Review University Without Borders for the Open Society (RUFSO)
ISSN: 2313-285X
Volume 21, 2020

Problématique de sécurité liée à l'utilisation de la messagerie instantanée dans les structures étatiques. Cas de l'application whatsApp au Burkina Faso.

Docteur Yanogo k Jean Hermann

Email:yanogohermann@yahoo.fr

Résumé

La messagerie instantanée peut être comprise comme des outils qui permettent l'échange des messages qui se fait très souvent par écrit et en temps réel de manière synchrone (LeMagIT, 2020). Elle est fréquemment solliciter pour résoudre des besoins de communications et d'échange de données. Au Burkina –Faso, dans les institutions étatiques, on assiste à la mise en place de groupes communément appelé groupe whatsapp dont l'objectif est de partager des informations entre membre du groupe dans le cadre d'un projet. Cela n'est pas sans conséquence pour ceux qui sont averti. En effet, certes la sécurité est améliorée selon les concepteurs, mais les risques pour la gestion de nos propres donnés et nos vies privées se posent.

Comme toute application, whatsapp pourrait comporter des failles de sécurité de nos données. En effet '' Une faille dans la version desktop de whatsapp a récemment été découverte par Gal weizman, chercheur à perimiterX. Cette dernière permettait à des hackers d'insérer du JavaScript dans les messages et d'accéder à vos fichiers à distance'' (Valentin Cimino, 2020). Les concepteurs prétendent avoir effectué des correctifs, mais il est à préciser que cela a probablement entrainé des vols de données. Il faut donc de la prudence dans les types de données qui sont échangés via cette application.

1. Introduction

Les avances technologiques dans le monde ont toujours amenées les gens à s'adonner à toutes nouvelles technologies qui leurs permettent de communiquer de manière plus simple et rapide. Le cas de l'application whatsapp se définit comme

une application de messagerie instantanée qui permet à des utilisateurs de communiquer avec leurs contacts qui qui ont eux aussi le même logiciel installé (Félix Marciano, 2020).

L'utilisation de cette application constitue-t-elle une problématique de sécurité pour les structures étatiques burkinabè ?

Au vue de l'utilisation de cette application de cette application dans les structures et des menaces qu'elles pourraient comporter, n'est-il pas capital de sonner l'alerte ?

Le cycle de vie de whatsapp est marque par l'existence de plusieurs failles de sécurité qui occasionne des espionnages qui porte atteinte à la gestion privée des données. En effet, selon le laboratoire de recherche en sécurité citizen lab, un avocat britannique a été vise par une attaque via un programme Pegasus. L'attaque a été bloquée par les équipes de whatsapp qui travaillaient sur la sécurisation des appels, après avoir eux-mêmes découvert une faille en début main dans l'application (Kesso Diallo, 2019). Certes les concepteurs prétendent avoir corrigé les failles mais la prudence sur son utilisation pour véhiculer des informations secrètes devraient faire l'objet de réflexion car cela montre l'existence de faille de sécurité sur l'application whatsapp qui pourrait constituer un danger pour les structures étatiques.

1.1.Problématique

L'environnement technologique au Burkina-Faso amène les travailleurs de l'état à utiliser l'application whatsapp pour faciliter les échanges de données via cette application dans le cadre de leurs activités quotidienne (travaux de projet, groupe de travail etc….). Cependant, il pourrait y avoir des risques méconnus de l'application qui pourraient échapper au control de ces travailleurs et si les données échangées entre eux sont d'une grande importance, elles pourraient se retrouver dans les mains d'autres personnes. On assiste à des alertes de failles de sécurités existantes dans l'application. En effet, '' La dernière vulnérabilité en date, découverte par l'agence de sécurité informatique PerimeterX, permettait, si elle était exploitée, de prendre le contrôle d'un compte et d'envoyer des messages. Il était également question de pouvoir accéder aux fichiers personnels d'un utilisateur qui utilisait whatsapp depuis un ordinateur'' (Jennifer Mertens, 2020)

L'application whatsapp peut-elle constituer une source d'insécurité pour les travailleurs de l'état Burkinabè lorsque les données échangées sont supposées être secrète ? On

constate une utilisation fréquente de cette application dans nombreux institutions étatiques. Les données échangées entre les travailleurs sont-elles de nature importante voir secrète ? Les concepteurs de l'application apporte tant que mal des correctifs à chaque découverte d'une nouvelle faille de sécurité. Mais cela n'est pas sans conséquence car avant chaque découverte de failles de sécurités, nous constatons déjà des victimes de ces failles d'où la nécessité d'en faire une alerte pour éviter d'exposer des données importante via l'application

2. Matériels et Méthodes

2.1. Matériels

2.1.1. Présentation de la zone d'étude

L'étude se porte sur les institutions étatiques du Burkina-Faso. L'institution étatique peut se définir comme une entité qui concerne l'état, son intervention dans la vie économique et sociale (CNRTL, 2012). On peut alors dire que les structures étatiques regroupent des administrations de service public. Le Burkina–Faso fait partie de l'espace soudano-sahélien. Il partage ses frontières avec la cote d'ivoire, le Benin, le Togo, le Ghana, le Mali, le Niger (UNIVERSALIS, 2020).

2.1.2. Questionnaire

Le questionnaire dans le milieu de la recherche est définit comme '' une technique de collecte de données quantifiables qui se présente sous la forme d'une série de questions posées dans un ordre précis'' (SurveyMonkey, 2020) . Dans notre étude, nous administrons des questions fermées. Ces questions fermées sont administrées aux travailleurs des structures étatiques

2.2. Méthodes

2.2.1. Echantillonnage

L'échantillonnage de notre étude se limite à la sélection des travailleurs dans les structures étatiques utilisant l'application whatsapp dans le cadre de leurs activités. Nous utilisons la formule suivante

$$\mathbf{N= Z^2_{\&} *P*Q/ e^2}$$

& = 0.5 implique que Z = 1,96

P = 0.5

Q = 1-p = 0,5

E = entre 1 et 10%

N : représente la taille de l'échantillon

Z^2 = de la loi normale centre réduite

& = représente le degré de confiance

E^2 = représente l'erreur maximal ou systématique

Nous aurons par conséquent

$N= 1,96^2* 0,5*0,5/ 0,1^2= 0,2401/0,01 = 97$

2.2.2. Collecte de données

Pour cette recherche, les données collectées sont des données secondaires et primaires. Les données primaires sont directement recueillies auprès des travailleurs des structures étatiques. En ce qui concerne les données secondaires, nous avons fait recourt à la documentation ou bibliothèques existantes.

3. L'état des failles de sécurité de whatsapp

Parlant de whatsapp, des recherches ont montré que ''une série de failles de sécurité a été découverte. Ces vulnérabilités pourraient permettre à des attaquants d'altérer le contenu des messages échangés via l'application par des utilisateurs'' (Charlie Osborne, 2019) .

La même source indique que '' les chercheurs en sécurité de check point Dickla Barda, Roma zaikin et aded Vanunu ont révélé trois méthodes d'attaque exploitant ces vulnérabilités. Selon ces chercheurs, les bugs pourraient permettre aux attaquants d'intercepter et de manipuler les messages envoyés dans les conversations privées et de groupe, donnant aux pirates informatiques un pouvoir immense pour créer et diffuser de la désinformation'' (Charlie Osborne, 2019). Ces failles existent du a l'architecture même de l'application rendant les résolutions des failles quasi-difficile. En effet, '' Facebook a déclaré que les bugs de whatsapp étaient causes par des '' limitations (de l'application) qui ne peuvent être résolues en raison de leur structure et de leur architecture '' (Charlie Osborne, 2019). La problématique de whatsapp s'étend jusqu'au phishing. En effet, '' Au quatrième trimestre de 2019 vade Secure a détecté 5020 URL de phishing whatsApp uniques, soit une augmentation de 13000 % par rapport au trimestre précédent '' (Vade secure, 2019). Pourtant les trois premiers trimestres de 2019 le phishing de whatsapp était quasiment inexistant (Vade secure, 2019).

Les travailleurs des structures étatiques s'adonnent aux applications instantanées sans y voir les risques qui sont cachés. En effet, '' recherche de symantec a révélé l'existence d'une faille dans les versions Android des messageries whatsapp et Télégram permettant à des hackers de manipuler les contenus medias (images, brochures, audio) envoyés entre deux utilisateurs'' (Dominique Filippone, 2019). La même source indique que les messageries instantanées ne sont pas

totalement sécurisées. En effet, '' Les messageries instantanées sont très pratiques. Mais elles sont également loin d'être <FULL SECURE> comme on peut s'en rendre compte avec les résultats de la dernière recherche en sécurité de Symantec. Dans leurs récents travaux, les chercheurs en sécurité du fournisseur américain yair Amit et Alon Gat ont pointé l'existence d'une vulnérabilité affectant les versions Android de whatsapp et telegram'' (Dominique Filippone, 2019)

La problématique de whatsapp ne s'arrête pas seulement pas seulement à ces risques. En effet, Le quotidien britannique The Guardien affirme que le backdoor (porte dérobée) de l'application de messagerie détenu par Facebook permettrait d'avoir accès aux conversations des utilisateurs'' (Le Net Expert, 2017) .

La même source indique que cette porte dérobée'' permet à whatsapp de récupérer, lorsque les téléphones sont éteints, des messages cryptes envoyés mais pas encore lus whatsapp peut alors les déchiffrer et les envoyer à nouveau au destinataire qui n'est pas informe du changement de chiffrement. L'expéditeur est quant à lui prévenu seulement s'il a activité une option de sécurité. Cette nouvelle opération de cryptage permet en pratique a whatsapp d'intercepter et de lire les messages de ses utilisateurs, explique le journal britannique '' (Le Net Expert, 2017). Au vue de cela on pourrait se dire que l'on pourrait faire de l'espionnage avec whatsapp. Les travailleurs des structures étatiques devraient être plus prudents quant aux types de données qui sont échangées via cette application dans le cadre de leurs activités. Les concepteurs de l'application se ventent d'une vie privée protégée grâce au chiffrement de bout en bout qu'offre l'application mais nous devront quand même au vue des alertes, être prudent sur les types d'informations qui sont échangées via cette application. En effet, selon le spécialiste Israélien du cyber sécurité, check point a révélé que des hackers professionnels de haute volée pourraient utiliser une faille de sécurité sur l'application de la messagerie instantanée whatsapp pour semer le désordre dans une conversation (Damien Licata Caruso, 2018). Le respect de la vie privée sur les applications de messagerie instantanées reste pose. L'application whatsapp est toujours au centre des débats quant aux failles de sécurité existentielles

4. Résultats

4.1. Résultat de l'enquête

Les questionnaires ont été distribués à 97 travailleurs dans différentes structure de l'état. Voici les principaux résultats.

A la question de savoir si les travailleurs utilisent l'application whatsapp dans le cadre de leurs travaux au service, nous obtenons le résultat suivant :

Statistics

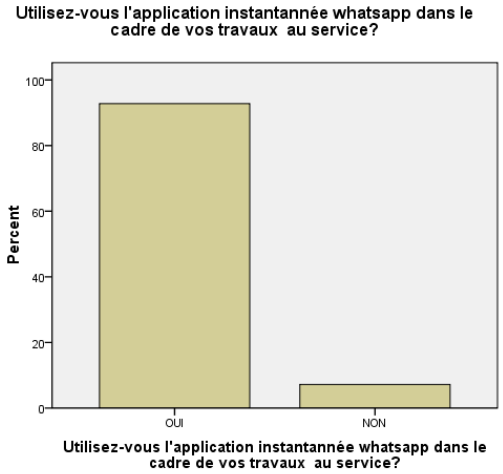
Utilisez-vous l'application instantanée whatsapp dans le cadre de vos travaux au service?

N	Valid	97
	Missing	0

Utilisez-vous l'application instantanée whatsapp dans le cadre de vos travaux au service?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	OUI	90	92,8	92,8	92,8
	NON	7	7,2	7,2	100,0
	Toal	97	100,0	100,0	

Tableau 1 : Statistique sur l'utilisation de whatsapp



Nous constatons au vue de ces chiffres que 92,8% des personnes enquêtées confirment qu'ils utilisent whatsapp au sein de leur service dans le cadre de leur activité. Malgré les risques de sécurité que cela pourraient entrainer nous constatons une utilisation accrue de l'application.

En effet, '' Les fraudeurs utilisant WhatsApp tentent souvent de vous persuader de remettre des détails qui peuvent être réutilisés notamment dans le vol d'identité, comme votre nom et votre adresse.

D'autres escroqueries essayeront d'installer des logiciels malveillants sur votre téléphone. Cela permet de vous espionner efficacement et collecter des informations qui peuvent être utilisées à des fins sinistres.'' (Mobilespy, 2015).

A la question de savoir à quelle circonstance utilisez-vous l'application Whatsapp dans le cadre de vos activités? Nous obtenons le résultat suivant :

Statistics

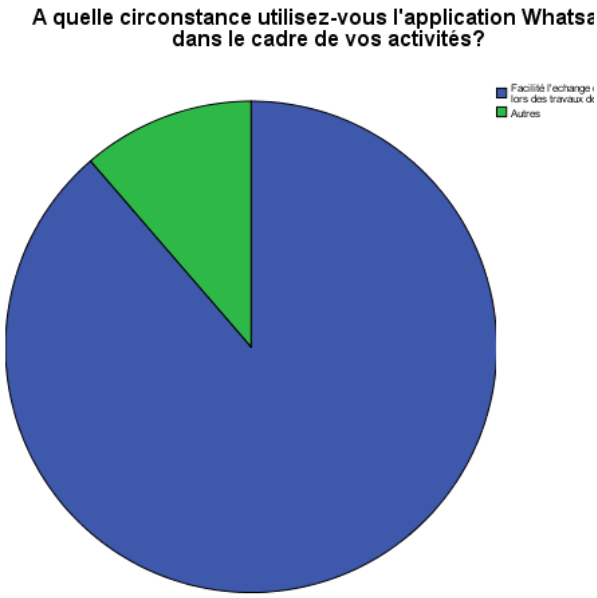
A quelle circonstance utilisez-vous l'application Whatsapp dans le cadre de vos activités?

N	Valid	97
	Missing	0

A quelle circonstance utilisez-vous l'application Whatsapp dans le cadre de vos activités?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Facilité l'échange des données lors des travaux de groupes	86	88,7	88,7	88,7
	Autres	11	11,3	11,3	100,0
	Total	97	100,0	100,0	

Tableau 2: Statistique sur le taux d'utilisation de whatsapp dans les structures publique



Pourcentage de l'utilisation de whatsapp dans les services dans le cadre de leurs activités

Nous constatons que 88,7% des travailleurs dans les structures étatiques utilisent whatsapp pour faciliter l'échange des données lors des travaux de groupe.

Cependant, plusieurs techniques peuvent être utilisées pour accéder à vos données. Certes les données sont cryptées mais pas impossible pour un hacker chevronné. En effet, '' Les conversations WhatsApp en elles-mêmes sont sécurisées, mais pas leur sauvegarde (sur le Cloud ou en stockage local sur votre téléphone) car elle n'est pas cryptée''. (Guide de protection numerique, 2020). La même source indique que '' gardez en tête qu'une personne malintentionnée pourrait avoir accès à vos messages, historiques d'appels, photos, etc., sur WhatsApp si elle parvient à s'introduire sur votre téléphone :

- Soit physiquement (en connaissant le code d'accès de votre téléphone, ou en accédant à un ordinateur synchronisé avec votre compte WhatsApp).
- Soit avec un logiciel espion , qui peut passer outre le cryptage des communications.
- Ou par hameçonnage : une personne malveillante peut vous rediriger vers un faux lien afin d'accéder à votre compte (ex : avec un faux code QR)'' (Guide de protection numerique, 2020).

Certains travailleurs des structures étatiques ne savent pas comment se protéger dans le cadre de l'utilisation de cette application dans leur service ce qui pourrait entrainer des problèmes de fuite de donnée et causer des préjudices à l'état. Vue la sensibilité de certaine informations qui sont échangées à travers l'application il est impérieux de limiter certaines informations via ce canal.

A la question de savoir quels types d'informations échangez-vous via whatsapp? Nous obtenons le résultat suivant :

Statistics

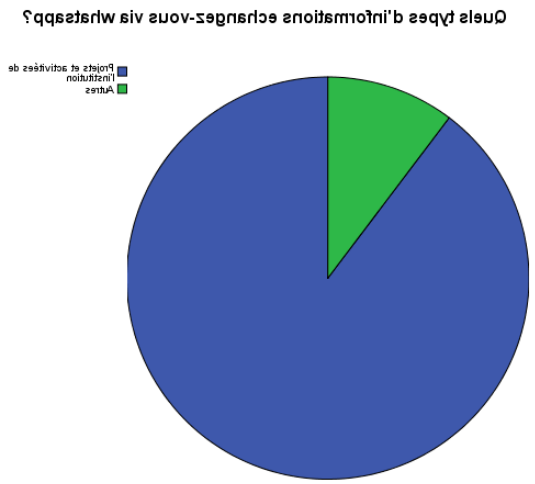
Quels types d'informations echangez-vous via whatsapp?

N	Valid	97
	Missing	0

Quels types d'informations échangez-vous via whatsapp?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Projets et activités de l'institution	87	89,7	89,7	89,7
	Autres	10	10,3	10,3	100,0
	Total	97	100,0	100,0	

Tableau 3: Statistique sur les types d'informations échangées via whatsapp



Pourcentage des types d'informations échangées via whatsapp

Nous constatons que 89,7% des travailleurs utilisent cette application pour les projets et activités de l'institution. Les risques pourtant sont énormes car des failles de sécurité de cette application sont énumérées constamment. En effet, '' Des pirates informatiques ont réussi à installer un logiciel espion sur des téléphones portables, en passant par WhatsApp, plus précisément, en profitant d'une faille sécuritaire dans l'application. Autrement dit, des inconnus parviennent à accéder à tout le contenu des appareils sur lesquels WhatsApp est installé''. (Olivier Peguy, 2019). Il est vrai que les concepteurs essaient de résoudre ces difficultés par des mis à jours constantes mais il est impérieux d'être vigilant avant d'en être victime. Les données secrètes des structures d'état peuvent faire l'objet d'espionnage sans qu'ils ne le sachent.

A la question de savoir si les travailleurs pensaient que leurs appels et données peuvent être espionnés? On obtient le résultat suivant :

Statistics

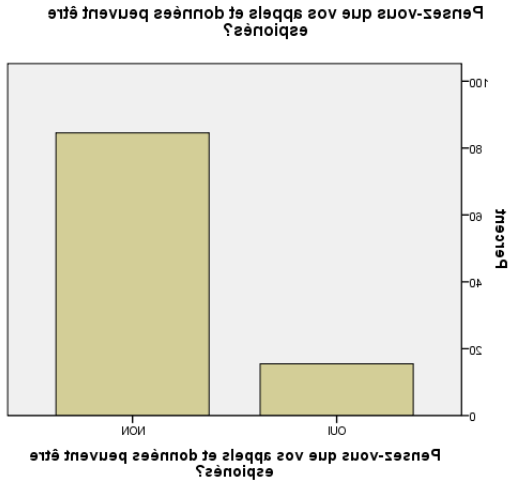
Pensez-vous que vos appels et données peuvent être espionnés?

N	Valid	97
	Missing	0

Pensez-vous que vos appels et données peuvent être espionnés?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	OUI	15	15,5	15,5	15,5
	NON	82	84,5	84,5	100,0
	Total	97	100,0	100,0	

Tableau 4:Statistique sur les avis d'une possibilité d'espionnage des données



Nous constatons que 84,5% des enquêtés ne savent pas qu'ils peuvent être espionne via whatsapp. Pourtant selon le guide de protection numérique un hacker chevronné peut atteindre ses exploits. En effet, selon Nils Matthiesen'' Une menace silencieuse rôde, à l'insu de la majorité des utilisateurs de WhatsApp : un instant d'inattention, et toutes vos conversations WhatsApp peuvent être espionnées par des tiers, et même pas besoin d'être un pirate chevronné. Si vous partagez vos grands et vos petits secrets avec vos amis sur WhatsApp, soyez extrêmement prudent'' (Nils Matthiesen, 2019)

5. Conclusion et Recommandations

5.1. Conclusion

Les applications instantanées sont fréquemment utilisées dans les structures étatiques. Certes ils apportent une simplicité dans les échanges de données, mais force est de reconnaitre qu'avec les différentes failles de sécurité liées à l'application whatsapp qui ont été énumérées par certains chercheurs nous amènent à être conséquent sur la prudence. En effet, l'administration publique burkinabè gère des projets et activités qui se doivent strictement secrets. Il serait incorrect de retrouver certaines données dans l'espace publique d'où l'importance de ne pas échanger des données d'une certaine importance via whatsapp dans l'administration publique. Cette étude nous a montré que bon nombre de travailleurs des structures de l'état ne sont pas prudents

sur les types de données échangées et ne sont pas conscients qu'ils peuvent être espionnés.

5.2. Recommandations

Les recommandations suivantes sont faites pour éviter de mettre en danger certains projets sensibles dans les structures étatiques.

Proposition de solutions visant à pallier les risques d'espionnage dans les structures étatique
1- Eviter le partage de données sensible via whatsapp notamment tout ce qui concerne les projets
2- Mettre en place un dispositif de communication local sécurisé de type master data management permettant aux travailleurs du publique d'échanger en toute sécurité
3- Sensibiliser les travailleurs à plus d'attention
4- Tester et améliorer de façon fréquente l'infrastructure de communication

Tableau 5: Proposition de solutions de protection des données

Références

Charlie Osborne. (2019, 08 08). *Whatsapp : une faille de sécurité découverte par Check Point*. Récupéré sur https://www.zdnet.fr: https://www.zdnet.fr/actualites/whatsapp-une-faille-de-securite-decouverte-par-check-point-39888965.htm

Charlie Osborne. (2019, 08 08). *Whatsapp : une faille de sécurité découverte par Check Point*. Récupéré sur https://www.zdnet.fr: https://www.zdnet.fr/actualites/whatsapp-une-faille-de-securite-decouverte-par-check-point-39888965.htm

CNRTL. (2012). *etatique*. Récupéré sur https://www.cnrtl.fr: https://www.cnrtl.fr/lexicographie/%C3%A9tatique

Damien Licata Caruso. (2018, 08 08). *Cette faille de sécurité pourrait compromettre vos échanges sur WhatsApp*. Récupéré sur https://www.leparisien.fr: https://www.leparisien.fr/high-tech/cette-faille-de-securite-pourrait-compromettre-vos-echanges-sur-whatsapp-08-08-2018-7847043.php

Dominique Filippone. (2019). *Une faille de sécurité corrompt les fichiers médias WhatsApp et Telegram*. Récupéré sur

https://www.lemondeinformatique.fr: https://www.lemondeinformatique.fr/actualites/lire-cyberattaque-sopra-steria-des-repercussions-chez-ses-clients-80803.html

Félix Marciano. (2020, 07 03). *Qu'est-ce que WhatsApp ?* . Récupéré sur https://www.commentcamarche.net: https://www.commentcamarche.net/faq/36900-qu-est-ce-que-whatsapp

Guide de protection numerique. (2020). *Je sécurise mes réseaux sociaux*. Récupéré sur https://www.guide-protection-numerique.com: https://www.guide-protection-numerique.com/je-securise-mes-reseaux-sociaux/whatsapp

Jennifer Mertens. (2020, 02 05). *WhatsApp : un bug permet d'accéder à vos conversations secrètes*. Récupéré sur https://geeko.lesoir.be: https://geeko.lesoir.be/2020/02/05/whatsapp-un-bug-permet-dacceder-a-vos-conversations-secretes/

Kesso Diallo. (2019, 05 14). *Espionnage: WhatsApp corrige une importante faille de sécurité*. Récupéré sur https://www.lefigaro.fr: https://www.lefigaro.fr/secteur/high-tech/espionnage-whatsapp-corrige-une-importante-faille-de-securite-20190514

Le Net Expert. (2017, 01 15). *Une faille de sécurité dans le système de messagerie Whatsapp ?* Récupéré sur https://www.lenetexpert.fr: https://www.lenetexpert.fr/une-faille-de-securite-dans-le-systeme-de-messagerie-whatsapp/

LeMagIT. (2020). *IM (Messagerie Instantanée)* . Récupéré sur https://www.lemagit.fr: https://www.lemagit.fr/definition/IM-Messagerie-Instantanee

Mobilespy. (2015). *4 dangers de WhatsApp à connaître*. Consulté le 11 05, 2020, sur https://www.mobilespy.fr: https://www.mobilespy.fr/espionner-whatsapp/4-dangers-de-whatsapp-a-connaitre

Nils Matthiesen. (2019, 02 09). *Attention ! Vous pouvez facilement être espionné via WhatsApp*. Récupéré sur https://www.avira.com: https://www.avira.com/fr/blog/attention-whatsapp-peut-facilement-etre-espionne

Olivier Peguy, O. (2019, 05 14). *L'application WhatsApp victime d'un sérieux problème de sécurité*. Récupéré sur https://fr.euronews.com: https://fr.euronews.com/2019/05/14/l-application-whatsapp-victime-d-un-serieux-probleme-de-securite

SurveyMonkey. (2020). *Questions fermées et questions ouvertes*. Récupéré sur https://fr.surveymonkey.com: https://fr.surveymonkey.com/mp/comparing-closed-ended-and-open-ended-questions/#quantifiable-data

UNIVERSALIS. (2020). *BURKINA FASO*. Récupéré sur https://www.universalis.fr: https://www.universalis.fr/encyclopedie/burkina-faso/

Vade secure. (2019). *Les failles de sécurité de WhatsApp*. Récupéré sur https://www.vadesecure.com: https://www.vadesecure.com/fr/securite-whatsapp/

Valentin Cimino. (2020, 02 10). *Une faille de sécurité découverte dans la version desktop de WhatsApp*. Récupéré sur https://siecledigital.fr: https://siecledigital.fr/2020/02/10/une-faille-de-securite-decouverte-dans-la-version-desktop-de-whatsapp/