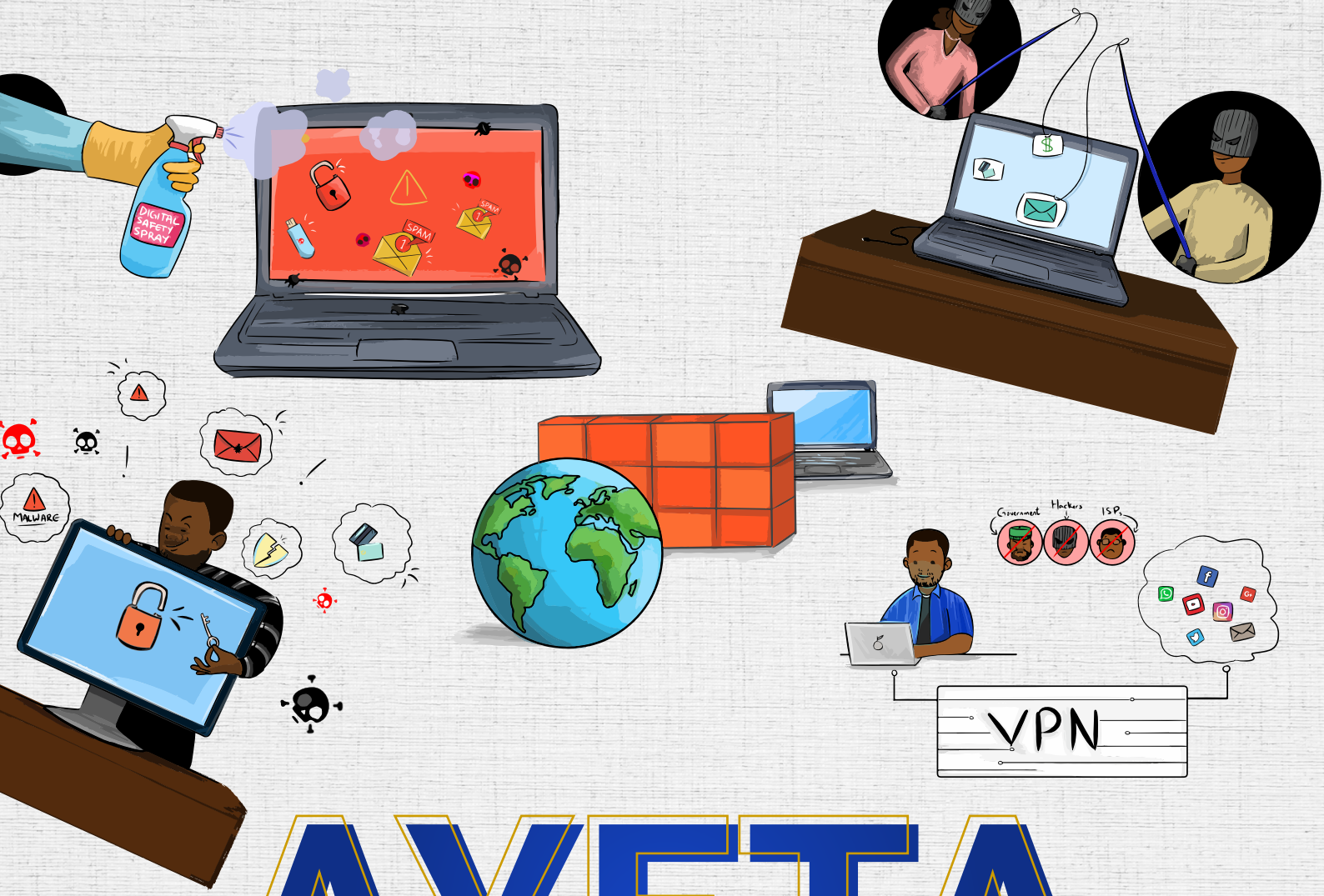
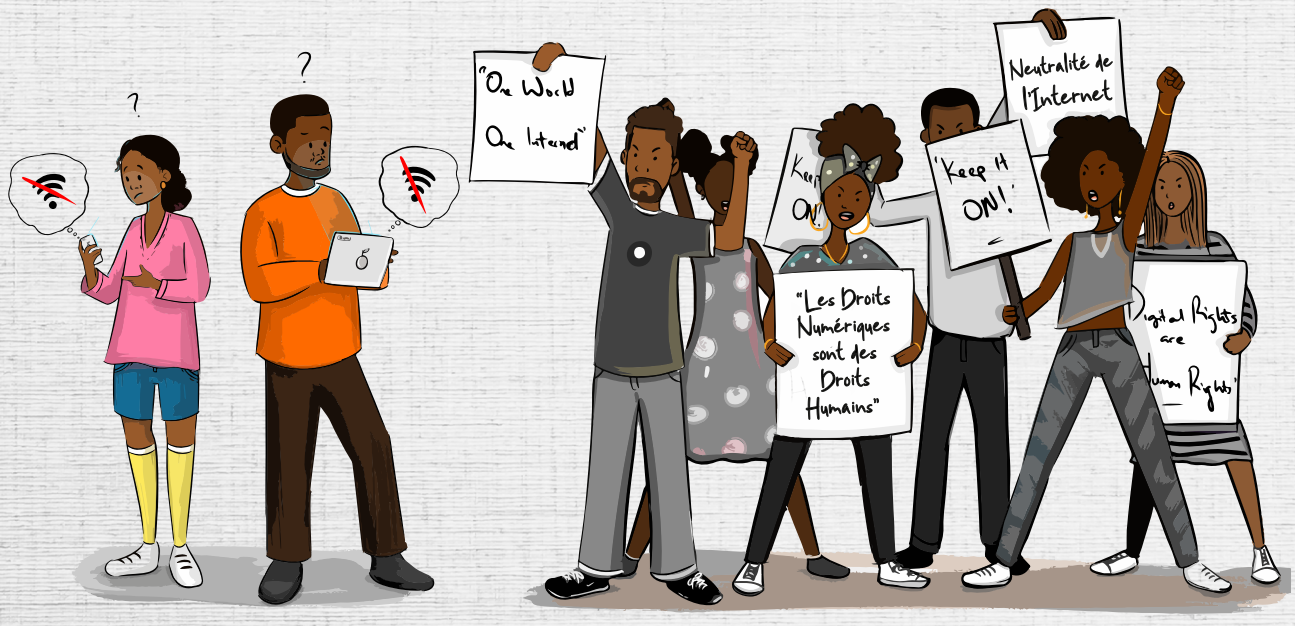


AYETA

Boîte à outils sur les Droits Numériques



Kingdom of the Netherlands

PARADIGM INITIATIVE

Stanford PACS
Center on Philanthropy and Civil Society
Digital Civil Society Lab

AVANT-PROPOS

Les défenseurs des droits numériques se préoccupant de plus en plus de leur sécurité numérique, il est essentiel qu'ils prennent des mesures pour se protéger lorsqu'ils sont dans l'exercice de leurs fonctions. Ce guide pratique fournit des conseils et des mesures de sécurité qui peuvent être prises dans les pratiques contraires des menaces potentielles. Elle comprend également des profils d'acteurs de la sécurité numérique, un calendrier des événements pertinents en matière de droits numériques sur le continent et, enfin et surtout, des liens vers des ressources telles que des études de cas sur la sécurité numérique dans certains pays africains, des modèles de notes d'orientation et de communiqués de presse et des modèles de déclarations communes. Une section du guide est consacrée aux interruptions de réseau, ce que vous pouvez faire pour les contourner, la manière de conserver des archives, les ressources d'information et de sensibilisation pour de tels moments.

Ce guide a été développé dans le cadre du projet 2020 Stanford Digital Civil Society Fellowship, avec le soutien du Fonds néerlandais pour les droits de l'homme. 'Gbenga Sesan et Bonface Witaba ont dirigé la coordination du projet, l'élaboration du programme d'études, la rédaction et l'édition, avec le soutien de l'équipe de Paradigm Initiative. La relecture et la révision en anglais ont été effectuées par Fisayo Alo. Nous remercions tout particulièrement Ashnah Kalemera (CIPESA), Berhan Taye (AccessNow), Demba Kandeh (School of Journalism & Digital Media, Université de Gambie), Ephraim Kenyanito (Article 19 UK), Koliwe Majama (AfDEC), Liz Orembo (KICTANet), Neema Iyer (Pollicy), Neil Blazevic, Oluwatosin Alagbe (PTCIJ), Oyinkansola Akintola-Bello (Co-creation Hub), Ronald Kekembo (FrontlineDefenders) et Vivian Affoah (Media Foundation for West Africa) pour la relecture de la première version du guide. Vos remarques constructives nous ont permis d'améliorer la version actuelle.

Ce guide est conçu pour répondre au besoin croissant de protéger les défenseurs des droits numériques, les journalistes, les lanceurs d'alerte et autres personnes travaillant avec des informations sensibles dans le Sud. Paradigm Initiative (PIN) vise à rendre le guide convivial et à s'assurer qu'il reste une ressource vivante en mettant à disposition des versions plus récentes. Pour ce faire, nous comptons sur vos commentaires, idées, critiques et histoires. Merci d'envoyer vos commentaires à hello@ayeta.africa

Table des matières

Chapitre I

Droits Numériques

1.1 Contexte

L'avènement d'Internet et son ouverture au monde en 1989 ont permis aux défenseurs des droits de l'homme d'innover dans leur utilisation des espaces en ligne pour faire progresser la liberté d'expression et la liberté d'association en ligne, ainsi que pour renforcer les moyens d'une société numérique. Aujourd'hui, l'internet est considéré comme un bien social qui relie plus de la moitié du monde. Cependant, il est devenu de plus en plus volatile et les défis posés aux activistes, aux défenseurs des droits de l'homme, aux dissidents et aux journalistes sont de plus en plus fréquents. Les régimes autoritaires ont eu recours à des outils et des stratégies numériques tels que la fermeture d'Internet, la censure en ligne et la surveillance numérique pour réprimer la liberté d'expression.

Figure 1: Personnages africains défendant les droits numériques

Comme mentionné dans le rapport 2019 de Paradigm Initiative sur les droits numériques en Afrique[1] , « Au cours de la dernière décennie, on a constaté une augmentation de l'impact des organisations africaines qui défendent les droits numériques - connectivité Internet abordable et de qualité, vie privée, liberté d'opinion, d'expression et d'association, entre autres. Contrairement à cette renaissance des droits numériques parmi les citoyens du continent, la vision des gouvernements africains concernant le rôle de la connectivité internet et de l'accès numérique au continent a largement consisté à conserver le pouvoir et le contrôle politiques par tous les moyens. L'instinct dominant a été largement de subordonner les droits et l'accès afin de conserver le contrôle politique sur les citoyens ».

Un rapport du CIPESA de 2019 révèle que jusqu'à 22 gouvernements africains ont ordonné des interruptions de réseau au cours des quatre dernières années et que depuis le début de 2019, 6 pays africains - Algérie, République démocratique du Congo (RDC), Tchad, Gabon, Soudan et Zimbabwe - ont connu des fermetures d'Internet, tandis que d'autres ont fait l'objet de mesures de contrôle des informations sous une forme ou une autre.[2] Les actions de ces pays contreviennent directement aux principes de la Déclaration africaine des droits et libertés sur Internet (AfDec),[3] ainsi qu'à la Déclaration Universelle des Droits de l'Homme (Résolution 217 A de l'Assemblée Générale).[4]

1.2 Que signifie droits numériques ?

Les droits numériques sont essentiellement des droits de l'homme à l'ère d'Internet. Les droits à la vie privée en ligne et à la liberté d'expression, par exemple, sont en fait des extensions des droits égaux et inaliénables énoncés dans la Déclaration Universelle des Droits de l'Homme des Nations Unies.[5] Les droits numériques concernent les droits des individus à l'accès à l'ordinateur et à la capacité d'utiliser et de publier des contenus numériques. Il s'agit des autorisations accordées pour l'utilisation équitable des matériaux numériques et du droit à la vie privée. Selon l'ONU, le fait de déconnecter les personnes d'Internet viole ces droits et va à l'encontre du droit international.[6]

1.3 Chartes, déclarations et protocoles relatifs aux droits de l'homme/numériques

Les droits numériques et les droits de l'homme doivent être synchronisés afin que les principes existants en matière de droits de l'homme soient appliqués à l'environnement Internet et à l'ensemble des domaines d'élaboration des politiques de l'Internet.

1 https://paradigmhq.org/download/dra19/
2 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/
3 https://africaninternetrights.org/articles/
4 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217%28III%29
5 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217%28III%29
6 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

1. Déclaration des Droits de l'Homme des Nations Unies

La Déclaration Universelle des Droits de l'Homme (DUDH) est un document qui fait date dans l'histoire des droits de l'homme. Rédigée par des représentants d'horizons juridiques et culturels différents de toutes les régions du monde, la Déclaration a été proclamée par l'Assemblée générale des Nations unies à Paris le 10 décembre 1948 (résolution 217 A de l'Assemblée générale) comme un standard commun de réalisations pour tous les peuples et toutes les nations. Elle énonce, pour la première fois, les droits fondamentaux de l'homme qui doivent être universellement protégés et elle a été traduite dans plus de 500 langues.[7]

2. Charte africaine des droits de l'homme et des peuples

La Charte africaine des droits de l'homme et des peuples (également connue sous le nom de Charte de Banjul) est un instrument international des droits de l'homme qui vise à promouvoir et à protéger les droits de l'homme et les libertés fondamentales sur le continent africain. La Charte a été adoptée le 1er juin 1981 et est entrée en vigueur le 21 octobre 1986. La Charte instituant l'Organisation de l'unité africaine (OUA) n'a imposé aucune obligation explicite aux États membres pour la protection des droits de l'homme, elle cependant, exige que les États parties tiennent dûment compte des droits de l'homme tels qu'ils sont énoncés dans la Déclaration universelle des droits de l'homme dans leurs relations internationales.[8]

3. Déclaration Africaine des Droits et Libertés de l'internet

La Déclaration africaine des droits et libertés sur Internet est une initiative panafricaine visant à promouvoir les normes en matière de droits de l'homme et les principes d'ouverture dans la formulation et la mise en œuvre de la politique Internet sur le continent. La déclaration vise à développer les principes nécessaires pour faire respecter les droits de l'homme et des peuples sur l'internet, et à cultiver un environnement internet qui puisse répondre au mieux aux besoins et aux objectifs de développement social et économique de l'Afrique. La déclaration s'appuie sur des documents africains relatifs aux droits de l'homme bien établis, notamment la Charte africaine des droits de l'homme et des peuples de 1981, la Déclaration de Windhoek sur la promotion d'une presse africaine indépendante et pluraliste de 1991, la Charte africaine sur la radiodiffusion de 2001, la Déclaration de principes sur la liberté d'expression en Afrique de 2002 et la Déclaration de la plate-forme africaine sur l'accès à l'information de 2011.[9]

4. Déclaration de principes de l'Union africaine sur la liberté d'expression et l'accès à l'information en Afrique

La Déclaration de principes sur la liberté d'expression en Afrique a été adoptée en 2002 par la Commission africaine des droits de l'homme et des peuples. Ce document sert de point de référence pour évaluer les résultats des pays africains devant la Commission. Il constitue également un point de référence solide pour la jurisprudence en Afrique.[10]

7 https://www.un.org/en/universal-declaration-human-rights/
8 https://au.int/en/treaties/african-charter-human-and-peoples-rights
9 https://africainternetrights.org/about/
10 https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf

5. Déclaration de l'Union Africaine sur la Gouvernance de l'Internet

La déclaration de l'Union africaine sur la gouvernance de l'internet a été élaborée dans le cadre d'un processus consultatif afin de tirer parti des avantages de l'économie numérique en créant un environnement propice et habilitant pour que les parties prenantes africaines se réunissent, délibèrent des questions émergentes critiques et contribuent à l'élaboration de politiques publiques de l'internet qui tiennent compte des besoins de l'Afrique. La déclaration sert de principes directeurs aux parties prenantes et constitue les valeurs et les piliers communs sur lesquels tous peuvent s'entendre et s'appuyer lors des délibérations et des débats futurs sur l'avenir de l'internet d'un point de vue africain.[11]

6. Protocole de la CEDEAO sur la Démocratie et la Bonne Gouvernance

Le Protocole de la CEDEAO sur la Démocratie et la Bonne Gouvernance a été adopté en décembre 2001 par les Chefs d'États et de Gouvernement comme un complément au Protocole lié au Mécanisme de Prévention, de Gestion, de Règlement des Conflits, de Maintien de la Paix et de la Sécurité (1999).[12]

1.4 Acteurs de la Sécurité Numérique

Figure 2: Acteurs de la Sécurité Numérique

11 https://au.int/sites/default/files/newseventsworkingdocuments/33025-wd- african_declaration_on_internet_governance_en_0.pdf
12 https://www.ohchr.org/EN/Issues/RuleOfLaw/CompilationDemocracy/Pages/ECOWASProtocol.aspx

De nombreux acteurs de la sécurité numérique ont pris diverses initiatives pour atténuer les vulnérabilités et les risques des journalistes et des défenseurs des droits de l'homme. Ces organisations peuvent être contactées pour obtenir des conseils et/ou une assistance sur des questions liées aux violations de données, aux rapports d'incidence, aux questions politiques, etc...

1. **AccessNow - https://www.accessnow.org/**
   AccessNow fournit une ligne d'assistance téléphonique de sécurité numérique 24 heures sur 24, des analyses politiques fondées sur des preuves, des actions de sensibilisation et des subventions aux organisations de base et aux groupes d'activistes qui travaillent avec les utilisateurs et les communautés les plus exposés aux violations des droits numériques.

2. **AfricanDefenders - https://africandefenders.org/**
   Un réseau panafricain de défenseurs des droits de l'homme composé de cinq organisations infrarégionales africaines, qui se consacre à la promotion et à la protection des défenseurs des droits de l'homme (DDH) sur le continent africain.

3. **Africtivistes - https://www.africtivistes.org/**
   Un réseau panafricain d'activistes et de blogueurs en ligne œuvrant pour la démocratie, comprenant une communauté de 200 cyber-activistes de 35 pays différents.

4. **Association for Progressive Communication (APC) - https://www.apc.org/**
   L'APC travaille à la construction d'un monde dans lequel tous les peuples ont un accès facile, égal et abordable au potentiel créatif des TIC pour améliorer leur vie et créer des sociétés plus démocratiques et égalitaires.

5. **Association of Media Women in Kenya (AMWIK) - http://amwik.org/**
   L'AMWIK est une association nationale de médias dont l'objectif est de renforcer la visibilité des femmes dans la société et de promouvoir leur participation au leadership et à la prise de décision.

6. **Article 19 - https://www.article19.org/**
   Article 19 – travaille sur deux libertés étroitement liées : la liberté de parole et la liberté de savoir, - cherche à faire en sorte que les gens, partout dans le monde, s'expriment librement et participent activement à la vie publique sans crainte de discrimination.

7. **Cc-Hub - https://cchubnigeria.com/**
   Communément appelé Cc-HUB ou le HUB, il s'agit d'une plateforme où des personnes orientées vers la technologie partagent des idées sur la résolution des problèmes sociaux

au Nigeria Communément appelé Cc-HUB ou le HUB.

8. **Central Africa Human Rights Defenders Network (Réseau des Défenseurs des Droits Humains en Afrique Centrale – REDHAC) - https://defenddefenders.org/africandefenders/**

   Cette organisation de défense des droits de l'homme basée en Afrique centrale accompagne et renforce le travail des défenseurs des droits de l'homme (DDH) dans le but d'atténuer leurs vulnérabilités et leurs risques, et de sensibiliser à la situation des droits de l'homme en Afrique centrale.

9. **Collaboration on International ICT Policy in East and Southern Africa (CIPESA) - https://cipesa.org/**

   Basé à Kampala, en Ouganda, le CIPESA est une organisation de politique d'Internet qui travaille en Afrique orientale et australe pour promouvoir une politique des TIC efficace et inclusive en Afrique.

10. **Committee to Protect Journalists (CPJ) - https://cpj.org/**

    Une organisation non gouvernementale américaine indépendante à but non lucratif, basée à New York, avec des correspondants dans le monde entier. Le CPJ promeut la liberté de la presse et défend les droits des journalistes dans le monde entier.

11. **Cyber Security Africa - https://www.cybersecurityafrica.com/**

    Une société de conseil en sécurité de l'information offrant une gamme complète de services et de produits pour aider les organisations à protéger leurs précieux actifs.

12. **Defend Defenders - https://defenddefenders.org/**

    Prête à protéger et à promouvoir les défenseurs des droits de l'homme dans les sous-régions de l'Est et de la Corne de l'Afrique.

13. **Digital Security Alliance (DSA) – https://defendersprotection.org/the-digital-security-alliance/**

    Une coalition d'organisations et d'experts individuels en sécurité numérique travaillant à la sécurisation des biens numériques de la société civile, des défenseurs des droits de l'homme, des journalistes et autres activistes face aux menaces posées par les puissantes entreprises, les criminels sans scrupules, l'État et d'autres acteurs non étatiques.

14. **Freedom House - https://freedomhouse.org/**

    Organisation non gouvernementale à but non lucratif basée aux États-Unis qui mène des recherches et des actions de sensibilisation sur la démocratie, la liberté politique et les droits de l'homme.

15. Frontline Defenders - https://www.frontlinedefenders.org/

Une organisation de défense des droits de l'homme basée en Irlande, fondée à Dublin en 2001 pour protéger ceux qui travaillent de manière non violente pour faire respecter les droits de l'homme d'autrui, tels que définis dans la Déclaration universelle des droits de l'homme.

16. Gambia Cyber Security Alliance - http://gamcybersecurityalliance.com/

Cette organisation basée en Gambie vise à sensibiliser les Gambiens à la cybersécurité, aux cyber menaces et à l'espionnage, et à leur donner les moyens d'être plus en sécurité sur Internet.

17. Gambia Press Union - http://www.gambiapressunion.org/our-work/

L'Union de la presse gambienne est un syndicat de journalistes en Gambie, créé en 1978 par un groupe de journalistes, qui a pour mission de promouvoir des médias libres et dynamiques.

18. Human Rights Defenders Network - Sierra Leone (HRDN-SL) https://namati.org/network/organization/pan-african-human-rights-defenders-network/

HRDN-SL est une coalition d'organisations de la société civile et d'individus travaillant pour la protection et la promotion des droits de l'homme en Sierra Leone. Elle a été créée en tant que branche locale du Réseau panafricain des défenseurs des droits de l'homme (PAHRDN) basé en Ouganda et du Réseau des défenseurs des droits de l'homme en Afrique de l'Ouest (WAHRDN) basé au Togo, avec le soutien technique du Service international pour les droits de l'homme (SIDH) basé à Genève.

19. Kenya ICT Action Network (KICTANET) - https://www.kictanet.or.ke

Un groupe de réflexion multipartite pour les acteurs intéressés et impliqués dans la politique et la réglementation des TIC. Son travail est guidé par quatre piliers : la défense des politiques, le renforcement des compétences, la recherche et l'engagement des acteurs. KICTANET est aussi un espace où les idées des participants peuvent être traduites en propositions concrètes pour résoudre les problèmes auxquels est confronté le secteur des TIC.

20. Media Foundation for West Africa (MfWA) - https://www.mfwa.org/

Créée en 1997 et basée à Accra, au Ghana, la MfWA est une organisation non gouvernementale régionale visant à promouvoir et à défendre le droit à la liberté d'expression de toutes les personnes, en particulier les médias et les défenseurs des droits de l'homme en Afrique de l'Ouest.

21. Media Legal Defense Initiative (MLDI) - https://www.mediadefence.org/

Une organisation non gouvernementale créée en 2008 pour fournir une assistance juridique aux journalistes et aux médias indépendants. Elle apporte également son soutien à la formation en droit des médias et encourage l'échange d'informations, d'outils de contentieux et de stratégies pour les avocats travaillant sur des affaires de liberté des médias.

22. National Coalition of Human Rights Defenders – Kenya (NCHRD-K) - https://defenderscoalition.org/

Une organisation nationale constituée en Trust en République du Kenya. Sa mission est de renforcer les capacités des défenseurs des droits de l'homme (DDH) à travailler efficacement dans le pays et à réduire leur vulnérabilité au risque de persécution.

23. Paradigm Initiative (PIN) - https://paradigmhq.org/

Paradigm Initiative est une entreprise sociale qui construit un système de soutien basé sur les TIC et défend les droits numériques afin d'améliorer les moyens de subsistance des jeunes mal desservis. Le programme de défense des droits numériques de PIN est axé sur le développement d'une politique publique pour la liberté de l'internet en Afrique.

24. Pollicy - https://pollicy.org/

Pollicy est une société de conseil et de développement technologique qui vise à améliorer la prestation de services gouvernementaux par un engagement et une participation civique accrus.

25. Safe Sisters - https://safesisters.net/

Safe Sisters est un programme de bourses pour les femmes défenseurs des droits de l'homme, les journalistes ou les travailleurs des médias et les activistes. Les boursières sont formées pour être capables de comprendre et de répondre aux défis de la sécurité numérique auxquels elles sont confrontées dans leur travail et leur vie quotidienne.

26. Women Human Rights Defenders (WHRD) - https://www.peacewomen.org/

Les femmes défenseurs des droits humains (FDH) sont à la fois des femmes défenseurs des droits humains et tout autre défenseur des droits humains qui travaillent à la défense des droits des femmes ou sur des questions de genre.

27. Women of Uganda Network (WOUGNET) - https://wougnet.org/

WOUGNET a été fondée en mai 2000. L'organisation se consacre à aider les femmes et les organisations de femmes à utiliser les technologies de l'information et de la communication, en se concentrant sur l'utilisation des téléphones mobiles, du courrier électronique et du web, ainsi que sur l'intégration des "moyens traditionnels" tels que la radio, la vidéo et le papier d'une manière qui permette une plus large diffusion.

1.5 Événements relatifs aux droits numériques

Chaque année, un certain nombre d'événements sur les droits et la sécurité numériques sont organisés dans toute l'Afrique. Ces événements rassemblent des parties prenantes de différents horizons, afin de discuter de questions politiques, de tendances émergentes et d'offrir une formation pratique.

Figure 3: Événements pertinents relatifs aux Droits Numériques

1. **African School on Internet Governance (AfriSIG):**
   Une initiative de formation multipartite qui vise à donner aux Africains la possibilité d'acquérir les connaissances et la confiance nécessaires pour participer efficacement aux processus et aux débats sur la gouvernance de l'internet aux niveaux national, régional et mondial. https://www.apc.org/en/project/african-school-internet-governance-afrisig

2. **Cc-HUB Digital Security Demo Day:**
   Journée de démonstration de sécurité numérique Cc-HUB : Les entreprises, la société civile, les étudiants et les passionnés de sécurité de l'information de Lagos et d'ailleurs convergent pour assister en direct à des cyber-attaques et des contre-mesures. https://cchubnigeria.com/cchub-hosts-first-cybersecurity-conference/

3. **Digital Rights and Inclusion Forum (DRIF):**
   Le DRIF est un forum bilingue organisé chaque année en avril par Paradigm Initiative, qui permet à la société civile, aux entreprises technologiques, aux gouvernements, aux universités et à d'autres parties prenantes de débattre de questions d'actualité mondiale concernant les droits de l'internet, en particulier en Afrique. https://drif.paradigmhq.org/

4. **East Africa Cyber Security Convention:**
   La Convention sur la cyber sécurité en Afrique de l'Est vise à doter les participants de connaissances sur la manière de limiter les menaces à la cyber sécurité. https://cloudsecurityalliance.org/csa_events/east-africa-cyber-security-convention/

5. **Forum on Internet Freedom in Africa (FIFAfrica):**
   Organisé chaque année en septembre par le CIPESA, il se concentre sur la promotion d'un Internet libre et ouvert en Afrique. https://cipesa.org/fifafrica/

6. **Initiatives Régionales / École sur la Gouvernance de l'Internet**
   East Africa School of Internet Governance (EASIG)
   West Africa School of Internet Governance (WASIG)

7. **Initiatives Nationales / École sur la Gouvernance de l'Internet**
   Kenya School of Internet Governance (KeSIG)
   Nigeria School of Internet Governance (NSIG)
   South Sudan School of Internet Governance (SSSIG)
   Tanzania School of Internet Governance (TzSIG)
   Arusha Women School of Internet Governance (AruWSIG)

1.6 Études de cas sur les droits numériques

Les tentatives de l'État de violer les droits des journalistes et des défenseurs des droits numériques par la législation, la fermeture d'Internet et les actions en justice, entre autres moyens, sont mises en évidence par des cas sélectionnés (voir les liens) au Nigeria, au Cameroun, Tanzanie et en Zimbabwe.

https://tinyurl.com/y5p57qkw
https://tinyurl.com/y3fedl7f
https://tinyurl.com/y324dmeu
https://tinyurl.com/y63gbr3m

1.7 Modèles de notes d'orientation

Les rôles des défenseurs des droits numériques, des journalistes et des autres activistes

sociaux sont mieux reconnus lorsqu'ils contribuent à apporter des solutions aux innombrables défis auxquels la société est confrontée.
Les liens suivants montrent quelques notes de synthèse dans ce sens.
.

https://tinyurl.com/y2ynk6oc
https://tinyurl.com/y3r9t974
https://tinyurl.com/y2v9ucfl

1.8 Modèle de déclaration de coalition

La tendance croissante des gouvernements africains à réglementer l'utilisation des médias sociaux par le biais de projets de loi généraux aux termes larges contribue à réduire l'ouverture d'Internet, à masquer les violations des droits de l'homme et à créer des obstacles à la stabilité à long terme et au dialogue pacifique. La capacité à s'opposer à cette tendance est renforcée lorsque les parties prenantes parlent d'une seule voix. Quelques exemples de déclarations faites par des coalitions pour traiter des questions connexes sont présentés dans les liens suivants.

https://tinyurl.com/yyt8kkhp
https://tinyurl.com/y5eku8et
https://tinyurl.com/y4l6lwkg
https://tinyurl.com/y38k8mut

Chapitre II

2.1 Sûreté et sécurité numérique

La sécurité numérique, appelée indifféremment sécurité sur internet, sécurité en ligne et/ou cyber sécurité, désigne un ensemble de pratiques et de précautions auxquelles une personne adhère lorsqu'elle utilise l'internet, dans le but de garantir que les informations personnelles sensibles et celles de son ou ses dispositifs restent sécurisées.

a. Comment rester protégé en ligne

Selon une mise à jour de l'infographie « What happens in an Internet minute » 2020, 190 millions de mails, 194 444 tweets, 19 millions de textes WhatsApp apparaissent toutes les 60 secondes. Les statistiques de l'ITU indiquant que plus de 4,5 milliards de personnes (50 %) de la population mondiale sont connectées en ligne, cela ne peut que signifier que les acteurs malveillants, les pirates, les menaces et les escroqueries en ligne sont plus nombreux que jamais. Pour garantir la sécurité numérique des journalistes, des défenseurs des droits numériques et des autres utilisateurs d'Internet, il convient de respecter toute une série de considérations d'hygiène numérique, afin d'aider à réduire les menaces et les incidents liés à la sécurité numérique.

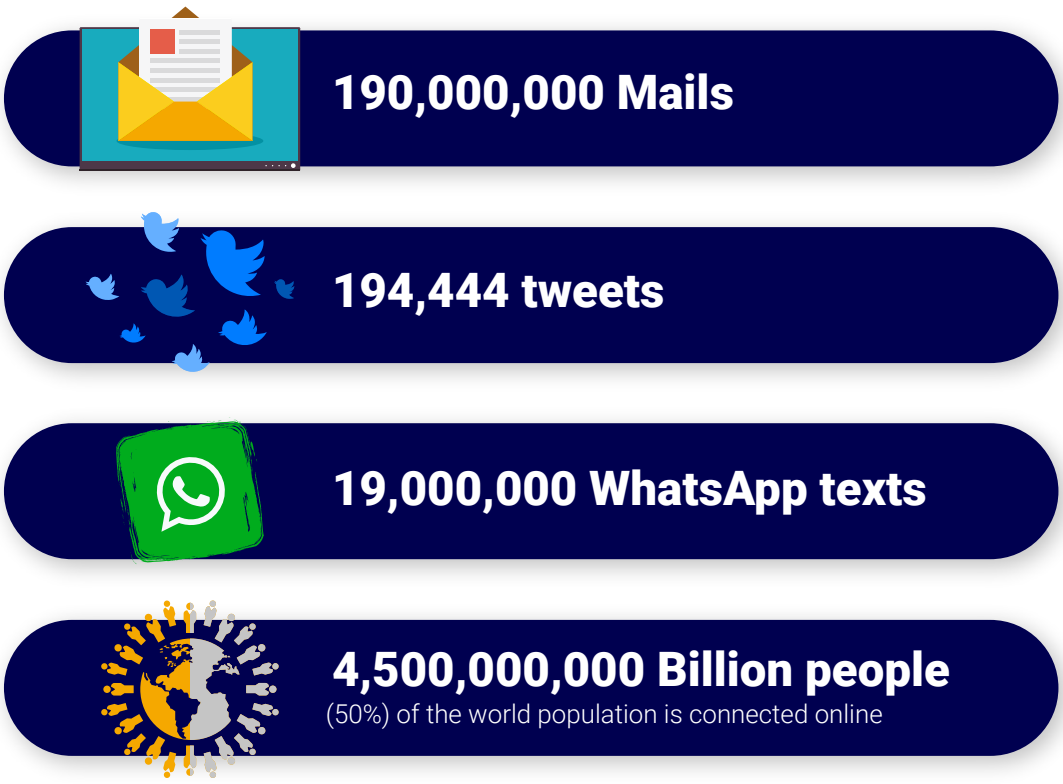


Figure 4: Que se passe-t-il en une minute sur Internet?

b. Hygiène Digitale

L'hygiène numérique est le terme fourre-tout qui désigne les pratiques et les comportements liés au nettoyage et à l'entretien de notre monde numérique. Cela inclut tout, de l'organisation des fichiers sur votre PC au verrouillage de vos comptes de médias sociaux, en passant par l'introduction de nouvelles applications ou technologies pour rendre votre vie numérique plus facile ou plus sûre. On peut entendre parler de cyber hygiène ou d'hygiène sur Internet, qui ont toutes la même signification.

Figure 5: Sécurité et hygiène numériques

c. Avantages de l'Hygiène Digitale

En protégeant les informations que vous partagez en ligne ou en sécurisant les dispositifs que vous utilisez, vous réduisez à la fois la probabilité d'être attaqué et la gravité d'une attaque réussie. Tout ce que vous mettez en ligne peut devenir une source ou une information utilisée par un mauvais acteur pour lancer une escroquerie ou une cyber-attaque contre vous. En tant qu'acteur des droits numériques, le maintien de bonnes pratiques d'hygiène numérique est essentiel pour assurer votre sécurité sur l'internet.

2.2 Pratiques d'Hygiène Digitale

Figure 6: Développer des habitudes sûres en ligne

a. Adopter des habitudes en ligne sûres

Il y a des choses faciles à faire pour rendre votre informatique en ligne plus sûre, sans acheter de technologie coûteuse ni investir beaucoup de temps dans la reconfiguration de votre réseau domestique. La liste ci-dessous est un bon point de départ et renvoie à d'autres parties de notre site pour obtenir des informations plus détaillées sur chaque mesure de sécurité.

1. Maintenez vos systèmes et vos logiciels à jour.[13]
2. Toujours avoir un anti-virus actuel/mis à jour.[14]
3. Éviter les escroqueries par phishing.[15]
4. Use a complex password or a password manager.[16]
5. Faire attention à ce que vous cliquez ; un site web malhonnête peut vous mettre en contact avec des cybercriminels et des acteurs malveillants.
6. Ne jamais laisser son ordinateur ou ses appareils sans surveillance. Verrouiller tous les écrans lorsque l'on se rend aux toilettes. Un système ouvert est une invitation ouverte à consulter vos données.
7. Créer un code pour son appareil mobile, et essayer de ne jamais le laisser allumé dans un avion[17]
8. Protéger ses données.
9. Pour tous les fichiers personnels, sauvegarder vos données ! On ne sait jamais quand on risque de perdre son disque dur, et si les données seront récupérables. Il existe de nombreuses options de stockage dans le nuage, un disque externe est également une option.[18]
10. Lorsqu'on fait des achats en ligne ou qu'on partage des données sensibles, il faut s'assurer que les informations envoyées sont cryptées en recherchant "https" ou l'icône de cadenas dans la barre d'adresse.
11. Faire preuve d'intelligence quant à ce que l'on partage (et ne partage pas) sur les médias sociaux.[19]
12. Dans le monde physique, il faut faire attention à l'ingénierie sociale. Il peut s'agir d'une tentative par un étranger de vous soutirer des informations que vous ne partageriez pas en ligne. Un anniversaire ? Lieu de vacances préféré ? Nom de votre premier animal de compagnie ? A-t-il vraiment besoin de ces informations ? Répondre à ces questions peut entraîner la compromission de vos comptes.
13. Surveillez vos comptes financiers et vos comptes de médias sociaux pour détecter toute activité suspecte.[20]

13 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/updates-patching
14 https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus
15 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing
16 https://cybersecurity.osu.edu/cybersecurity-you/passwords-authentication/passwords
17 https://cybersecurity.osu.edu/cybersecurity-you/protect-personal-devices/mobile-devices
18 https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/file-backups
19 https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/file-backups
20 https://cybersecurity.osu.edu/about/teams/identity-access-management

b. Mots de passe & Authentification

Si vous cherchez un moyen d'améliorer votre cyber sécurité, la sécurité par mot de passe est le point de départ. Idéalement, un mot de passe est un mécanisme de sécurité de base qui consiste en une phrase de passe secrète créée à l'aide de caractères alphabétiques, numériques, alphanumériques et symboliques, ou d'une combinaison de ceux-ci. Ce mécanisme de sécurité est utilisé pour limiter l'accès à un système, une application ou un service aux seuls utilisateurs qui l'ont mémorisé ou stocké et/ou sont autorisés à l'utiliser.
La pratique standard en matière de sécurité numérique consiste à créer des mots de passe forts, à ne pas réutiliser les mots de passe, à utiliser des mots de passe et une authentification à plusieurs facteurs, à prendre soigneusement en considération les questions de réinitialisation des mots de passe, à ne pas noter les mots de passe et, enfin et surtout, à utiliser un gestionnaire de mots de passe.

c. Générateurs de mots de passe

Un générateur de mots de passe est un outil logiciel qui crée des mots de passe aléatoires ou personnalisés pour les utilisateurs. Il aide les utilisateurs à créer des mots de passe plus forts qui offrent une plus grande sécurité pour un type d'accès donné.

d. Importance des générateurs de mots de passe

Les générateurs de mots de passe aident ceux qui doivent constamment trouver de nouveaux mots de passe pour garantir l'accès autorisé aux programmes et gérer un grand nombre de mots de passe pour la gestion des identités et des accès. Parmi les autres types d'outils, on peut citer un coffre-fort de mots de passe, où les utilisateurs gèrent un grand nombre de mots de passe dans un endroit sécurisé.

e. Gestionnaires de mots de passe

Un gestionnaire de mots de passe est un outil qui permet de créer et de stocker des mots de passe afin que de nombreux mots de passe différents puissent être utilisés sur différents sites et services sans avoir à les mémoriser. Les gestionnaires de mots de passe .
Password managers:

- **Génèrent des mots de passe forts qu'un être humain aurait peu de chances de deviner.**
- **Stockent plusieurs mots de passe (et les réponses aux questions de sécurité) en toute sécurité.**
- **Protègent tous les mots de passe avec un seul mot de passe principal (ou phrase secrète).**[21]

KeePassXC est un exemple de gestionnaire de mots de passe qui est open-source et gratuit. Cet outil peut être conservé sur le bureau ou intégré dans

21 https://ssd.eff.org/en/glossary/passphrase

un navigateur web.[22] KeePassXC n'enregistre pas automatiquement les modifications faites lorsqu'on l'utilise, aussi s'il y a un plantage après que des mots de passe aient été ajoutés, ils peuvent être perdus à jamais, mais ce paramètre peut être modifié dans les réglages. Notez qu'utiliser des gestionnaires de mots de passe c'est comme mettre tous ses œufs dans le même panier et à les protéger avec votre vie. Le risque avec des gestionnaires de mots de passe pirates et que, lorsqu'on est piraté, l'accès au « panier » implique l'accès à tous vos « œufs ».

2.3 Attaques communes de mots de passe

Figure 7: Mots de passe sécurisés

a. Essayer des mots de passe courants

L'une des façons les plus faciles et les plus courantes de pirater un compte est d'essayer [23] des mots de passe communs ou pour faire quelques recherches sur la victime ciblée et essayer quelques mots de passe liés à cette personne. Un rapport de CNN de 2019 a révélé que les dix mots de passe les plus utilisés et les plus piratés étaient :

1. 123456
2. 123456789
3. qwerty
4. password 5.
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345

22 https://ssd.eff.org/en/glossary/web-browser
23 https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

Ce sont des mots de passe TRÈS peu sûrs. Ils sont faciles à deviner et les cyber criminels commencent toujours à essayer d'accéder aux comptes avec des mots de passe faibles comme ceux-ci.
Nous recommandons également de NE JAMAIS utiliser des mots de passe qui contiennent les informations suivantes :

- **Votre prénom ou les prénoms des membres de votre famille ou de vos amis,**
- **Votre date d'anniversaire ou celle des membres de votre famille ou de vos amis,**
- **Le nom de vos animaux de compagnie, et**
- **Les lieux où vous vivez ou vous avez vécu y compris les villes ou les noms de rues.**

Le nombre d'informations sur une personne sur internet est impressionnant. Alors, si votre mot de passe contient des informations qui se rapportent à vous que l'on peut trouver sur internet ou en parlant à vos amis, il peut facilement être deviné.

b. Attaque par force brute

Une attaque par force brute essaye simplement toutes les combinaisons possibles de caractères autorisés jusqu'à qu'elle trouve une correspondance. Ce genre d'attaque est très efficace sur des mots de passe plus courts et elle peut même pirater des mots de passe composés de caractères aléatoires. Mais la longueur est importante. Une attaque par force brute ne sera pas très efficace et si votre mot de passe est assez long, il sera quasiment impossible à pirater. Regardez le tableau qui indique le temps qu'il faudra pour attaquer par force brute les mots de passe selon leur longueur et leur complexité. N'oubliez pas que ce tableau estime que l'ordinateur peut essayer plus de 1000 mots de passe par seconde.

Longueur du mot de passe	Tous les caractères	Minuscules uniquement
***	0.86 secondrs	0.02 secondes
****	1.36 minutes	0.46 secondes
*****	2.15 heures	11.9 secondes
******	8.51 jours	5.15 minutes
*******	2.21 années	2.23 heures
********	2.10 siècles	2.42 jours
*********	20 millénaires	2.07 mois
**********	1 899 millénaires	4.48 années
**********	180 365 millénaires	1.16 siècle
**********	17 184 05 millénaires	3.03 millénaires
**********	1 627 797 068 millénaires	78.7 millénaires
**********	154 640 721 434 millénaires	2 046 millénaires

Figure 8: Tableau de longueur / difficulté d'un mot de passe

Notez que le temps nécessaire pour pirater un mot de passe augmente de manière exponentielle à chaque caractère ajouté à votre mot de passe. Pour un mot de passe composé de caractères aléatoires de tous types, la différence entre 6, 7, 8 et 9 caractères est de l'ordre des jours, des années, des siècles et des millénaires ! Remarquez également combien de temps il faut pour pirater un mot de passe qui contient tous les types de caractères, comparé à un mot de passe de même longueur qui n'utilise que des caractères minuscules.

c. Créer et conserver des mots de passe forts et sécurisés

Réutiliser des mots de passe est une pratique de sécurité extrêmement mauvaise. La réutilisation des mots de passe est une pratique de sécurité extrêmement mauvaise. Si un individu mal intentionné met la main sur un mot de passe que vous avez réutilisé dans plusieurs services, il peut accéder à un grand nombre de vos comptes. C'est pourquoi il est si important d'avoir des mots de passe multiples, forts et uniques. Heureusement, un gestionnaire de mots de passe peut vous aider.[24]

d. Créer des mots de passe forts en utilisant des matrices

Il y a quelques mots de passe que vous devez mémoriser et qui doivent être particulièrement forts. Il s'agit notamment de:

- **mots de passe pour vos appareils**
- **mots de passe pour le cryptage (comme le cryptage intégral du disque)**[25]
- **le mot de passe principal,** [26] **ou "phrase secrète,"**[27] **pour votre gestionnaire de mots de passe**
- **le mot de passe de votre email**[28]

L'une des nombreuses difficultés rencontrées lorsque les gens choisissent eux-mêmes leurs mots de passe est que ces derniers ne sont pas très bons pour faire des choix aléatoires et imprévisibles.[29] Un moyen efficace de créer un mot de passe fort et mémorisable[30] est d'utiliser les matrices[31] et une liste de mots[32] pour choisir les mots au hasard. Tous ensemble, ces mots forment votre "phrase secrète". Une "phrase secrète" est un type de mot de passe plus long pour une sécurité supplémentaire. Pour le cryptage de votre disque et votre gestionnaire de mots de passe, nous vous recommandons de choisir au minimum 6 mots.

Pourquoi utiliser un minimum de six mots ? Pourquoi utiliser des matrices pour choisir des mots au hasard dans une phrase ? ? Plus le mot de passe est long et aléatoire, plus il est difficile à deviner, tant pour les ordinateurs que pour les humains. Pour savoir pourquoi vous avez besoin

24 https://ssd.eff.org/en/glossary/password-manager
25 https://ssd.eff.org/en/glossary/encryption
26 https://ssd.eff.org/en/glossary/master-password
27 https://ssd.eff.org/en/glossary/passphrase
28 https://ssd.eff.org/en/glossary/password
29 http://people.ischool.berkeley.edu/~nick/aaronson-oracle/
30 https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
31 https://www.eff.org/dice
32 https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt

d'un mot de passe aussi long et difficile à deviner, voici une vidéo explicative.[33]

Si votre ordinateur ou votre appareil est compromis et qu'un logiciel espion est installé, ce dernier peut vous regarder taper votre mot de passe principal et peut voler le contenu du gestionnaire de mots de passe. Il est donc très important de garder votre ordinateur et vos autres appareils à l'abri des logiciels malveillants lorsque vous utilisez un gestionnaire de mots de passe.

e. Synchronisation des mots de passe sur plusieurs appareils

De nombreux gestionnaires de mots de passe permettent l'accès à des mots de passe sur différents appareils grâce à une fonction de synchronisation des mots de passe. Ce qui signifie que lorsqu'un mot de passe est synchronisé sur un appareil, il le sera automatiquement sur tous les autres appareils. Les gestionnaires de mots de passe peuvent stocker des mots de passe "dans le cloud", c'est à dire encryptés sur un serveur à distance. Lorsque les mots de passe sont nécessaires, ces gestionnaires les récupèrent et les décryptent[34] tautomatiquement. Les gestionnaires de mots de passe utilisant leurs propres serveurs sont plus pratiques, mais ils sont sensiblement plus vulnérables aux attaques. Si les mots de passe sont stockés sur l'ordinateur et dans le cloud, un hacker n'a pas besoin de prendre possession de l'ordinateur pour trouver les mots de passe. (Néanmoins, il devra casser la phrase secrète du gestionnaire de mots de passe). Si cela vous inquiète, ne synchronisez pas les mots passe dans le cloud, à la place choisissez de les stocker sur les appareils eux-mêmes.

- **Note!**

Conservez une sauvegarde de la base de données des mots de passe, au cas où. Il est utile d'avoir une sauvegarde si la base de données des mots de passe est perdue lors d'un crash du système, ou si l'appareil est volé. Les gestionnaires de mots de passe ont généralement un moyen de faire une sauvegarde, ou on peut utiliser le programme de sauvegarde habituel.

2.4 Authentification multi-facteurs et mots de passe uniques

Des mots de passe forts et uniques rendent l'accès aux comptes numériques beaucoup plus difficile pour les malfaiteurs. Pour protéger davantage vos comptes numériques, activez l'authentification à deux facteurs.[35] . Certains services proposent une authentification à deux facteurs (également appelée 2FA, authentification à plusieurs facteurs ou vérification en deux étapes), qui exige que les utilisateurs possèdent deux composants (un mot de passe et un

33 https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice
34 https://ssd.eff.org/en/glossary/decrypt
35 https://ssd.eff.org/en/glossary/two-factor-authentication

second facteur) pour accéder à leur compte. Le second facteur peut être un code secret unique ou un numéro généré par un programme s'exécutant sur un appareil mobile.
L'authentification à deux facteurs à l'aide d'un téléphone mobile peut se faire de deux manières:

- **le téléphone peut exécuter une application d'authentification qui génère des codes de sécurité (comme Google Authenticator[36] ou Authy[37]) ou en utilisant un dispositif matériel autonome (tel qu'une clé YubiKey) ; ou**
- **le service peut envoyer un message SMS avec un code de sécurité supplémentaire qui est utilisé chaque fois qu'une connexion est nécessaire.**

Si vous avez le choix, choisissez l'application d'authentification ou le dispositif matériel autonome au lieu de recevoir les codes par SMS. Il est plus facile pour un pirate de rediriger ces codes vers son propre téléphone que de contourner l'authentificateur. Certains services, tels que Google, permettent également de générer une liste de mots de passe à usage unique. Ceux-ci sont destinés à être imprimés ou écrits sur papier et à être portés sur vous. Chacun de ces mots de passe ne fonctionne qu'une seule fois, de sorte que si l'un d'entre eux est volé par un logiciel espion lorsque vous le saisissez, le voleur ne pourra plus l'utiliser pour quoi que ce soit à l'avenir.

a. Authentification multi-facteurs ("MFA")

L'authentification multi-facteurs (AMF) est une fonction de sécurité offerte par de nombreux sites web, applications et dispositifs qui améliore considérablement la sécurité des comptes. Techniquement, l'AMF peut se référer à un système dans lequel il existe plus de deux formes d'authentification.

b. Comment fonctionne l'Authentification Multi-Facteurs ("MFA)

Si vous disposez d'une configuration AMF pour un compte donné (site web, application ou appareil), lorsque vous vous connectez avec votre nom d'utilisateur et votre mot de passe, le serveur de ce compte va vous demander une seconde forme d'authentification indépendante avant de vous laisser entrer dans le système. C'est comme lorsqu'un compte bancaire est ouvert et qu'on demande à voir une photo d'identité et une autre forme d'identification, comme la carte de sécurité sociale ou le passeport international. Il est beaucoup plus difficile de prétendre être quelqu'un que vous n'êtes pas lorsque vous devez prouver qui vous êtes de deux manières différentes !

c. Méthodes d'authentification multi-facteurs

Nous recommandons d'enregistrer au moins deux dispositifs pour une authentification à plusieurs facteurs. Ainsi, si vous perdez un dispositif, vous pouvez vous protéger en effaçant les données à distance et en utilisant l'autre dispositif pour vous authentifier. Avec la MFA,

36 https://support.google.com/accounts/answer/1066447?hl=en
37 https://authy.com/

la seconde authentification peut être effectuée à l'aide de plusieurs méthodes différentes. Prenons donc un moment pour passer en revue les plus courantes.

i. Méthode "Push" de l'application pour appareil mobile

Le moyen le plus populaire d'obtenir la deuxième forme d'authentification est de "pousser" une application sur votre appareil mobile. Il existe toute une série d'applications d'authentification qui sont gratuites et faciles à mettre en place et encore plus faciles à utiliser pour l'authentification ! Avec cette méthode, le serveur de compte auquel vous essayez de vous connecter enverra un "push" à votre appareil mobile. Ce "push" est une notification qui apparaîtra sur l'appareil mobile et dira quelque chose du genre : "Hé, quelqu'un essaie de se connecter à ce site web, c'est bien vous ? Devons-nous le laisser entrer ? En général, il y a un gros bouton vert et un gros bouton rouge pour que vous puissiez facilement répondre "Oui" ou "Non" d'une simple pression. Si vous appuyez sur "Oui", vous êtes connecté. Mais si vous n'avez pas fait la demande de connexion initiale, vous savez que quelqu'un a votre mot de passe et essaie de se connecter à votre compte. Vous pouvez appuyer sur le bouton "Non" et l'accès sera refusé. Vous pouvez alors aller vous connecter vous-même et changer votre mot de passe pour que l'agresseur revienne à la case départ.

Il s'agit d'une mesure de sécurité simple, mais extrêmement efficace. Le principal avantage de cette méthode est qu'un pirate doit non seulement compromettre votre mot de passe, mais aussi avoir un accès physique à votre appareil mobile et doit pouvoir se connecter à cet appareil. Les chances que tout cela se produise sont extrêmement faibles. En fait, elles sont pratiquement nulles si vous utilisez des mots de passe corrects et si vous surveillez votre téléphone. Un autre avantage de cette méthode est que vous recevez une notification en temps réel lorsque quelqu'un essaie de se connecter illégalement à votre compte. Comme mentionné ci-dessus, vous pouvez utiliser cette connaissance pour réagir rapidement en changeant votre mot de passe

ii. Méthode du code d'application pour les appareils mobiles

Parfois, le serveur du compte ne vous enverra pas de push, mais il peut vous demander de taper un code unique généré par l'application d'authentification de votre appareil mobile. Ces codes sont courts (peut-être 6 chiffres) et peuvent donc sembler peu sûrs. Ce qui est bien, c'est que les codes sont re-générés toutes les minutes environ et qu'ils sont basés sur un algorithme qui n'est connu que de votre application d'authentification et du serveur de compte auquel vous essayez de vous connecter. Il serait extrêmement difficile pour un cybercriminel de deviner correctement le code à six chiffres dans ces circonstances, car le délai est très court. Là encore, le principal avantage est que le pirate doit avoir un accès physique à votre appareil mobile et la possibilité de s'y connecter. Un inconvénient est que vous ne recevez aucune notification en temps réel si quelqu'un essaie de se connecter à votre compte. En général, cette méthode est également une

option de secours à la méthode “push”. La plupart des applications d’authentification prennent en charge les deux méthodes.

iii. Méthode du code SMS

Cette méthode utilise également votre appareil mobile, mais elle n’utilise pas d’application. Elle fonctionne donc avec des téléphones non intelligents. Si vous configurez cette méthode d’AMF, lorsque vous vous connectez avec votre nom d’utilisateur et votre mot de passe, le serveur du compte enverra à votre téléphone portable un message texte avec un code à usage unique. Vous devrez ensuite taper ce code sur le site web ou le portail de l’appareil où vous avez saisi votre mot de passe. Cette méthode présente tous les avantages de la méthode “push”, mais elle n’est pas aussi pratique car vous devez taper le code. Vous recevrez une notification en temps réel de toute tentative de connexion, car vous recevrez un message texte à chaque tentative. Un inconvénient est qu’un pirate ne doit pas nécessairement pouvoir se connecter à votre téléphone. Il doit disposer physiquement du téléphone, mais les messages texte apparaissent souvent sur l’écran du téléphone même lorsque celui-ci est verrouillé.

iv. Méthode du code par Email

Cette méthode ressemble beaucoup à la méthode du code SMS, sauf que le code est envoyé à un compte de courrier électronique que vous avez pré-communiqué avec le serveur du compte auquel vous essayez d’accéder. Le plus souvent, vous le mettrez en place lorsque vous vous inscrirez au service multi-facteurs que vous utilisez. Si vous comptez utiliser ce type d’AMF, vous devrez vous assurer que votre compte de courrier électronique est lui-même sécurisé, ce qui signifie probablement que vous devez activer l’AMF pour accéder au compte de courrier électronique en question. La raison en est que le courrier électronique peut être consulté de n’importe où, y compris du même terminal informatique où le cybercriminel essaie de se connecter à votre compte. En d’autres termes, cette méthode ne nécessite pas d’accès physique à un dispositif indépendant. C’est pourquoi vous devriez avoir un mot de passe fort pour votre courrier électronique qui n’est utilisé nulle part ailleurs. Si vous faites cela, cette méthode exigerait essentiellement que le pirate connaisse deux de vos mots de passe. Cependant, le fait de le forcer à accéder à un autre dispositif est une option plus forte et plus sûre. Si un site web n’autorise que ce type d’AMF, c’est très bien. Allez-y, configurez-le et exigez ensuite une authentification sur votre appareil mobile pour accéder à votre courrier électronique. Alors, tout est parfait

v. Jeton physique

Cette méthode était plus populaire avant l’avènement des smartphones. Un “jeton” physique est un petit appareil qui génère continuellement des codes de la même manière qu’une application d’authentification sur votre appareil mobile. Il fonctionne tout aussi

bien, mais il présente l'inconvénient supplémentaire de vous obliger à surveiller cet autre appareil. De nos jours, nos vies sont liées à nos téléphones portables. Vous pouvez imaginer la possibilité de perdre un token et de ne même pas vous rendre compte qu'il a disparu pendant un certain temps. Si vous en avez un, conservez-le dans un endroit sûr. Si vous devez le transporter, vous pouvez l'attacher à votre porte-clés.

2.5 Authentification à Deux Facteurs ("2FA")

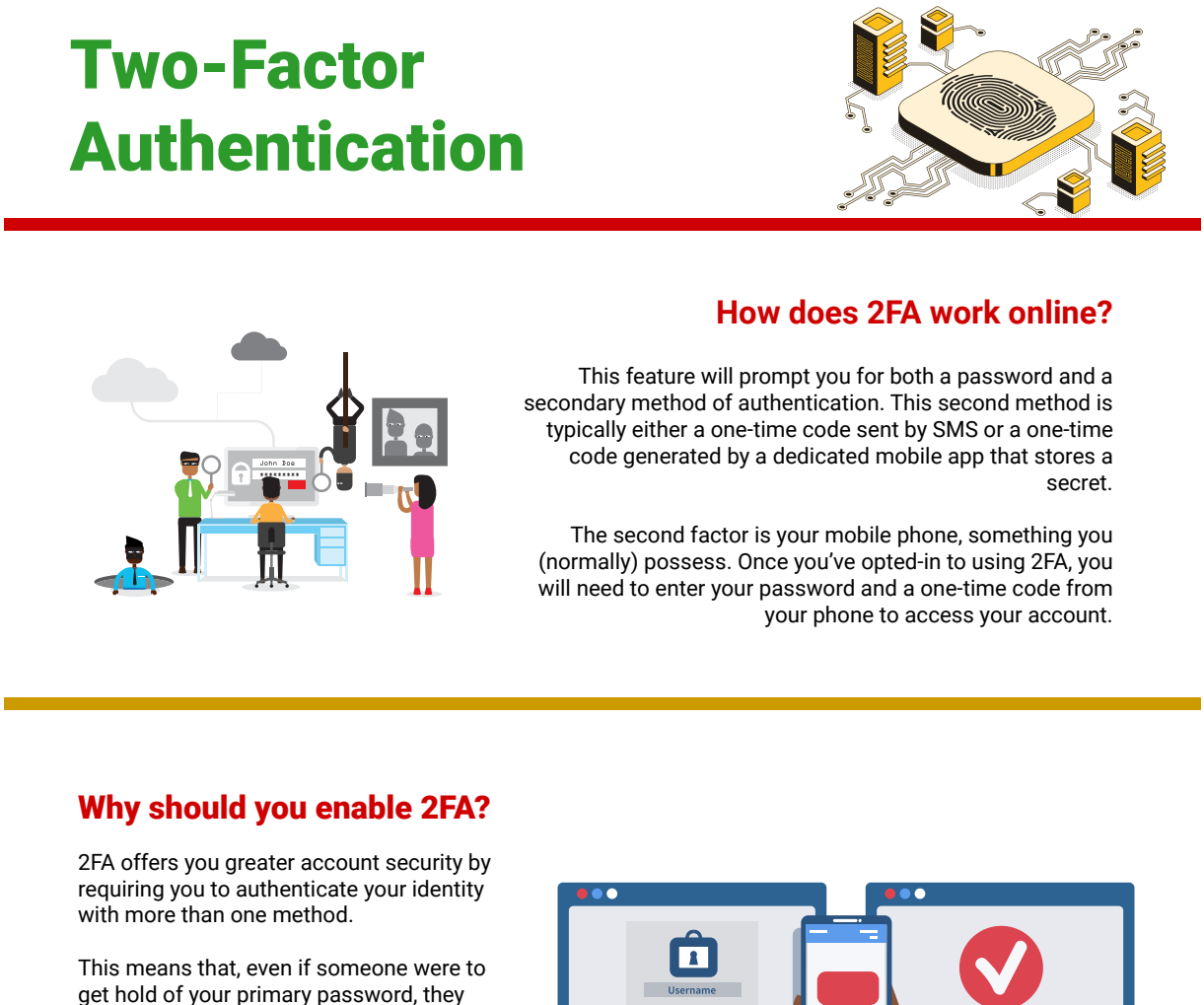


Figure 9: Comment fonctionne l'authentification à 2 facteurs?

L'Authentification à deux facteurs (or "2FA") est un type, ou un sous-ensemble, d'authentification multifactorielle, et c'est un moyen de permettre à un utilisateur de s'identifier auprès d'un fournisseur de services en exigeant une combinaison de deux méthodes d'authentification différentes. Il peut s'agir de quelque chose que l'utilisateur connaît (comme un mot de passe ou un code PIN), de quelque chose que l'utilisateur possède (comme un jeton physique ou un téléphone portable), ou de quelque chose qui est attaché ou inséparable de l'utilisateur (comme ses empreintes digitales).

a. Comment fonctionne cette 2FA en ligne?

Plusieurs services en ligne - dont Facebook, Google et Twitter - proposent la 2FA comme alternative à l'authentification par mot de passe uniquement. Si vous activez cette fonction, un mot de passe et une méthode d'authentification secondaire vous seront demandés. Cette seconde méthode est généralement soit un code temporel envoyé par SMS ou un code à usage unique généré par une application mobile dédiée qui stocke un secret (comme Google Authenticator, Duo Mobile, l'application Facebook ou Clef). Dans les deux cas, le deuxième facteur est votre téléphone portable, que vous possédez (normalement). Certains sites web (dont Google) prennent également en charge les codes de sauvegarde à usage unique, qui peuvent être téléchargés, imprimés sur papier et stockés dans un endroit sûr comme sauvegarde supplémentaire. Une fois que vous avez choisi d'utiliser 2FA, vous devrez entrer votre mot de passe et un code à usage unique depuis votre téléphone pour accéder à votre compte.

b. Pourquoi activer la 2FA?

La 2FA vous offre une plus grande sécurité de compte en vous obligeant à authentifier votre identité par plus d'une méthode. Cela signifie que, même si quelqu'un mettait la main sur votre mot de passe principal, il ne pourrait pas accéder à votre compte à moins d'avoir également votre téléphone portable ou un autre moyen d'authentification secondaire.

c. Y a-t-il des inconvénients à utiliser des 2FA?

Bien que la 2FA offre un moyen d'authentification plus sûr, il existe un risque accru de se voir bloquer son compte si, par exemple, vous égarez ou perdez votre téléphone, changez votre carte SIM[38] ou voyagez dans un pays sans activer l'itinérance. De même, l'utilisation de la 2FA signifie que vous pourriez transmettre plus d'informations à un service que vous ne le souhaitez. Supposons que vous utilisiez Twitter et que vous vous inscriviez en utilisant un pseudonyme.[39] Même si vous évitez soigneusement de donner à Twitter vos informations d'identification, et que vous n'accédez au service que via Tor ou un VPN[40], tant que vous activez le SMS 2FA, Twitter aura nécessairement un enregistrement de votre numéro de téléphone portable. Cela signifie que si un tribunal l'y contraint, Twitter peut relier votre compte à vous via votre numéro de téléphone. Cela peut ne pas être un problème pour vous, surtout si vous

38 https://ssd.eff.org/en/glossary/sim-card
39 https://ssd.eff.org/en/glossary/pseudonym
40 https://ssd.eff.org/en/glossary/vpn

utilisez déjà votre nom légal sur un service donné, mais si le maintien de votre anonymat est important, réfléchissez à deux fois avant d'utiliser le SMS 2FA.

d. Authentification par facteur universel

L'authentification universelle, également connue sous le nom de single sign-on (SSO), est une méthode de vérification de l'identité sur le réseau qui permet aux utilisateurs de naviguer de site en site en toute sécurité sans avoir à saisir plusieurs fois des informations d'identification. Avec l'authentification universelle, un abonné entre un ensemble de paramètres (tels qu'un nom d'utilisateur et un mot de passe) au début de chaque session de réseau. Les données d'authentification pour tout site visité par la suite sont automatiquement générées pendant la durée de cette session. L'un des plus grands défis en matière de sécurité sur Internet est le fait que chaque site Web possède son propre système d'authentification. Un utilisateur typique de l'internet, qui possède deux ou trois adresses électroniques sur le web et qui fréquente une demi-douzaine de vendeurs en ligne pour acheter ou vendre des choses, doit mémoriser plusieurs noms d'utilisateur et mots de passe. Cela peut être difficile à moins que les données d'authentification ne soient écrites ou stockées sous forme de fichier texte, ce qui devient alors un problème de sécurité. L'authentification universelle peut éliminer ce problème sans compromettre la sécurité ou la vie privée.

2.6 Pare-feu

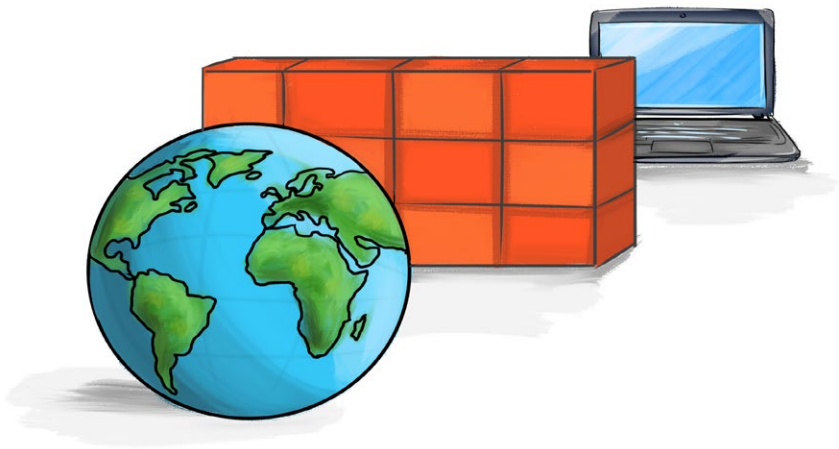


Figure 10: Pare-feu

Système de sécurité des réseaux qui protège un ordinateur contre les connexions indésirables vers ou depuis les réseaux locaux et l'Internet, en particulier les intranets. Les pare-feu peuvent être mis en œuvre sous forme de matériel et de logiciel, ou une combinaison des deux. Un pare-feu[41] peut avoir des règles qui interdisent le courrier électronique sortant ou les connexions

41 https://ssd.eff.org/en/glossary/firewall

à certains sites web. Les pare-feu peuvent être utilisés comme première ligne de défense pour protéger un dispositif contre des interférences inattendues. Ils peuvent également être utilisés pour empêcher les utilisateurs d'accéder à l'internet de certaines manières.

a. Pare-feu matériels et logiciels

Les pare-feu peuvent être matériels ou logiciels, mais la configuration idéale sera constituée des deux. En plus de limiter l'accès à votre ordinateur et à votre réseau, un pare-feu est également utile pour permettre l'accès à distance à un réseau privé par le biais de certificats d'authentification et de connexions sécurisées. Les pare-feu matériels peuvent être achetés en tant que produits autonomes, mais ils se trouvent généralement dans les routeurs à large bande et doivent être considérés comme un élément important de la sécurité de votre système et de la configuration de votre réseau. La plupart des pare-feu matériels disposent d'un minimum de quatre ports réseau pour connecter d'autres ordinateurs, mais pour les réseaux plus importants, une solution de pare-feu de réseau d'entreprise est disponible. Les pare-feu logiciels sont installés sur votre ordinateur, comme tout autre logiciel, et vous pouvez les personnaliser, ce qui vous permet de contrôler leur fonction et leurs caractéristiques de protection. Un pare-feu logiciel protégera votre ordinateur contre les tentatives extérieures de contrôle ou d'accès à votre ordinateur. Les pare-feu peuvent également être un composant du système d'exploitation de votre ordinateur. Par exemple, le pare-feu Windows est une application de Microsoft Windows qui notifie les utilisateurs de toute activité suspecte. L'application peut détecter et bloquer les virus, les vers et les pirates informatiques en cas d'activité nuisible.

a. Techniques de filtrage des pare-feu

Les pare-feu sont utilisés pour protéger les réseaux domestiques et d'entreprise. Un programme ou un dispositif matériel typique de pare-feu filtre toutes les informations qui transitent par l'internet vers votre réseau ou votre système informatique. Il existe plusieurs types de techniques de pare-feu qui empêchent les informations potentiellement dangereuses de passer:

- **Filtre de paquets :** Examine chaque paquet[42] entrer ou sortir du réseau et l'accepter ou le refuser selon des règles définies par l'utilisateur. Le filtrage de paquets est assez efficace et transparent pour les utilisateurs, mais il est difficile à configurer. En outre, il est susceptible de faire l'objet d'une usurpation d'adresse IP [43]
- **Passerelle d'applications :** Applique des mécanismes de sécurité à des applications spécifiques, comme les serveurs FTP[44] et Telnet[45] C'est très efficace, mais cela peut entraîner une dégradation des performances.
- **Passerelle de niveau circuit:** Applique des mécanismes de sécurité quand une connexion TCP[46] ou UDP[47] est établie. Une fois la connexion établie, les paquets

42 https://www.webopedia.com/TERM/P/packet.html
43 https://www.webopedia.com/TERM/I/IP_spoofing.html
44 https://www.webopedia.com/TERM/F/ftp.html
45 https://www.webopedia.com/TERM/T/Telnet.html
46 https://www.webopedia.com/TERM/T/Telnet.html
47 https://www.webopedia.com/TERM/U/User_Datagram_Protocol.html

peuvent circuler entre les hôtes sans autre vérification.

- **Serveur Proxy :** Interception de tous les messages entrant et sortant du réseau. Le serveur proxy[48] dissimule efficacement les véritables adresses de réseau.

En pratique, de nombreux pare-feu utilisent deux ou plusieurs de ces techniques de concert. Un pare-feu est considéré comme une première ligne de défense dans la protection des informations privées. Pour plus de sécurité, les données peuvent être cryptées.

2.7 Cryptage

Le cryptage consiste à brouiller une information ou un message mathématiquement (crypter), de sorte qu'il semble dénué de sens, mais peut néanmoins être restauré dans sa forme originale par une personne ou un dispositif qui possède un élément de données capable de le déchiffrer (une clé de décryptage). Cela limite l'accès à l'information ou au message, car sans la bonne clé, il est presque impossible d'inverser le cryptage et de récupérer l'information originale. Le cryptage est l'une des nombreuses technologies qui composent le domaine appelé cryptographie.

Le cryptage de bout en bout garantit qu'un message est transformé en message secret par son expéditeur initial, et décodé uniquement par son destinataire final. D'autres formes de cryptage peuvent dépendre d'un cryptage effectué par des tiers. Cela signifie qu'il faut faire confiance à ces parties pour le texte original. Le cryptage de bout en bout est généralement considéré comme plus sûr, car il réduit le nombre de parties qui pourraient interférer ou casser le cryptage.

2.8 Réseaux privés virtuels (VPN)

Un réseau privé virtuel (ou VPN) est une méthode permettant de connecter un ordinateur en toute sécurité au réseau d'une organisation située de l'autre côté d'Internet. Lorsque l'on est connecté à un VPN, toutes les données de navigation sur le web semblent provenir du VPN lui-même, plutôt que de son propre fournisseur d'accès à Internet (ou ISP).[49] Les informations sensibles peuvent comprendre les données fournies par les formulaires de contact ou les informations relatives aux cartes de crédit. L'utilisation d'un VPN masque l'adresse IP[50] attribuée par votre FAI aux sites auxquels vous accédez, ce qui ajoute une couche de confidentialité. Outre le masquage de votre adresse IP d'origine, il permet également de crypter vos données lors de leur transfert vers le site auquel vous accédez.

48 https://www.w ebopedia.com/TERM/P/proxy_server.html
49 https://en.wikipedia.org/wiki/Internet_service_provider
50 https://ssd.eff.org/en/glossary/ip-address

a. VPN commerciaux

Un réseau privé virtuel commercial est un service privé qui propose de relayer en toute sécurité vos communications Internet via leur propre réseau. L'avantage de ce système est que toutes les données que vous envoyez et recevez sont cachées des réseaux locaux, ce qui les met à l'abri des criminels, des fournisseurs d'accès Internet locaux peu fiables ou de toute autre personne qui espionne votre réseau local. Un VPN peut être hébergé dans un pays étranger, ce qui est utile à la fois pour protéger les communications d'une administration locale et pour contourner la censure nationale. L'inconvénient est que le trafic est décrypté au niveau des VPN commerciaux[51]. Cela signifie que vous devez faire confiance au VPN commercial (et au pays où il est situé) pour ne pas espionner votre trafic. Si un VPN commercial peut offrir une " protection ", il ne garantit pas nécessairement la sécurité.

b. VPN gratuit

Un VPN gratuit est un service qui vous donne accès à un réseau de serveurs VPN, ainsi qu'aux logiciels nécessaires, sans que vous ayez à payer quoi que ce soit. Si un VPN gratuit peut vous faire "économiser" de l'argent, il peut cependant présenter un risque sérieux de perte de contrôle de vos données. Exemples de VPN: NordVPN,[52] Private Internet Access VPN,[53] Windscribe VPN,[54] CyberGhost VPN,[55] TunnelBear[56] etc.

Note ! Avant de choisir un service VPN, lisez toujours les avis des utilisateurs pour connaître leurs problèmes. En outre, vérifiez toujours la réputation du fournisseur de services VPN et voyez où il se trouve - vous pouvez probablement éviter tout fournisseur de services hébergé dans un pays dont l'historique de sécurité est douteux..

2.9 Navigation Tor

Tor est un logiciel libre et gratuit qui permet de communiquer de manière anonyme. Son nom est dérivé de l'acronyme du nom du projet de logiciel original "The Onion Router". Tor a des fonctionnalités intégrées qui vous protègent du suivi, de la surveillance et des empreintes digitales sur le web.

2.10 DuckDuckGo

DuckDuckGo est un moteur de recherche sur Internet qui met l'accent sur la protection de la vie privée des internautes et évite la bulle de filtres des résultats de recherche personnalisés.

51 https://ssd.eff.org/en/glossary/commercial-vpn
52 https://nordvpn.com/
53 https://www.privateinternetaccess.com/pages/techradar
54 https://windscribe.com/upgrade?promo=WS50OFF&afftag=tomsguide-6233319505430609000&affid=fghzq9e1
55 https://www.cyberghostvpn.com/en_US/?media_source=inhouse_affiliates&lp=pro_homepage&transaction_id=1 020f5087b76582644982b711aa6e1&affiliate=futurenet%2FTechRadar&offer_id=135&coupon=YT2M&conversionpoint=externalCP&channel=External+LPs&affiliate_google_cli
56 https://www.tunnelbear.com

DuckDuckGo se distingue des autres moteurs de recherche en ne profilant pas ses utilisateurs et en montrant à tous les utilisateurs les mêmes résultats de recherche pour un terme de recherche donné.

2.11 Conseils de cyber-sécurité pour le travail à domicile

La nouvelle pandémie de Coronavirus (COVID-19) a contraint le monde à une distanciation sociale, l'une des principales mesures pour contenir la propagation de la COVID-19 et "aplatir la courbe". Cela a obligé de nombreuses organisations à demander à leurs employés de travailler à domicile (télétravail). Le télétravail (travail à domicile), quelle qu'en soit la raison, s'accompagne de ses propres défis en ce qui concerne les menaces à la cyber sécurité. Vous trouverez ci-dessous une liste compilée de directives sur la sécurité du télétravail.

Conseils pour les travailleurs à distance

N'utilisez que le Wi-Fi auquel vous faites confiance. Avec une connexion non sécurisée, les personnes se trouvant à proximité peuvent fouiner dans votre trafic.

- Utiliser des dispositifs homologués par l'entreprise.
- Mettre à jour le logiciel antivirus.
- Mettre à jour tous les logiciels et le système d'exploitation.
- N'oubliez pas de faire des sauvegardes périodiques. Les fichiers importants doivent être sauvegardés régulièrement. Dans le pire des cas, le personnel pourrait par exemple être victime d'une demande de rançon. Dans ce cas, tout est perdu sans sauvegarde.
- Assurez-vous que vous utilisez une connexion sécurisée à votre environnement de travail. Cela signifie que vous utilisez un VPN ou un autre moyen sécurisé comme Teamviewer.
- Méfiez-vous des courriels de phishing. Il faut se méfier de tout courrier électronique demandant de vérifier ou de renouveler vos identifiants, même s'il semble provenir d'une source fiable. Essayez de vérifier l'authenticité de toute demande importante ou suspecte par d'autres moyens, ne cliquez pas sur des liens suspects et n'ouvrez pas de pièces jointes suspectes.

Conseils pour les employeurs

- Se concentrer sur la sécurisation des systèmes qui permettent l'accès à distance, comme les VPN. Veiller à ce que ces systèmes soient entièrement patchés, à ce que les pare-feu soient correctement configurés et à ce que des logiciels anti-malware et de prévention des intrusions soient installés.

- Ne jamais exposer directement le protocole RDP (Remote Desktop Protocol) à l'internet (nécessite une connexion VPN au préalable).
- Mettre en œuvre l'authentification multi-facteurs dans la mesure du possible.
- Pensez à restreindre l'accès aux systèmes sensibles, le cas échéant Envoyez des courriels de sensibilisation au phishing à vos employés
- L'utilisation de logiciels non autorisés à des fins officielles (appelés "shadow IT") peut augmenter lorsque l'on travaille à distance, ce qui augmente les risques en matière de sécurité et de respect de la vie privée. Assurez-vous que le personnel est au courant de la politique, de la confidentialité et des obligations légales qui s'appliquent aux informations de votre entreprise.
- Analysez vos plans d'intervention en cas d'incident et, si nécessaire, mettez-les à jour pour tenir compte du personnel travaillant à distance.
- Analysez vos plans de continuité et d'urgence. Assurez-vous qu'ils sont à jour.

2.12 Video Conferencing Tools

2020 a vu un changement de paradigme majeur dans les réunions traditionnelles in-situ, la plateforme Zoom connaissant un boom parmi tant d'autres. Cette évolution a également été marquée par la multiplication des « Zoom Bombing », où des individus malveillants ont pénétré dans les réunions et perturbé les conférences téléphoniques. Pour éviter ce genre d'incidents, les conseils ci-dessous mettent en évidence les mesures qui peuvent être adoptées.

Conseils pour les vidéoconférences et les groupes de discussion

- Veiller à ce que les participants puissent participer uniquement sur invitation.
- Demander un mot de passe pour participer à la réunion
- Dans la mesure du possible, demander l'approbation de l'administrateur avant que quelqu'un puisse se joindre à la réunion
- Ne pas publier de liens de réunion sur les médias sociaux.
- Veiller à ce que les logiciels de vidéoconférence et de chat soient toujours à jour.

Autres outils de vidéo conférence:

- Jitsi – https://jitsi.org/
- Google Meets – https://apps.google.com/meet/
- BlueJeans – https://www.bluejeans.com
- Signal – https://www.signal.org
- Cisco Webex – https://www.webex.com
- Microsoft Teams – https://teams.microsoft.com

2.13 Menaces sur la sécurité numérique : Malware & Ransomware

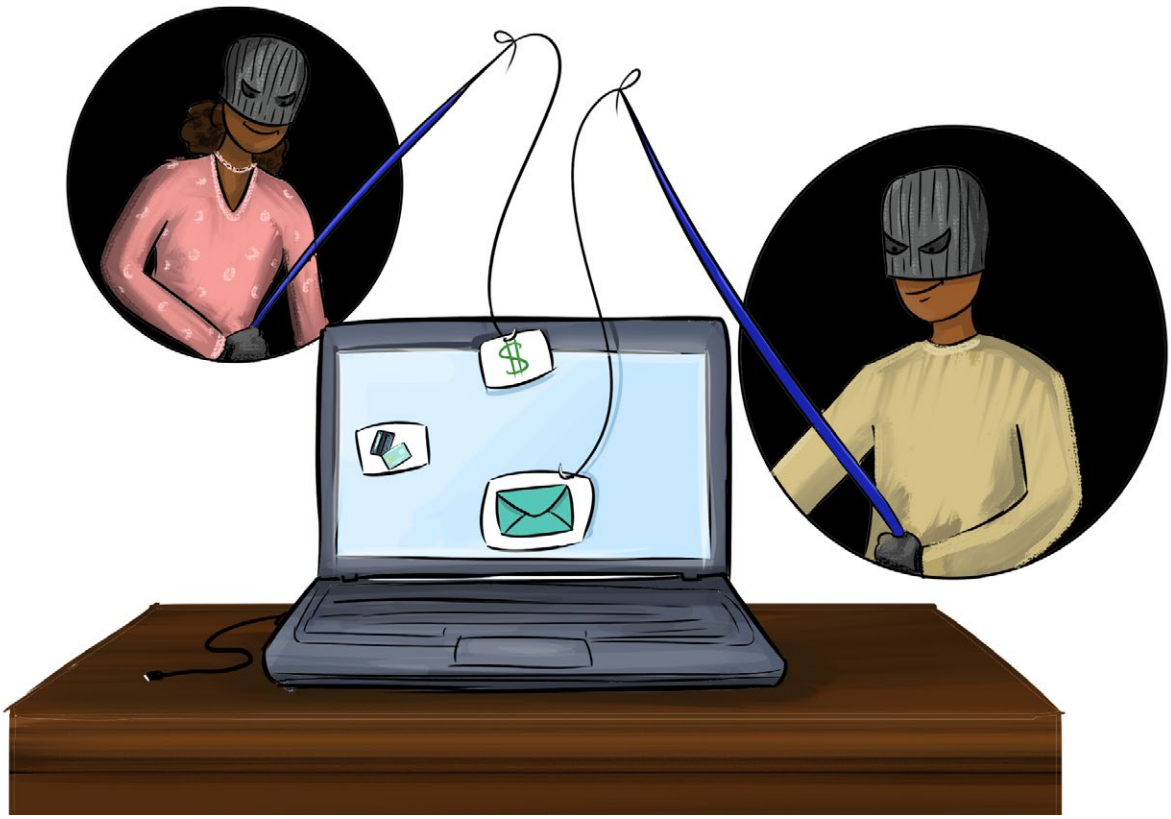


Figure 11: Détection du spam, du phishing, des logiciels malveillants et des virus

a. Malware

Malware est l'abréviation de « malicious software » (logiciel malveillant). Il s'agit d'un programme ou d'un fichier conçu pour être perturbateur, invasif et nuisible à un système informatique. Les types de logiciels malveillants comprennent les virus, les logiciels espions, les logiciels publicitaires et les vers. Ils sont le plus souvent transmis par des pièces jointes de courrier électronique, des messages instantanés, des téléchargements poste à poste, le phishing et des sites web trompeurs. Les épidémies de virus causent des dommages en détruisant les données sur les ordinateurs infectés et/ou en augmentant le trafic réseau en déclenchant des messages électroniques qui transportent le virus vers toutes les adresses électroniques d'un carnet d'adresses ou vers une combinaison aléatoire d'adresses. Si les virus ne sont pas stoppés rapidement, l'afflux de courriels peut inonder les serveurs, perturbant le service de courrier électronique pour tous. Les logiciels antivirus sont identifiables par leurs actions et de nombreux outils sont en place pour combattre la menace qui pèse sur l'ordinateur.

Mesures préventives contre les Malware

Avec un peu d'effort, vous pouvez protéger votre ordinateur et contribuer à éviter des problèmes plus importants. Les étapes suivantes permettront de prévenir une attaque ou de traiter les virus si un ordinateur est infecté.

- Installer un logiciel antivirus[57] sur votre ordinateur.
- Gardez vos définitions de virus à jour[58] même s'il n'y a pas de rapport sur un nouveau virus.
- Ne pas ouvrir ou exécuter une pièce jointe inopinée.[59]
- Désactivez la fonction de prévisualisation dans vos programmes pour une protection accrue.
- Désactivez également toute fonction du programme qui pourrait ouvrir automatiquement un courriel, un message instantané, un fichier joint ou un téléchargement.

b. Ransomware

Les ransomwares sont des logiciels malveillants conçus pour bloquer l'accès à tout ou partie d'un système informatique jusqu'à ce qu'une somme d'argent soit payée. Comme les pirates cherchent à maximiser leur gain, les cibles sont généralement des entités de plus grande taille (entreprises, services, collèges, organisations) qui non seulement sont susceptibles de disposer des fonds, mais qui subissent également une perte importante lorsqu'elles ne peuvent pas accéder à leurs systèmes. Cependant, les individus restent une cible des ransomware car ils peuvent être une porte d'entrée dans les systèmes d'une entreprise. Lorsqu'il s'agit de prévenir ou de détecter les ransomwares, il n'y a pas de solution miracle. Cependant, vous pouvez utiliser quelques-unes des techniques suivantes pour prévenir et détecter les ransomwares, ce qui peut vous aider à réduire le risque d'obtenir des logiciels malveillants.

Mesures préventives contre les Ransomware

- **Limiter l'accès au réseau de partage de fichiers :**
  N'autorisez que le niveau d'accès requis par la fonction commerciale de l'utilisateur. Limiter l'accès aux partages de fichiers du réseau empêchera un ordinateur infecté par un logiciel rançon de le propager à d'autres ordinateurs du réseau.
- **Garder toutes les applications à jour :**
  Assurez-vous que toutes les applications sont à jour. Les applications obsolètes qui n'ont pas les correctifs de sécurité les plus récents les rendent vulnérables aux ransomwares et autres logiciels malveillants.
- **Utiliser un Anti-virus :**
  Un antivirus est un outil qui aide à détecter et à supprimer les logiciels malveillants de votre ordinateur. Vous devez toujours garder un antivirus à jour pour vous permettre de détecter et de nettoyer les logiciels malveillants qui pourraient avoir été installés

57 https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus
58 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/updates-patching
59 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing

sur votre ordinateur.

2.14 Surveillance et surveillance de masse

Cela comprend le suivi de la localisation, l'inspection approfondie des paquets, la reconnaissance faciale, la surveillance de masse et l'interception des communications. La surveillance a un effet néfaste sur la volonté des écrivains et des journalistes de faire des recherches et de publier des articles, et rend plus difficile la protection des sources.

2.15 Attaques de phishing

Les campagnes de "phishing" ou de "spear phishing" utilisent souvent des liens ou des pièces jointes dans les e-mails ou sur les médias sociaux qui véhiculent des logiciels malveillants. Une fois que l'on clique sur ces liens, ils peuvent causer des dommages importants. Les logiciels malveillants peuvent permettre aux pirates d'obtenir toutes les informations qu'ils souhaitent à partir d'un ordinateur compromis, y compris les informations personnelles, les données et les sources d'un journaliste.

2.16 Attaques de faux domaines

Il s'agit de sites web créés pour usurper l'identité de personnes légitimes à des fins malveillantes. Les médias indépendants et les sites web de la société civile en ont souvent été victimes. Les faux sites servent à diffuser des logiciels malveillants ou à publier de fausses informations dans le but de discréditer le vrai site médiatique ou un journaliste en particulier.

2.17 Attaques de l'homme du milieu (MitM)

Les pirates s'insèrent entre un utilisateur et un site cible. Par exemple, un routeur sans fil est configuré pour agir comme un point d'accès Wi-Fi dans un lieu public, afin de faire croire aux gens qu'il est légitime. Lorsque des personnes s'y connectent, le pirate a un accès instantané aux données qui passent par le routeur.

2.18 Attaques par déni de service (DoS)

Ces attaques sont assez courantes et impliquent qu'un ou plusieurs ordinateurs et connexions Internet inondent un serveur de trafic, le rendant ainsi inaccessible aux autres. Pour les

journalistes, ces attaques empêchent l'information d'atteindre le public et peuvent devenir coûteuses, car le nombre de visiteurs diminue et une aide technique est nécessaire.

2.19 Cyber-harcèlement

Le cyber harcèlement désigne l'utilisation d'Internet ou d'autres moyens électroniques pour traquer ou harceler une personne, un groupe ou une organisation. Il peut s'agir de fausses accusations, de diffamation, de calomnie. Il peut également comprendre la surveillance, l'usurpation d'identité, les menaces, le vandalisme ou la collecte d'informations pouvant être utilisées pour menacer, humilier ou harceler.

2.20 Cyber-intimidation

La cyber-intimidation est l'utilisation de moyens électroniques tels que le courrier électronique, les médias sociaux, la messagerie instantanée et d'autres formes de communication en ligne dans le but d'abuser, d'intimider ou de dominer un individu ou un groupe.

Resources

1. https://tinyurl.com/y2kkmckg
2. https://tinyurl.com/y37nrxd7
3. https://tinyurl.com/yyu2y5ub
4. https://tinyurl.com/yxzfprhj
5. https://tinyurl.com/y25p5q3e
6. https://tinyurl.com/y3szuuhz
7. https://tinyurl.com/y692p5yw
8. https://tinyurl.com/yy92uvrc
9. https://tinyurl.com/y28vrj7z
10. https://tinyurl.com/yxpd2vpg

Chapitre III

3.1 Sécurité numérique et physique

a. La sécurité numérique lors des manifestations

À un moment ou à un autre de leur travail, les acteurs des droits numériques se retrouvent impliqués dans des manifestations pour faire entendre leur voix. Le port de dispositifs numériques lors de ces manifestations peut toutefois être utilisé contre les manifestants, étant donné que les groupes chargés de l'application de la loi disposent d'outils de surveillance numérique, tels que de fausses tours de téléphonie mobile et une technologie de reconnaissance faciale, qui peuvent être utilisés pour identifier les manifestants et surveiller leurs mouvements et leurs communications, mettant ainsi en péril leur sécurité et leur vie privée. Avant de se rendre à des manifestations pacifiques, les manifestants doivent prendre en compte leur vie privée numérique. Voici quelques éléments à prendre en compte.

b. Garder la préparation de la manifestation privée

Le fait de disposer d'un service de réseau privé virtuel digne de confiance peut aider les organisateurs de manifestations à dissimuler leur trafic Internet. Les manifestants peuvent également utiliser des outils tels que le navigateur Tor60, qui masquent l'activité en ligne d'un utilisateur en bloquant les traqueurs et en cryptant plusieurs fois le trafic de leur réseau. Il est également très important de s'assurer que les manifestations sont organisées au moyen d'applications cryptées de bout en bout plutôt que par des messages en texte clair (comme les SMS)

c. Chiffrement intégral des disques des appareils numériques

Si votre appareil est confisqué par les forces de l'ordre, perdu ou volé, le cryptage intégral du disque peut en fin de compte contribuer à protéger les données stockées sur votre appareil. Les appareils Android[60] et iOS[61] sont dotés de capacités de chiffrement intégral intégrées. Ces capacités doivent être protégées par des mots de passe robustes pour éviter toute intrusion par le biais d'une force brute.

d. Installer Signal

Signal est une application disponible à la fois sur iOS[62] et Android[63] qui propose un cryptage puissant de bout en bout pour protéger à la fois les messages textes et les appels vocaux. En plus du cryptage des communications individuelles, Signal permet le cryptage des discussions de groupe. L'application a également ajouté récemment la possibilité de faire disparaître les messages entre 10 secondes et une semaine après leur première lecture. Contrairement

60 https://source.android.com/security/encryption/full-disk.html
61 https://www.apple.com/business/docs/iOS_Security_Guide.pdf
62 https://ssd.eff.org/en/module/how-use-signal-ios
63 https://ssd.eff.org/en/module/how-use-signal-android

à certains autres services comme SnapChat, ces messages éphémères ne seront jamais stockés sur un serveur et sont supprimés de votre appareil après avoir disparu.

e. Sauvegardez vos données

Prenez des précautions pour limiter les coûts potentiels liés à la perte d'accès à votre appareil, qu'il soit perdu, volé ou confisqué par les forces de l'ordre. Sauvegardez régulièrement vos données et conservez cette sauvegarde dans un endroit sûr pour vous éviter des maux de tête plus tard.

f. Téléphone jetable

Pour les manifestants qui craignent que leur téléphone soit surveillé, une solution temporaire mais idéale serait de se procurer un téléphone " jetable ", un appareil prépayé ou payé en liquide et utilisé dans le but exprès de rester en contact avec les gens pendant une manifestation pacifique. Les téléphones jetables peuvent permettre aux utilisateurs de rester en contact avec les gens, surtout si les choses deviennent difficiles, sans exposer toutes les données de leur appareil de tous les jours. Une autre solution consiste à mettre votre téléphone en mode avion, ce qui pourrait servir le même objectif. Pour en savoir plus, consultez le site https://ssd.eff.org/en/module/attending-protest.

g. Sécurité physique

La menace physique qui pèse sur les militants des droits numériques est aussi réelle que les menaces à la sécurité numérique. Ces menaces vont des arrestations, du harcèlement, de la confiscation des appareils et de la détention par des acteurs étatiques. Cela les expose à un risque potentiellement élevé, un facteur qui met en péril leur sécurité. Afin d'atténuer les menaces à la sécurité physique, les militants des droits numériques sont invités à être attentifs aux signes de menace à leur sécurité personnelle, en tenant compte de leur environnement, des lois et du type de personnes dans la communauté. La règle de base est la suivante : pour qu'un acteur des droits numériques parvienne à protéger les autres, sa propre sécurité doit être garantie.

3.2 Réduire les menaces à la sécurité physique

Pour limiter les risques, les acteurs du secteur des droits numériques doivent prendre en considération les éléments suivants :

a. Accepter le risque:

Accepter le risque signifie que la victime qui a besoin de protection doit pouvoir savoir qu'elle peut être en danger dans l'exercice de ses activités. Avec une telle conscience, la personne

est censée être prête à atténuer le risque ou le potentiel de risque. Par exemple, lorsque vous allez effectuer un travail humanitaire dans une zone de guerre, vous devez savoir que votre sécurité est en jeu ; vous devez donc être prêt à courir si nécessaire, à appeler à l'aide et vous devez contacter et expliquer votre mission aux combattants impliqués dans les combats afin qu'ils puissent vous accorder l'accès à la zone. En outre, lorsque vous savez que vos données peuvent être exposées à des risques de cyber-attaque. Si vous souhaitez lancer une attaque, vous devez créer un mot de passe fort, vérifier les faits concernant les plateformes numériques que vous comptez utiliser, partager vos données avec des personnes de confiance et stocker vos données sur différents supports de stockage.

b. Éviter les risques:

Connaître le risque est une chose et l'éviter en est une autre. Lorsque vous apprenez l'existence d'un risque, vous devez l'éviter par tous les moyens ; vous n'avez pas besoin de revendiquer des droits ou du pouvoir à ce moment-là. Pour éviter le risque, votre communication et vos actions doivent refléter et/ou changer en fonction de la situation dans laquelle vous vous trouvez. C'est-à-dire que vous devez contrôler votre langage corporel et utiliser vos mots à bon escient, vous devez évaluer l'environnement avant de commencer toute activité ou de vous engager avec des personnes, vous devez comprendre s'il y a un risque potentiel ou non, et enfin, lorsqu'il s'avère que vous êtes une cible, vous devez réagir avec vigueur pour résister à votre agresseur.

c. Vous devez avoir et présenter votre idéologie aux bonnes personnes:

Votre idéologie peut vous mettre en danger lorsque vous la faites connaître. En tant que défenseur des droits de l'homme, vous devez avoir un certain niveau de connaissances sur les personnes à qui vous confiez vos informations ou auxquelles vous vous associez, car les gens ne sont pas obligés d'accepter vos idées.

d. En tant que représentant d'une organisation, vous devez en savoir plus sur vous-même et sur l'organisation :

Pour éviter les risques en tant que leader, vous devez savoir qui vous êtes, ce que vous faites et les personnes que vous représentez. Il est très important que vous sachiez où vous allez ; cette préparation est très utile lorsque vous êtes en détention préventive en tant que suspect. La façon dont vous vous présentez, votre position et votre organisation ont une influence significative sur la façon dont vous serez traité par vos gardiens. Dans la plupart des cas, le suspect innocent sera libéré après s'être présenté correctement. Le langage corporel, le choix des mots et le calme total doivent être bien gérés pendant l'arrestation et l'enquête.

e. Contexte:

Que ce soit dans votre région, en dehors de votre région ou n'importe où dans le monde, vous devez tenir compte des questions suivantes et y répondre : "Qui suis-je ? Où suis-je ? Qui sont-

ils ? Ces questions sont très importantes car, quelles que soient les activités que vous menez, vous devez prendre en considération les questions ci-dessus pour votre sécurité. Par exemple, un défenseur des droits de l'homme ne peut pas se trouver dans les casernes de l'armée et condamner les atrocités commises par les soldats ; cela révèle l'absence de recoupement en répondant aux questions ci-dessus et en ne prenant pas en considération les mesures de sécurité dans le cadre de votre profession et les facteurs externes. En pareil cas, vous risquez d'être arrêté et détenu pour avoir exprimé votre opinion devant eux et dans leurs locaux..

f. Éviter les zones à risques :

Les zones comme les limites des villes, les foules, les banques, les zones de circulation, les rassemblements publics, les zones de conflit ou de guerre, etc. sont des zones à risque et nous devons apprendre quand et à quelle heure nous rendre dans ces zones, en tenant compte de votre profession et de votre position. Par exemple, il n'est pas conseillé à un militant des droits de l'homme de se rendre dans des zones de conflit sans la garantie d'être à l'abri des belligérants. L'étude de cas concerne les régions anglophones du Cameroun où il y a un conflit entre les séparatistes et les forces gouvernementales ; pour leur sécurité, les travailleurs humanitaires ne peuvent pas accéder aux zones de confrontation sans la garantie d'un passage sûr de la part des combattants. En effet, ils peuvent être blessés par des balles perdues, arrêtés ou kidnappés s'ils ne sont pas assurés de leur sécurité par les combattants..

g. Vêtements:

vous devez être conscient de votre apparence et savoir comment vous habiller lorsque vous menez des activités humanitaires. Par exemple, si vous êtes un travailleur humanitaire, lorsque vous allez travailler sur le terrain, vous devez porter des chaussures légères et vous habiller de manière à pouvoir facilement vous échapper d'une scène ou courir lorsque le besoin s'en fait sentir. Si votre zone n'est pas sécurisée, évitez de porter ou de vous habiller de manière coûteuse dans ces zones car vous pourriez être ciblé en fonction de la manière dont ils ont observé que vous vous habillez. Évitez de contacter des personnes que vous ne connaissez pas dans les zones isolées, car elles peuvent représenter une menace pour votre sécurité, et évitez de porter des vêtements trop serrés, car cela pourrait vous empêcher de courir en cas de besoin.

h. Ne pas résister sous la menace d'un fusil ou dans les casernes:

Lorsque vous êtes arrêté, kidnappé ou entouré de voleurs, faites ce qu'ils veulent que vous fassiez afin de protéger votre vie. Ne résistez pas parce qu'ils peuvent vous tuer ; pensez d'abord à votre sécurité.

i. Ayez tout ce dont vous avez besoin lorsque vous partez en mission, y compris une trousse de premiers secours:

Chaque fois que vous êtes en mission, en tant que leader/acteur, vous devez emporter, en plus

de vos besoins de base, des quantités raisonnables tenant compte de votre santé, de votre voyage, des conditions climatiques du lieu, des conditions financières, de votre instinct, etc. Il s'agit de votre sécurité physique, car vous devez accepter le risque et prévoir les solutions possibles avant de partir en mission.

j. Avoir toujours un contact de confiance et de réseautage:

Dans toutes les professions, surtout lorsqu'il s'agit de métiers à risques comme l'activisme en faveur des droits de l'homme, vous devez prévoir le risque d'arrestation, d'enlèvement et/ou d'attaque de vos données. Comme facteurs atténuants, vous devez avoir des personnes de confiance à qui vous pouvez communiquer vos informations, y compris le lieu où vous vous rendez, le moment où vous êtes attendu sur place, le moment où vous êtes attendu de retour, ce qui est prévu au cas où il y aurait un appel à l'inquiétude, etc.

k. Conserver, connaître et mémoriser les contacts d'urgence :

Vous devez disposer de numéros de contact d'urgence tels que ceux de la police, des services d'ambulance, des pompiers, de l'hôpital, etc. Téléchargez et installez des applications qui peuvent suivre votre appareil lorsque vous êtes en difficulté. Pour en savoir plus : https://tinyurl.com/y5wje4zk

Ressources

11. https://tinyurl.com/y34p99o6
12. https://tinyurl.com/yy4t25hm
13. https://tinyurl.com/y2nn2ot9
14. https://tinyurl.com/y32w6ra
15. https://tinyurl.com/y369rudo
16. https://tinyurl.com/y6arpfw6
17. https://tinyurl.com/y85p49a3
18. https://tinyurl.com/y33cxu2u
19. https://tinyurl.com/y5wje4zk
20. https://tinyurl.com/y6spa5zk
21. https://tinyurl.com/y4tv7srz

Chapitre IV

4.1 Coupures d'Internet

Figure 12: Arrêt d'Internet

L'article 19 de la Déclaration universelle des droits de l'homme garantit à tout individu le droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit. Toutefois, ces dernières années, on a constaté une tendance accrue des États africains à recourir au contrôle de l'information sur leurs citoyens. Cela a fait d'Internet un espace plus volatile, et le nombre de défis posés aux activistes, aux défenseurs des droits de l'homme, aux dissidents et aux journalistes serait en augmentation[64] r

64 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/

Les régimes autoritaires ont eu recours à des outils et des tactiques numériques tels que la fermeture d'Internet, la censure en ligne et la surveillance numérique pour réprimer la liberté d'expression. Selon Freedom on the Net 2018[65] de Freedom House, "les gouvernements du monde entier resserrent le contrôle sur les données des citoyens et utilisent les allégations de "fausses nouvelles" pour réprimer la dissidence, érodant ainsi la confiance dans l'internet ainsi que les fondements de la démocratie". Un rapport du CIPESA de 2018 a révélé que jusqu'à 22 gouvernements africains avaient ordonné des interruptions de réseau au cours des quatre dernières années et que depuis le début de 2019, 6 pays africains - Algérie, République démocratique du Congo (RDC), Tchad, Gabon, Soudan et Zimbabwe - ont connu des fermetures d'Internet.

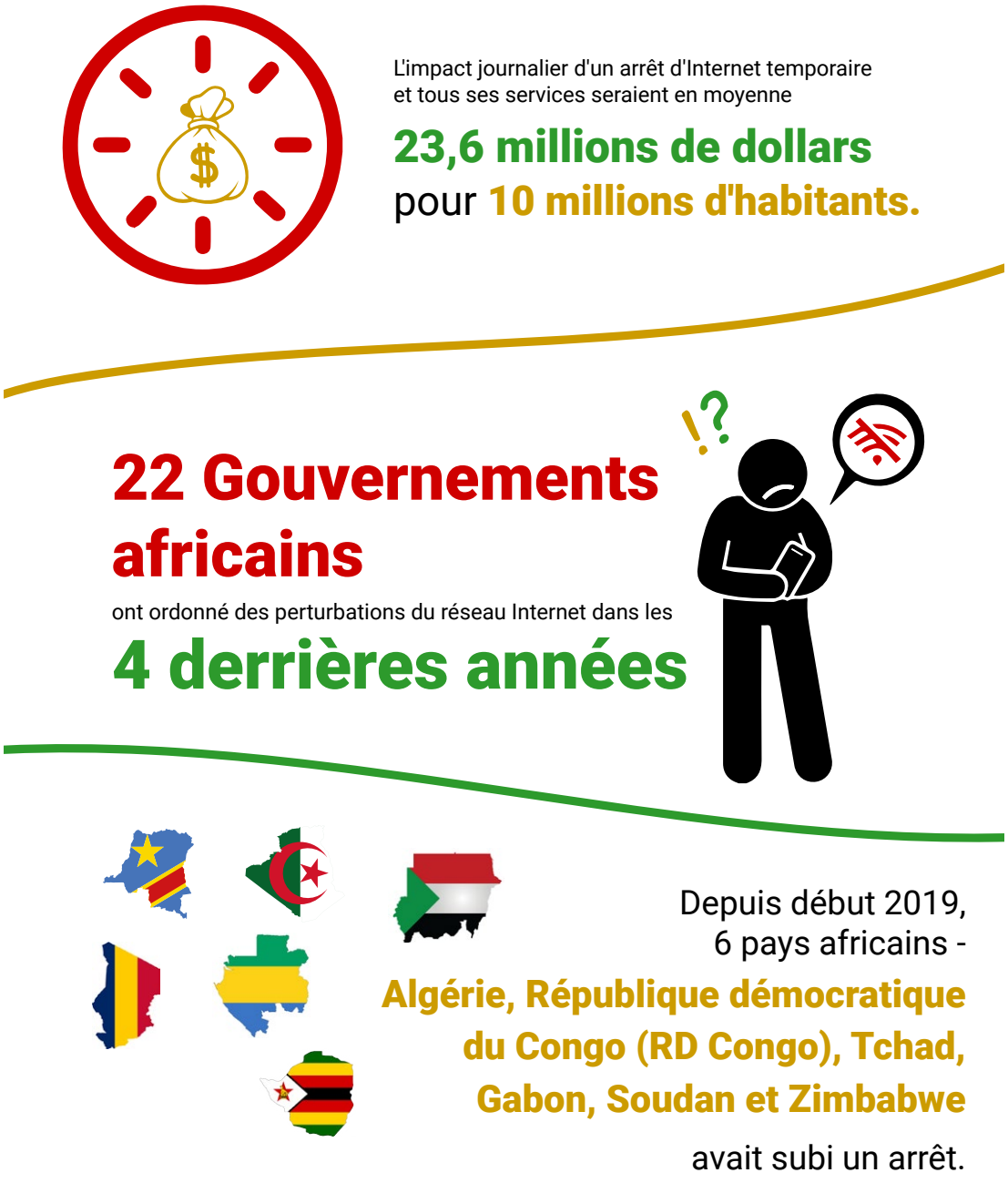


Figure 13: Données d'arrêt d'Internet en Afrique

65 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/

En outre, un rapport de Paradigm Initiative 2019[66] a révélé qu'un certain nombre de gouvernements africains ont fermé l'Internet pour des raisons politiques, en adoptant des réglementations strictes sur le contenu en ligne, et/ou en utilisant des attaques ciblées de logiciels espions contre les défenseurs des droits de l'homme. Le rapport ajoute que cette exportation des modèles chinois et russes de tactiques dites "d'État de droit" pour contrôler l'Internet a entraîné un renforcement du contrôle gouvernemental et des violations des droits numériques par le biais d'une législation qui est ostensiblement rédigée pour promouvoir l'ordre public dans les sociétés africaines. Ces fermetures ont eu des répercussions économiques négatives dans les pays en question. Une étude de Deloitte[67] révèle que pour un pays fortement connecté à l'internet, l'impact journalier d'une fermeture temporaire de l'internet et de tous ses services serait en moyenne de 23,6 millions de dollars pour 10 millions d'habitants. En dépit de cette décision de divers États de restreindre les espaces numériques et, ce faisant, de limiter le travail de ceux qui sont en première ligne pour défendre les droits de l'homme et les droits numériques, un certain nombre d'outils d'anonymat et de contournement d'Internet, tels que les VPN et les serveurs proxy basés sur le Web, offrent de l'espoir aux acteurs des droits de l'homme, aux défenseurs des droits numériques, aux journalistes et aux lanceurs d'alerte, entre autres.

4.2 Contourner les fermetures d'Internet et la censure

L'anonymat sur Internet et les outils de contournement tels que les VPN, les navigateurs Tor et les pserveurs proxy basés sur le Web offrent un espoir aux acteurs des droits de l'homme, aux défenseurs des droits numériques, aux journalistes et aux lanceurs d'alerte, entre autres.

a. Réseau privé virtuel (VPN)

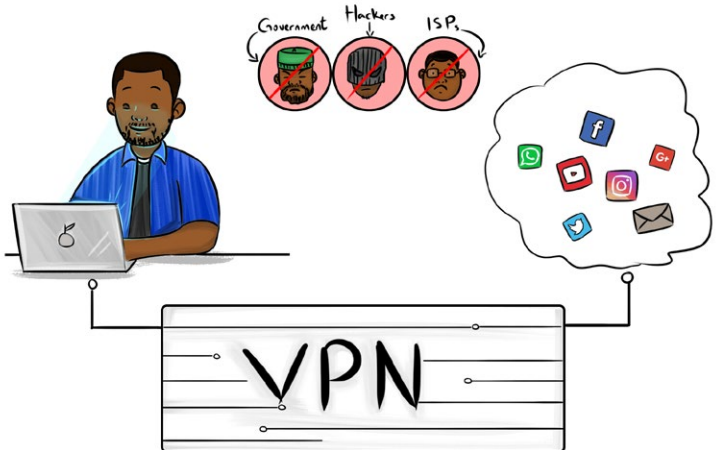


Figure 14: Utilisation des VPN

66 http://paradigmhq.org/download/dra19/
67 https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the- economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html

Comme nous l'avons déjà expliqué au chapitre II dans la partie consacrée à la sécurité numérique, un réseau privé virtuel (VPN) est une méthode permettant de connecter votre PC et/ou un appareil connecté à Internet de manière sécurisée au réseau d'une organisation située de l'autre côté d'Internet. Lorsque vous utilisez un VPN, toutes vos communications Internet sont regroupées, cryptées, puis relayées à cette autre organisation, où elles sont décryptées, décompressées, puis envoyées à leur destination. Pour le réseau de l'organisation, ou tout autre ordinateur sur l'Internet élargi, il semble que la demande de votre ordinateur vienne de l'intérieur de l'organisation, et non de votre emplacement. Les VPN sont utilisés par des particuliers pour contourner la censure locale ou pour déjouer la surveillance locale.

4.3 Mesurer les coupures d'Internet et la censure

a. L'observatoire ouvert des interférences de réseau (OONI)

L'Open Observatory of Network Interference (OONI) est un projet de logiciel libre qui vise à renforcer les efforts décentralisés pour accroître la transparence de la censure sur Internet dans le monde. L'OONI développe des logiciels libres et open source[68] appelé **OONI Probe** que l'on peut utiliser pour mesurer :

- Le blocage des sites web;
- Le blocage des messageries instantanées (WhatsApp, Facebook Messenger et Telegram);
- Le blocage des outils de contournement de la censure (comme Tor et Psiphon);
- La présence de systèmes (middleboxes) dans votre réseau qui pourraient être responsables de censure et/ou de surveillance; et
- La vitesse et les performances de votre réseau.

En lançant OONI Probe,[69] vous avez la possibilité de collecter des données qui peuvent potentiellement servir pour prévoir la censure d'internet puisqu'il vous montre comment, quand, où et par qui elle est mise en œuvre.

4.4 Sensibilisation contre les fermetures d'Internet en Afrique

a. Le coût de l'outil d'arrêt (COST)

COST est un outil en ligne basé sur des données qui permet de mesurer le coût des coupures d'Internet et de convaincre les gouvernements de maintenir l'Internet en service. L'outil permet à quiconque - journalistes, chercheurs, défenseurs, décideurs politiques, entreprises et bien d'autres - d'estimer rapidement et facilement le coût économique des interruptions de l'Internet. S'appuyant sur les méthodologies élaborées par la Brookings Institution[70] et

68 https://github.com/ooni/probe
69 https://ooni.org/install/
70 https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

le CIPESA[71], l'outil Cost of Shutdown Tool (COST) estime le coût économique des coupures d'internet, des coupures de données mobiles et des restrictions des médias sociaux en utilisant des milliers d'indicateurs régionaux de la Banque mondiale, de l'UIT, d'Eurostat et du recensement américain.

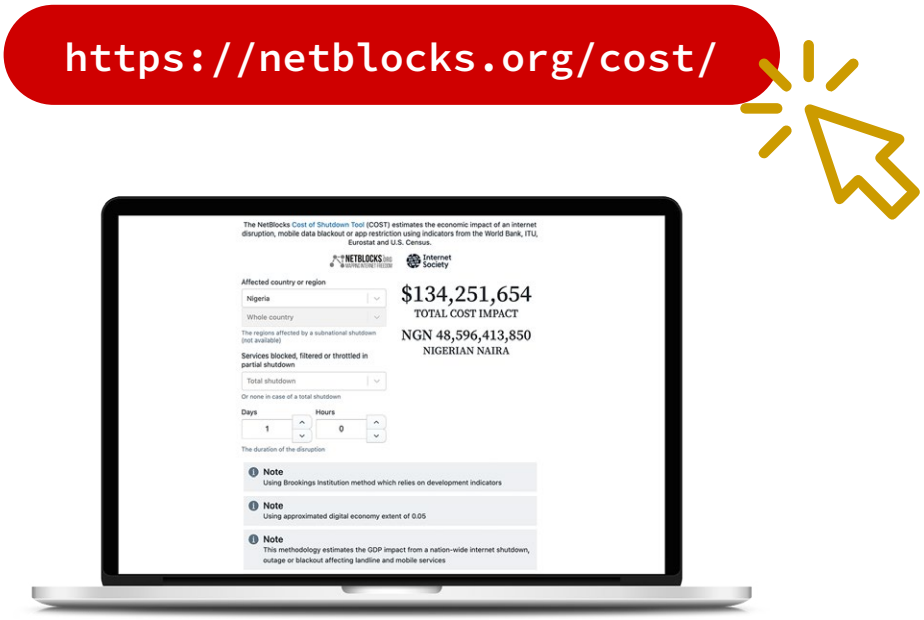


Figure 15: Plaidoyer contre les coupures d'Internet en Afrique

b. Campagne #KeepItOn

Cette campagne mondiale, menée par AccessNow, vise à exhorter les gouvernements du monde entier à ne pas fermer l'Internet et à permettre la libre circulation de l'information..

71 https://cipesa.org/

Ressources

1. https://tinyurl.com/y4sul3dd
2. https://tinyurl.com/y5xxucxy
3. https://tinyurl.com/y49ckklq
4. https://tinyurl.com/y669mw6v
5. https://tinyurl.com/y6dhe2o4
6. https://tinyurl.com/y46tnwuk

Glossaire

Add-on - Un add-on est un logiciel qui modifie un autre logiciel en changeant son fonctionnement ou ses capacités. Souvent, les add-ons peuvent ajouter des fonctions de confidentialité ou de sécurité aux navigateurs web ou aux logiciels de messagerie électronique. Certains modules complémentaires sont des logiciels malveillants, il faut donc veiller à n'installer que ceux qui sont reconnus et proviennent de sources officielles.

Anonymat – La condition d'anonymat

Anti-virus - Un logiciel anti-virus est un logiciel pour votre PC utilisé pour prévenir, détecter et supprimer les logiciels malveillants, y compris les virus informatiques, les vers et les chevaux de Troie. Quelques exemples de logiciels anti-virus sont McAfee, Avast, AVG et Kaspersky.

Censure - La censure de l'Internet est le contrôle ou la suppression de ce qui peut être consulté, publié ou visualisé sur l'Internet, promulgué par les autorités de régulation ou les gouvernements.

Contournement – L'utilisation de diverses méthodes et outils pour contourner la censure sur Internet.

Cryptographie - L'art de concevoir des codes secrets qui vous permettent d'envoyer et de recevoir des messages à un destinataire sans que les autres puissent comprendre le message

Hygiène numérique - Désigne l'organisation des fichiers sur votre PC, le verrouillage de vos comptes de médias sociaux, l'introduction de nouvelles applications ou technologies pour rendre votre vie numérique plus facile ou plus sûre.

Droits numériques - Les droits numériques sont principalement des droits de l'homme à l'ère de l'internet.

Cryptage - Un processus qui prend un message et le rend illisible sauf pour une personne qui sait comment le "décrypter" pour le remettre sous une forme lisible.

Clé de cryptage - Une clé de cryptage est un élément d'information qui sert à convertir un message en une forme illisible. Dans certains cas, vous avez besoin de la même clé de cryptage pour décoder le message. Dans d'autres cas, la clé de cryptage et la clé de décryptage sont différentes.

Pare-feu - Un outil qui protège un ordinateur contre les connexions indésirables vers ou

depuis les réseaux locaux et l'Internet. Un pare-feu peut avoir des règles qui interdisent le courrier électronique sortant ou les connexions à certains sites web. Les pare-feu peuvent être utilisés comme première ligne de défense pour protéger un appareil contre les interférences inattendues. Ils peuvent également être utilisés pour empêcher les utilisateurs d'accéder à l'internet de certaines manières.

Coupures internet – Une coupure d'Internet est une perturbation intentionnelle de l'Internet ou des communications électroniques, les rendant inaccessibles ou effectivement inutilisables, pour une population spécifique ou dans un lieu donné, souvent pour exercer un contrôle sur le flux d'informations

Adresse IP – Une adresse IP (Internet Protocol) est ce qui identifie de manière unique les appareils connectés sur l'internet.

Malware - Malware est l'abréviation de malicious software, c'est-à-dire des programmes conçus pour effectuer des actions indésirables sur votre appareil. Les virus informatiques sont des logiciels malveillants. Tout comme les programmes qui volent des mots de passe, vous enregistrent secrètement ou effacent vos données.

Système d'exploitation (OS) - Un programme qui exécute tous les autres programmes sur un ordinateur ou un appareil. Windows, Linux, Android et les systèmes d'exploitation OS X et iOS d'Apple sont tous des exemples de systèmes d'exploitation.

Gestionnaire de mots de passe. Un gestionnaire de mots de passe est un outil qui crée et stocke des mots de passe pour vous, afin que vous puissiez utiliser plusieurs mots de passe différents sur différents sites et services sans avoir à les mémorise.

Phrase secrète - Une phrase secrète est une sorte de mot de passe, mais elle est plus longue qu'un mot de passe qui est généralement composé d'un seul mot.

PC (Personal Computer)- Un ordinateur multi-usage

PGP - PGP ou Pretty Good Privacy a été l'une des premières applications populaires de la cryptographie à clé publique. PGP a été développé par Phil Zimmermann1991 pour aider les militants et autres personnes à protéger leurs communications.

Proxy – Un proxy est une application ou un appareil serveur qui sert d'intermédiaire pour les demandes des clients qui recherchent des ressources auprès des serveurs qui fournissent ces ressources. Un serveur proxy fonctionne donc pour le compte du client lorsqu'il demande un service, masquant potentiellement la véritable origine de la demande au serveur de ressources.

Question de sécurité - Il s'agit de requêtes liées à un mot de passe dont vous seul êtes censé connaître la réponse.

Logiciel – Il s'agit d'un terme générique utilisé pour désigner les applications, les scripts et les programmes qui fonctionnent sur un appareil

Tor- Tor est un logiciel libre et gratuit qui permet de communiquer de manière anonyme. Le nom est dérivé d'un acronyme du nom du projet de logiciel original "The Onion Router".

Authentification à deux facteurs (2FA) - L'authentification à deux facteurs (ou "2FA") est un moyen de permettre à un utilisateur de s'identifier auprès d'un fournisseur de services en exigeant une combinaison de deux méthodes d'authentification différentes. Il peut s'agir de quelque chose que l'utilisateur connaît (comme un mot de passe ou un code PIN), de quelque chose que l'utilisateur possède (comme un jeton matériel ou un téléphone portable), ou de quelque chose qui est attaché ou inséparable de l'utilisateur (comme ses empreintes digitales).

URL (Uniform Resource Locator) - L'adresse d'une page Internet.

Virtual Private Network (VPN)– Un réseau privé virtuel est un réseau auquel nous pouvons accéder pour nous connecter à l'internet via un tunnel crypté. Notre fournisseur d'accès Internet, ou quiconque fouillant dans le Wi-Fi gratuit que nous utilisons pour accéder au web, ne peut voir que notre connexion au service VPN, tandis que le site web que nous visitons n'enregistrera qu'une connexion provenant des serveurs VPN. Pour décider quel est le meilleur VPN pour vous, lisez ce guide.

Virus - Un virus pour PC est un morceau de code capable de se copier et a généralement un effet néfaste, comme la corruption d'un système informatique ou la destruction de données. Proxy sur le Web - Un site web qui permet à son utilisateur d'accéder à d'autres sites web, bloqués ou censurés. En général, le proxy web vous permet de saisir une adresse web (ou URL) sur une page web, puis de réafficher cette adresse web sur la page du proxy. Plus facile à utiliser que la plupart des autres services de contournement de la censure.

AYETA

Digital Rights Toolkit

PARADIGM INITIATIVE

ParadigmHQ.org

@ParadigmHQ

/ParadigmHQ

/ParadigmHQ

Kingdom of the Netherlands

Stanford PACS
Center on Philanthropy and Civil Society
—
Digital Civil Society Lab