recensés, et autant de solutions pour se prémunir et réagir efficacement.

Pour ne pas devenir une cyber-victime malgré nous et rester sans défense contre les intrusions, voici le premier kit de survie numérique.

Responsable de la sécurité numérique pour la création du « Pentagone à la française » et au sein de grands groupes internationaux, Sébastien Dupont est impliqué depuis vingt ans sur le terrain de la protection des données.

Flammarion

19-II Création Studio Flammarion

Vous êtes fous d'aller sur Internet !

DU MÊME AUTEUR

Le Management ZEN, allier performance et sérénité, Éditions AFNOR.

Sébastien Dupont

Avec la collaboration de David d'Equainville

Vous êtes fous d'aller sur Internet !

Comment survivre au monde numérique et à ses pièges

Flammarion

ISBN : 978-2-0814-4711-0

Sommaire

Introduction

Je ne voulais pas écrire ce livre.

Je trouvais trop dangereux de diffuser publiquement une synthèse sur les risques des outils numériques. Si j'avais été un serrurier, aurait-il été bénéfique à mes clients d'expliciter à tout le monde les fragilités des différentes serrures sur le marché, et de contribuer à une possible multiplication des intrusions ? Est-ce qu'un exposé des menaces ne va pas favoriser la défiance des internautes ? Non. Ils sont déjà dans le paradoxe d'utiliser en masse Internet tout en se méfiant des acteurs qui « aspirent » leurs données. Un expert en cyberdéfense n'a pas vraiment vocation à devenir le grain de sable qui aggrave les difficultés déjà existantes et freine l'élan numérique de chacun.

Mais je ne voulais pas non plus me dérober. Après tout, l'essence de ce métier, au-delà de sa capacité à vous rendre paranoïaque et à vous faire douter chaque semaine de l'intégrité de vos propres systèmes, est bien de sécuriser les technologies numériques au service des entreprises ou des particuliers. Car il n'y a pas de raison que monsieur et madame Tout-le-

monde soient laissés sur le bord de la route du numérique. Trop de personnes souffrent, s'inquiètent ou sont victimes du numérique. Il n'y a pas de raison que ce sujet reste un sujet de spécialistes. Il faut s'en emparer pour le démystifier et faire progresser les valeurs d'humanisme : le numérique au service de chacun. À force de nous adapter à cette révolution, nous en avons accepté tous les travers.

Mon travail consiste donc à sécuriser les réseaux d'ordinateurs et les flux de données de grands groupes et d'organisations étatiques. Je ne m'ennuie jamais tant le parcours d'obstacles est varié. Il y a de si nombreux pièges à éviter. Je connais les petits travers de mes homologues, toujours méfiants quant à l'arrivée d'une nouveauté technologique (il y a peu de chance que vous trouviez une enceinte connectée au domicile d'un expert sécurité). Et toujours avec une légère tendance à vouloir proposer des solutions pointues pas toujours opérationnelles pour le commun des mortels. Ne pas noter les mots de passe et ne pas réutiliser le même, d'accord. Mais comment faire quand la moyenne des Français en possède une bonne douzaine ?

J'ai également conscience de la futilité de conserver d'anciens téléphones portables, même si ceux-ci sont a priori moins vulnérables puisque sourds et aveugles aux évolutions technologiques des générations suivantes. Et je connais les limites de nos compétences lorsque nous croyons devenir des experts d'un sujet en particulier et que notre ego prend le dessus. L'hyperspécialisation engendre des angles morts. Je sais, par exemple, que sécuriser un site marchand n'induit pas

forcément un avis pertinent sur les réseaux sociaux utilisés par tous les âges. Je sais aussi que la masse d'information diffusée sur les enjeux de la protection des données a tendance à égarer les plus patients d'entre nous.

Enfant de l'Internet, puisque j'ai eu la chance d'expérimenter les premières classes informatiques dès l'âge de 13 ans, j'ai vu évoluer nos usages numériques à la vitesse du gigabit. De génération en génération, de X, Y à Z, les unes à la suite des autres, mais dans l'ordre inverse des choses, les plus jeunes tirant l'expertise des plus vieux. Je ne peux m'empêcher de penser qu'en matière de sécurité numérique, peu importe aujourd'hui la connaissance qu'ont les utilisateurs de la technologie, il est désormais urgent pour eux de maîtriser le B.A.-BA.

Depuis que nous avons fait le choix de numériser l'ensemble de nos activités, professionnelles et privées, notre survie est en jeu. Il ne s'agit pas seulement de notre survie virtuelle, mais bien de notre vie quotidienne qui pourrait être entravée. Dès aujourd'hui, pas un pan de nos actions n'est à l'abri d'un échange de données binaires… et donc d'une cyberattaque ou d'un dysfonctionnement. Même pour transférer la propriété d'une carte grise de voiture, il faut réaliser la demande sur… Internet. Si tous les chemins menaient à Rome, tous nos chemins passeraient par Internet. J'ai la sensation que le risque, calé sur la même courbe de progression que les innovations informatiques et les masses de données traitées, n'a pas fini de perturber cette révolution de l'interactivité. Ce n'est pas une vue de l'esprit : si nous ne

collaborons pas mieux et plus rapidement pour nous protéger des failles inhérentes à la conception des outils, nos libertés s'en trouveront grandement amputées.

Mon métier consiste à analyser les dangers des systèmes et à présenter des synthèses intelligibles pour aider les non-initiés à agir en conséquence. On ne peut pas à la fois diriger une entreprise et suivre toutes les évolutions technologiques en matière de sécurité. Mon expérience est fondée sur toutes les erreurs déjà commises, et toutes les solutions qui ont été trouvées par la profession afin de les corriger. J'en profite pour remercier tous ceux que j'ai pu rencontrer et qui m'ont transmis leur savoir. Dans une entreprise, je m'adresse aussi bien à des spécialistes du traitement de la donnée qu'à des néophytes, stratèges dans d'autres domaines que l'informatique. Les difficultés à faire évoluer les habitudes pour anticiper un risque me sont familières. De même que des années de prévention ont été nécessaires pour faire évoluer les bonnes pratiques de l'hygiène et de la santé, de l'alimentation saine, je sais qu'un effort comparable nous attend en matière de sécurité numérique. Je comprends ceux qui n'y voient pas suffisamment clair pour s'intéresser au sujet. Oui, il y a une partie subjective et non scientifique qu'il faut assumer. J'entends ceux qui pensent que les cyber escrocs ont et auront toujours un coup d'avance mais non, ce n'est pas une raison suffisante pour baisser les bras. Nous n'avons plus de temps à perdre. Voilà ce que je me disais en rédigeant les premières pages de ce guide de survie numérique.

Autant s'y mettre tout de suite.

J'ai suivi une méthode aussi simple qu'efficace : celle de faire feu de tout bois dans le but d'éclairer suffisamment les risques encourus par les usagers de nos machines écrans et autres applications interactives, communément appelées « Oui-Oui », en référence à ce personnage de fiction qui hoche la tête en signe d'assentiment, pour la porte qu'elles nous ouvrent volontiers sur le monde du numérique. Mais rassembler et expliciter les informations dispersées n'est pas une chose si aisée. Entre les bulletins des experts, ceux des diverses institutions, les notes des hackers et des amateurs, il y a de quoi perdre la tête et tous nous égarer. Vous ne trouverez pas les chiffres en milliers de milliards de dollars annonçant les dommages au niveau mondial, ni ceux en centaines de milliards annonçant un marché florissant de la cybersécurité. Il est difficile de cautionner leur crédibilité.

Pour rester le plus pratique possible, j'ai entrepris même de tester moi-même les risques des « Oui-Oui » les plus récents, de Facebook à WhatsApp, toute la panoplie des offres relationnelles, jusqu'aux sites de rencontre. Et je n'eus pas à attendre longtemps avant de déceler les premières manifestations du danger.

Deux semaines après mon inscription sur un site de rencontre, je fus victime d'une arnaque à l'effeuillage orchestrée avec brio, tant psychologiquement que techniquement. En un rien de temps après mon inscription je fus harponné par un « brouteur », ces animateurs qui gèrent différents profils factices, féminins ou masculins, toujours à l'écoute des besoins de leurs

proies. Après le miel, la bastonnade numérique. J'étais invité à régler une rançon sous peine de voir divulguer à mes contacts, personnels et professionnels, une vidéo où j'apparaissais en fâcheuse posture et que l'imposteur prenait un malin plaisir à faire tourner en boucle sur mon Smartphone, mon « Oui-Oui » préféré. Bigre ! La qualité du montage de ce faux était remarquable. J'étais victime d'un maître chanteur. Elle était loin l'époque où les arnaqueurs avaient l'orthographe vacillante et la syntaxe exotique. Aujourd'hui, à l'écran, ce sont des avatars tout à fait crédibles de médecins, d'avocats, d'enseignants, et parfois même d'amis conviés à votre table, qui tentent de vous faire les poches. Heureusement que j'avais pris quelques précautions avant de faire le grand saut.

La cybercriminalité a pris du poids avec les années. Europol, l'agence européenne de police criminelle, comptabilise plus de dix milliards d'euros de préjudice, toutes techniques confondues. Un chiffre en constante progression. Évoquer la criminalité numérique fait émerger une information essentielle : les escroqueries ne visent pas uniquement les plus riches car, pour reprendre l'adage, en matière de réseau, les petits ruisseaux et l'automatisation peuvent engendrer de très grandes rivières. Nul besoin d'être une personnalité en vue pour être la cible ou la victime d'un chantage à la réputation. Nous sommes tous des cyber-victimes potentielles, d'autant plus que nous ignorons la nature des dangers qui nous guettent au détour d'une annonce sur Internet ou d'un faux courriel de notre banque, et que nous ne prenons aucune des mesures qui s'imposent. En cas

d'arnaque, nous « oublions » même de porter plainte, pensant à tort que cela ne servira à rien, moitié honteux de s'être laissé berner technologiquement, moitié vaincu par une démarche qu'on pense vaine et fastidieuse. Tout ceci a pour conséquence de fausser les statistiques, freinant la prise de conscience du phénomène par les pouvoirs publics.

Malgré cette opacité, le gouvernement estime tout de même à plus de 1 milliard d'euros par an le coût de la menace, de quoi la prendre très au sérieux si l'on envisage de ne pas se faire dépouiller au coin du réseau. Bien pire encore qu'un impact financier, il faut se méfier de l'utilisation abusive de données sur des populations fragiles. Rappelons-nous la terrible actualité d'une jeune adolescente italienne qui a mis fin à ses jours après la diffusion en ligne, contre son gré, d'une vidéo relevant de sa vie privée. Un cas malheureusement de plus en plus fréquent.

Est-il encore nécessaire de vous convaincre de vous réveiller sans plus tarder ?

Il est indispensable de prendre la mesure de la situation et de ne plus différer la confrontation avec la réalité. Nous avons besoin de réponses concrètes. Pourquoi est-il si compliqué de trouver une aide pratique sur le sujet, du plus simple des conseils au plus complexe ? Pourquoi les différents acteurs institutionnels avancent-ils en ordre de marche dispersé, alors que leurs efforts devraient être coordonnés ? Face à un tel enjeu de société, les questions se bousculent. L'information sur le site www.cybermalveillance.gouv.fr/ est-elle suffisante ? A-t-on réellement évalué le

coût administratif des escroqueries électroniques ? Et pourquoi des plaignants ne réussissent-ils pas à se faire rembourser auprès de leur banque après un *card-jacking* si leur code secret a été volé ?

Le monde numérique ne serait-il pas un monstre qui s'apprête à nous dévorer ?

Pour éviter un naufrage individuel et collectif, faut-il se passer des innovations de la révolution informatique, feindre d'ignorer qu'un petit pays européen, l'Estonie, a mis en place des services numériques performants, e-carte d'identité centralisant les données de chaque citoyen, économisant 2 % de son produit intérieur brut (PIB) ? Il serait urgent de porter un regard critique sur les risques intrinsèques à nos habitudes numériques, de passer enfin derrière nos écrans. Au même titre qu'il existe des conduites à tenir lorsque l'on risque de rencontrer dans certaines contrées un ours (comme ne pas bivouaquer à proximité de ses provisions), nous nous devons de préserver nos données privées (tout en sachant qu'il est illusoire de chercher un niveau de sécurité élevé avec un ordinateur ou un Smartphone, quelle que soit leur sécurisation, l'outil invulnérable étant un mythe). La sécurité n'existe pas. C'est comme en amour, seules les preuves existent. Il faudra prendre le temps d'aller chercher des fleurs.

C'est pourquoi, face à la vague de transformation sans précédent qui s'est levée et arrive sur nous à grande vitesse (Big Data, Internet des objets, Intelligence artificielle, etc.) bousculant les règles économiques et sociales établies, j'ai jugé utile d'établir une

cartographie accessible de ce que vivent les Français et de proposer un kit de survie numérique en milieu hostile, le premier du genre, afin que chacun puisse se connecter en toute connaissance de cause et en toute sécurité.

Votre Smartphone est un mouchard

Les Smartphones rapportent gros

En vingt ans seulement, le téléphone portable a envahi notre quotidien. Son usage s'est généralisé à 5 milliards de personnes dans le monde, soit la quasi-totalité de la population mondiale. Dans certaines régions de la planète, il constitue le moyen de communication le plus fiable, et parfois même l'unique outil de communication.

Le téléphone mobile a connu un tel engouement et développement de ses services, qu'il est en passe de détrôner les ordinateurs traditionnels. En une décennie, il a acquis leur puissance de calcul, favorisant au passage le marché des applications mobiles, multiplié par dix en quelques années, pas loin des prévisions d'un chiffre d'affaires de 100 milliards[1] de dollars dans le monde. Il y a de quoi être fasciné. Surtout

1. « Gartner Says by 2017, Mobile Users Will Provide Personalized Data Streams to More Than 100 Apps and Services Every Day », Gartner, 22 janvier 2014.

lorsque l'on apprend que cet outil unique embarque au moins autant en technologies qu'une fusée mettant en orbite des satellites, et que son coût de développement a été de plus d'un milliard d'euros. D'ailleurs, on ne sait plus comment l'appeler : téléphone intelligent, ordiphone, téléphone connecté ? On en oublierait presque qu'il a été conçu à l'origine pour échanger des nouvelles de vive voix avec nos semblables.

Ceux qui n'ont pas cru à son développement s'en sont mordu les doigts et ont dû mettre les bouchées doubles pour rattraper leur retard. Les plus avertis ne l'ont pas vu venir, comme Steve Ballmer, directeur général de Microsoft, qui regrette au début des années 2000 de n'avoir redéployé des talents à la construction de smartphone. Mais le plus fascinant concerne la sécurité de ces engins de haute technologie, aussi sous-estimée que les perspectives de ce marché l'avaient été à l'époque des premiers téléphones mobiles.

Nous connaissons mal les risques liés aux ordinateurs, mais est-ce que nous avons conscience des failles de nos Smartphones ? Faut-il s'inquiéter de l'existence de chevaux de Troie glissés dans le code des applications à télécharger, des techniques de clonage d'un téléphone ou des conséquences d'un SMS frauduleux ? Existe-t-il des risques spécifiques que nous ignorons, qui pourraient insuffler un doute fatal (et salvateur) à la confiance accordée à la pratique de ces couteaux suisses numériques ? Car le danger est bien réel. En autorisant les Smartphones à exposer sur Internet et conserver au fil de leur utilisation des informations personnelles sur nos vies et nos habitudes, nous

offrons prise à tous les observateurs illégitimes, malveillants ou juste intolérants. Pour faire face à cela, les professionnels de la sécurité des systèmes informatiques s'intéressent à « protéger la donnée », protection qui devient la question centrale de cette problématique sécuritaire.

Même s'il n'est pas question d'arrêter d'utiliser nos Smartphones tant ils ont su se rendre indispensables, il nous faut reprendre en main le contrôle du partage de données, et moins nous exposer par ignorance des risques. Prendre conscience, par exemple, que le simple prêt de son appareil à un tiers, même à une personne de confiance (ou à un enfant jouant avec le Smartphone d'un adulte), sans de solides mesures de sécurité, augmente par erreur ou malveillance les risques de vol de données personnelles qui peuvent se traduire par des atteintes à la vie privée ou des pertes financières.

Nous parlons librement au téléphone, mais je suis toujours surpris de la liberté de ton que nous employons, la sensation forte et rassurante de confidentialité éprouvée par tout un chacun. Peu de gens s'imaginent être sur écoute. Ils seraient dans un avion, un train, dans les transports en commun ou dans un marché à faire leurs courses qu'ils seraient plus prudents sur leurs sujets de conversation.

Combien de criminels se sont retrouvés sous les verrous à cause d'un téléphone ? Soit pris dans les filets de la géolocalisation le jour où ils réalisaient ou préparaient leur forfait, soit tenus en laisse par des écoutes téléphoniques, l'un des outils technologiques les plus

puissants aux mains des enquêteurs des services de police.

Alors si nous ne sommes pas tous des criminels, sommes-nous pour autant des cibles, même si nous n'avons rien à cacher ? C'est là que le sujet se complique, et les solutions d'espionnage de Smartphones en vente libre sur Internet ne simplifient guère les choses. Inscrire « espionner un portable » dans un moteur de recherche vous dirige tout droit sur des solutions clés en main. Et moyennant un coût de 100 euros environ, sans aucune compétence technologique, ces actions totalement illégales peuvent être menées par n'importe qui.

Bien que les conflits conjugaux nés des résultats d'une fouille sauvage du contenu du Smartphone de l'un des deux conjoints par l'autre soient nombreux, rappelons que le Code pénal (article 226-1) punit d'un an d'emprisonnement et de 45 000 euros d'amende le fait de porter atteinte à l'intimité de la vie privée d'autrui.

Les logiciels d'espionnage sont puissants, peu visibles, et permettent d'accéder (comme le font la plupart des applications) aux activités de l'appareil photo, des appels téléphoniques, des applications de messagerie et des réseaux sociaux. État de santé, état financier, état psychologique, relation avec la famille et les tiers, relation administrative, petits accidents de la vie, jardins secrets, toutes nos données personnelles sensibles sont concernées. Plus grave, certaines applications proposent une fonctionnalité « d'enregistreur des touches saisies », les fameux *keylogger*, ce

qui permet d'accéder à nos mots de passe et à nos données bancaires lors de nos achats en ligne.

Mais ce n'est pas tout. Imaginez-vous dans un aéroport, un café ou une zone commerciale, là où se trouvent des bornes en libre-service, avec l'impératif de recharger au plus vite la batterie de votre appareil sans savoir que ces bornes peuvent héberger des logiciels malveillants (*malwares*[1]) transférables en cas de connexion. Il est en effet possible d'infecter un téléphone mobile avec un tel logiciel, rien qu'en le branchant à une borne de rechargement factice, ce qui revient à un piratage total. Cela a été démontré lors d'une conférence de hackers éthiques avec la reprogrammation de la mémoire d'un Smartphone pour y installer en toute discrétion une application permettant d'avoir accès à des fonctionnalités de l'appareil. De plus, sachez que le branchement de votre Smartphone sur un ordinateur induit des échanges d'informations lors de la connexion : le nom du Smartphone, le fabricant, le numéro de série, des indications concernant le système d'exploitation, voire l'identifiant de la puce électronique. Informations qui peuvent être récupérées à des fins de piratage ultérieur.

Quoi qu'il en soit, une fois votre machine pleine d'énergie, vous décidez alors d'utiliser le réseau sans-fil offert par votre café, hôtel, ou aéroport, pour accéder à Internet. Bien que très pratiques, la sécurité de ces réseaux ne peut pas être garantie. En vous connectant, vous donnez accès à votre téléphone, sans le savoir, à celui qui contrôle le système Wi-Fi offert. Il peut s'agir

1. Voir Lexique en fin d'ouvrage.

de l'administrateur officiel du service, mais aussi d'un pirate informatique qui aurait mis la main sur le système. Le plus souvent, il s'agit même d'un système mis en place par un pirate informatique qui usurpe un service Wi-Fi en ajoutant une lettre au nom d'un réseau légitime, pour faire « comme si », et ainsi récupérer vos identifiants qu'il utilisera ultérieurement pour son compte.

Avec un peu de chance, vous passerez peut-être entre les gouttes de ces cyber-pièges.

En revanche, vous aurez du mal à échapper aux SMS et autres appels téléphoniques surtaxés. Ce type d'arnaque a en effet atteint des niveaux de développement industriel, les escrocs multipliant les astuces et les victimes pour que les 3 euros de l'appel et les 3 euros à la minute se transforment en millions.

Difficile de ne pas s'inquiéter en recevant un message d'alerte du type : « Votre abonnement de 58 euros a bien été pris en compte », suivi des (fausses) coordonnées du service client à contacter sur un numéro surtaxé, dont le message enregistré tourne en boucle indéfiniment.

Plus de 50 000 personnes auraient été arnaquées par un escroc des numéros surtaxés par le biais de trois millions de messages envoyés au rythme effréné de dix mille SMS par jour, depuis des dizaines de cartes SIM différentes. L'escroquerie aurait rapporté environ 600 000 euros, déposés sur des comptes à l'étranger.

*
* *