الأمن الرقمي
وحماية المعلومات

الحق في استخدام شبكة آمنة

HRDO
هردو

مركز هردو
لدعم التعبير الرقمي
HRDO CENTER
To Support the Digital Expression

الأمن الرقمي
وحماية المعلومات
الحق في استخدام
شبكة آمنة

مركز هردو لدعم التعبير الرقمي
القاهرة ٢٠١٧

الأمن الرقمي وحماية المعلومات

الحق في استخدام شبكة آمنة

مركز هردو

لدعم التعبير الرقمي

www.hrdoegypt.org

info@hrdoegypt.org

المحتويات

تمهيد	٥
الأمان الرقمي	٦
الخصوصية على شبكة الإنترنت	٦
معايير ضمان المعلومات	٧
الأمن الرقمي في الدستور المصري	٨
الاتجاهات الدولية لتعزيز ودعم الأمان الرقمي	٨
كيف تحظي بخدمة آمنة من خلال بعض الخطوات	١٣
تطبيقات ينصح باستخدامها للصحفيين والمدافعين عن حقوق الإنسان للتمتع بمستوي حماية أفضل	١٤
نصائح لاستخدام هواتف ذاكية آمنة	١٦
بعض الخطوات الأساسية لتشفير الأجهزة الذكية	١٨
خمس أدوات لحماية حساباتك على وسائل التواصل الاجتماعي	١٨
إشارات مرجعية	٢١

تمهيد

في العام ٢٠١٧، حيث وصلت ثورة المعلومات والتكنولوجيا إلى درجة قد تفوق الاستيعاب، وأصبح أكثر من نصف سكان العالم مستخدمين لشبكة الإنترنت، وأصبحت الشبكة العنكوبتية مجتمع كبير لا تفصله الحدود يوفر الإتاحة وبيئة التواصل والعمل والتوثيق والتخزين لكل المستخدمين من البشر بل فاقت كمان الإماكانات التكنولوجية والرقمية تلك الحدود بكثير. أصبح الحديث عن الحقوق المرتبطة بالوجود على الإنترنت لا جدال فيه ولا يحتمل تباطؤ في الإقرار وفرض الالتزامات على الدول في كل ما يخص الخصوصية والأمان الشخصي وحرية التعبير والرأي والحق في الثقافة والتعلم والحق في الوصول والإتاحة وكل تلك الحقوق الإنسانية الأصيلة.

وفي هذا العصر الذي أصبح كثير من النشطاء والصحفيين والمدافعين عن حقوق الإنسان في دول عدة نشاطهم الرئيسي على الأنترنت ويحتاجون إلى معايير من الأمان تضمن سلامتهم الشخصية وتلك المعايير قد يهدمها مجهود الأنظمة شديدة المراقبة في التتبع والاختراق وايضا عدم اهتمام وحذر أي شخص من المنظومة بما قد يحدد مكانه وهويته ونوع المحتوى وتفاصيله ويعصف بسلامة الفرد أو الفريق..أصبح الحديث عن الأمان الرقمي على مستويين أولهما ضبط أداء الدول والتزاماتها تجاه حماية الأمن الرقمي والحريات الرقمية وأيضا توعية وتنبيه المستخدمين إل كيفية حماية أمنهم الرقمي والعمل على تطوير نظم الحماية بما يتوافق مع معاييير حماية الأمن القومي وبدون توسع غير مقبول فيما يعرف بالأمن القومي.

لهذا يصدر مركز هردو هذا التقرير للتأكيد على مسألة الأمن الرقمي وموقعها من الأهتمام وبعض الخطوات الأساسية لضمان حماية جيدة أثناء التواجد على شبكة الإنترنت.

الأمان الرقمي

المقصود بالأمان الرقمي هو كيفية استخدام شبكة الإنترنت استخدام فعال بدون التعرض لأي تهديدات أو مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات.

وفي إطار ثورة التكنولوجيا والمعلومات والتطور المتسارع للتقنيات الرقمية، وبعد أن أصبح أكثر من نصف سكان العالم مستخدمون نشطون للإنترنت ومواقع التواصل الاجتماعي، وأصبحت وسائل التواصل الاجتماعي هي الطريقة الأسهل للتواصل بين الأفراد والمجموعات وتبادل المعلومات سواء على الصعيد المهني أو الأنساني، أصبح النشاط الرقمي يحتك بالحريات والحق في الخصوصية والأمان في مقابل رغبة الدول في السيطرة على الفضاء الرقمي والتجسس على مواطنيها أو التحكم في نشاطاتهم أو على صعيد آخر المراقبة المخابراتية لرصد نشاط بعض الأفراد أو اختراق حساباتهم، وربما تكون عمليات تهديد السلامة من أفراد وعصابات للوصول إلى معلومات تهدد صاحبها ويمكن استغلالها.

في ظل كل تلك الفوضى والإتاحة وصراعات القوى والأنظمة الدائمة مع الحقوق والحريات الإنسانية نشأ مفهوم الأمن الرقمي لحماية الأفراد والجماعات والمنظمات من التهديدات والمخاطر التي قد يواجهونها عند استخدام شبكة الإنترنت.

الخصوصية على شبكة الإنترنت

تنص المادة (١٢) من الإعلان العالمي لحقوق الإنسان على "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات."، فالحق في حماية كل فرد لحياته ومعلوماته الخاصة مكفول بالمواثيق الدولية وحق أصيل من حقوق الإنسان. وتعد الخصوصية ببساطة هي الحد الذي يفصل بين ما يحق للآخرين أو المجتمع معرفته عن حياتنا الخاصة وما لا يحق للآخرين أو المجتمع معرفته عن حياتنا الخاصة. وبتعبير آخر تعني قدرة أو حق شخص أو مجموعة من الأشخاص في البت في ما يمكن نشره من معلومات عنهم على العلن وما لا يمكن نشره.

وفي عدد من دول العالم تعد انتهاكات الخصوصية الفردية جريمة يعاقب عليها القانون، وانتهاكات الخصوصة مجرمة بدرجات في كل دول العالم، حسب درجة

تبني تلك الدولة لمفاهيم حرية وحقوق المواطنين. على سبيل المثال تعد سوريا من الدول التي كانت تنتهك خصوصيات مواطنيها وتجبر مقاهي ونوادي الإنترنت على الاحتفاظ بسجلات بأسماء وأرقام هوية مستخدمي الإنترنت وفترات الاستخدام مع تسجيلات كاملة للاستخدام دون علم الزوار.

كما تقوم عدد من الدول باختراق وتعقب الهواتف الجوالة والذكية عبر حصولها على بيانات الاتصال المتعلقة بأي شخص تريده عبر سلطتها القانونية على شركات الاتصال، وتملك بعض السلطات الحق في التنصت على المكالمات وتسجيلها أو تعطي لنفسها هذا الحق بما يخالف القانون.

والخصوصية عبر الإنترنت قد تكون معلومات تحدد شخصية مستخدم الإنترنت كتاريخ الميلاد والاسم الحقيقي والصورة الشخصية وعنوان الشخص أو رقم جواز سفره (PII)، أو معلومات غير محددة للشخصية (non-PII) مثل سلوك زائر ما لموقع ما على الإنترنت، أو سرية محادثات شخصية أو بيانات مقصورة على عدد محدد من الأفراد.

معايير ضمان المعلومات

هناك ثلاثة معايير أساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بمثلث أو ثلاثي CIA، وهي السرية والأمانة والتوافر.

ويقصد بالسرية عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء الرقمي. وتعني الأمانة عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحيث يضمن المستخدم دقة نقل ما يريد من معلومات دون تدخل في أثناء النقل أو التخزين أو المعالجة. أما فيما يخص التوافر فهو استمرار توفر المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة.

ودائما ما يهتم المطورون والعاملون في مجال الأمن الرقمي والأمن المعلوماتي على ضمان الثلاث عناصر بشكل أساسي من خلال وسائل تقنية وإجرائية تناسب المستخدمين وتوفر لهم الحماية.

الأمن الرقمي في الدستور المصري

مادة (٥٧): "للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون.

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها بشكل تعسفي، وينظم القانون ذلك ".

مادة (٦٥): "حرية الفكر والرأي مكفولة. ولكل إنسان حق التعبير عن رأيه بالقول أو الكتابة أو التصوير أو غير ذلك من وسائل التعبير والنشر."

الاتجاهات الدولية لتعزيز ودعم الأمان الرقمي

إن الحديث عن العالم الرقمي الذي أصبح ملتقى التجمع والوجود الافتراضي العالمي هو حديث عن مجمل منظومة الحقوق الإنسانية بنقل تطبيقها على الواقع الطبيعي إلى تطبيقها على الفضاء الرقمي، وبالتالي تخضع معايير الأمن الرقمي لحق الإنسان الأصيل في الخصوصية و حرية الرأي والتعبير وحرية التنظيم وحرية اعتناق أراء أو عقائد معينة وبعبارة أكثر وضوحا "كل ما يخضع لمنظومة حماية حقوق الإنسان على الأرض، يخضع لنفس المنظومة على شبكة الإنترنت".

- **ميثاق حقوق الإنترنت لجمعية الاتصالات المتقدمة (APC)**

تم وضع ميثاق حقوق الإنترنت على يد جمعية الاتصالات المتقدمة في ورشة عمل حقوق شبكة الإنترنت في جمعية الاتصالات المتقدمة بأوروبا، والتي تم عقدها في براغ، في فبراير عام ٢٠٠١. وهذا الميثاق يقوم على ميثاق الاتصالات الشعبي وهو يهدف إلى تطوير سبع أفكار رئيسية، هي:

الوصول إلى الإنترنت للجميع، وحرية التعبير وحرية التنظيم، والوصول إلى المعارف والتعليم المشترك والتأليف – البرمجيات مفتوحة المصدر المجانية وتطوير التقنيات، والخصوصية والمراقبة والتشفير، وحوكمة الإنترنت، وحماية الوعي وإعمال الحقوق. وتذكر جمعية الاتصالات المتقدمة أن القدرة على مشاركة المعلومات والتواصل بحرية باستخدام شبكة الإنترنت أمر ضروري من أجل إعمال

حقوق الإنسان على النحو المجسد في الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية والعهد الدولي الخاص بالحقوق المدنية والسياسية واتفاقية القضاء على جميع أشكال التمييز ضد المرأة.

- **القمة العالمية حول مجتمع المعلومات (WSIS) ٢٠٠٣**

في ديسمبر عام ٢٠٠٣، تم عقد القمة العالمية حول مجتمع المعلومات (WSIS) تحت رعاية الأمم المتحدة. وبعد مفاوضات طويلة بين الحكومات والشركات وممثلي المجتمع المدني، تم تبني إعلان مبادئ القمة العالمية حول مجتمع المعلومات، والذي يعيد التأكيد على حقوق الإنسان:

" إننا نعيد تأكيدنا على شمولية كل حقوق الإنسان والحريات الأساسية وعدم تجزئتها والترابط بينها، بما في ذلك حق التطوير على النحو الموضح في إعلان فيينا. كما أننا نعيد تأكيدنا كذلك على أن الديمقراطية والتطوير المستدام واحترام حقوق الإنسان والحريات الأساسية بالإضافة إلى الحوكمة الرشيدة على كل المستويات هي عوامل مترابطة ويقوي بعضها بعضاً. كما أننا نعقد العزم كذلك على تقوية سيادة القانون في الشئون الدولية وكذلك الشئون القومية".

كما يشير إعلان القمة العالمية حول مجتمع المعلومات بشكل خاص إلى أهمية حق حرية التعبير في "مجتمع المعلومات" :

" نحن نؤكد مجدداً على أن للجميع الحق في حرية الرأي والتعبير، كأساس ضروري لمجتمع المعلومات، وكما هو موضح في البند ١٩ من الإعلان العالمي لحقوق الإنسان، وأن هذا الحق يشتمل على الحرية في تبني الآراء بدون تدخل، بالإضافة إلى الحق في البحث عن المعلومات والأفكار وتلقيها ونقلها عبر أية وسيط بغض النظر عن الحدود. ويعد الاتصال عملية اجتماعية جوهرية، وحاجة بشرية أساسية، كما أنها تعد بمثابة الأساس لكل المنظمات الاجتماعية. وهو أمر مركزي في مجتمع المعلومات. ويجب أن تتاح الفرصة للجميع في كل مكان للمشاركة، ويجب ألا يتم استثناء أي شخص من الامتيازات التي يوفرها مجتمع المعلومات".

كما أقر إعلان مبادئ القمة العالمية حول مجتمع المعلومات كذلك "بأنه من الضروري منع استخدام موارد وتقنيات المعلومات للأغراض الجنائية والإرهابية، مع احترام حقوق الإنسان.".

- **قرار الجمعية العمومية للأمم المتحدة بشأن حماية الحق في الخصوصية الرقمية**

عندما أصبحت مناقشة الحقوق الرقمية تحتاج إلى تركيز خاص ومساحات مباشرة وليش ربط بحزمة الحقوق الإنسانية الأصيلة التي تم إقرارها دوليا، جاء قرار الجمعية العامة للأمم المتحدة رقم ١٦٦/٦٩ بشأن الحق في الخصوصية في العصر الرقمي والذي جاء نصه :

" إن الجمعية العامة، إذ تؤكد من جديد مقاصد ميثاق الأمم المتحدة ومبادئه، وإذ تؤكد من جديد أيضا حقوق الإنسان والحريات الأساسية بصيغتها المكرسة في الإعلان العالمي لحقوق الإنسان ومعاهدات حقوق الإنسان الدولية ذات الصلة، بما في ذلك العهد الدولي الخاص بالحقوق المدنية والسياسية والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، وإذ تؤكد من جديد كذلك إعلان وبرنامج عمل فيينا، وإذ تشير إلى قرارها ١٦٧/٦٨ المؤرخ ١٨ كانون الأول/ديسمبر ٢٠١٣ بشأن الحق في الخصوصية في العصر الرقمي، وإذ ترحب باتخاذ مجلس حقوق الإنسان القرار ١٣/٢٦ المؤرخ ٢٦ حزيران/يونيه ٢٠١٤ بشأن تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، وإذ ترحب أيضا بعمل مفوضية الأمم المتحدة لحقوق الإنسان بشأن الحق في الخصوصية في العصر الرقمي وإذ تلاحظ مع الاهتمام تقريرها عن هذا الموضوع، وإذ تشير إلى حلقة النقاش بشأن الحق في الخصوصية في العصر الرقمي المعقودة خلال الدورة السابعة والعشرين لمجلس حقوق الإنسان، وإذ تلاحظ تقرير المقرر الخاص لمجلس حقوق الإنسان المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، وتقرير المقرر الخاص للمجلس المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، وإذ تلاحظ مع التقدير التعليق العام رقم ١٦ الصادر عن اللجنة المعنية بحقوق الإنسان بشأن حق الشخص في أن تُحترم خصوصياته وشؤون أسرته وبيته ومراسلاته وفي التمتع بالحماية اللازمة لشرفه وسمعته، وإذ تلاحظ أيضا في الوقت نفسه القفزات التكنولوجية الواسعة التي حصلت منذ اعتماد التعليق، وإذ تسلم بالحاجة إلى مواصلة القيام، استنادا إلى القانون الدولي لحقوق الإنسان، بمناقشة وتحليل المسائل المتصلة بتعزيز وحماية الحق في الخصوصية في العصر الرقمي، والضمانات الإجرائية والرقابة وسبل الانتصاف المحلية الفعالة، وأثر المراقبة على الحق في الخصوصية وغيره من حقوق الإنسان، والحاجة إلى دراسة مبادئ عدم التعسف والمشروعية، وجدوى تقييمات الضرورة والتناسب فيما يتعلق بممارسات المراقبة،

وإذ تلاحظ الاجتماع العالمي لأصحاب المصلحة المتعددين بشأن مستقبل إدارة الإنترنت المعقود في ساو باولو، البرازيل، في نيسان/أبريل ٢٠١٤، وإذ تسلم بأن

التصدي بفعالية للتحديات المرتبطة بالحق في الخصوصية في سياق تكنولوجيا الاتصالات الحديثة سيتطلب العمل المتواصل والمتضافر من جانب أصحاب المصلحة المتعددين، وإذ تلاحظ أيضا أن سرعة وتيرة التطور التكنولوجي تمكن الأشخاص في العالم بأسره من استخدام تكنولوجيات المعلومات والاتصالات الجديدة، وتعزز في الوقت نفسه قدرة الحكومات والشركات والأشخاص على مراقبة الاتصالات واعتراضها وجمع البيانات، مما قد يؤدي إلى انتهاك حقوق الإنسان أو النيل منها، ولا سيما الحق في الخصوصية، على النحو المبين في المادة ١٢ من الإعلان العالمي لحقوق الإنسان، والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية، وتشكل بالتالي مسألة تثير قلقا متزايدا، وإذ تؤكد من جديد حق الإنسان في الخصوصية الذي لا يسمح بتعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصياته أو في شؤون أسرته أو بيته أو مراسلاته، وحقه في التمتع بحماية القانون من مثل هذا التدخل، وإذ تسلم بأن ممارسة الحق في الخصوصية أمر مهم لإعمال الحق في حرية التعبير والحق في اعتناق الآراء دون مضايقة والحق في حرية التجمع السلمي وتكوين الجمعيات، وهي إحدى الدعائم التي يقوم عليها المجتمع الديمقراطي، وإذ تؤكد أهمية الاحترام التام لحرية استقاء المعلومات وتلقيها ونقلها للغير، بما في ذلك الأهمية الأساسية للوصول إلى المعلومات والمشاركة الديمقراطية، وإذ تلاحظ أن البيانات الوصفية يمكن أن تترتب عليها فوائد، ولكن أنواعا معينة من البيانات الوصفية، إذا تم تجميعها، يمكن أن تكشف عن المعلومات الشخصية، ويمكن أن يُستشف منه سلوك الشخص، وعلاقاته الاجتماعية، وأفضلياته الخاصة وهويته،

وإذ تشدد على أن مراقبة الاتصالات و/أو اعتراضها على نحو غير قانوني أو تعسفي وجمع البيانات الشخصية على نحو غير قانوني أو تعسفي، أمور تنتهك الحق في الخصوصية ويمكن أن تمس بالحق في حرية التعبير وقد تتعارض مع مبادئ المجتمع الديمقراطي، باعتبارها أعمالا تدخلية بدرجة كبيرة، بما في ذلك عند الاضطلاع بها على نطاق واسع،

وإذ تلاحظ بوجه خاص أن مراقبة الاتصالات الرقمية يجب أن تكون متسقة مع الالتزامات الدولية المتصلة بحقوق الإنسان وأن تتم بالاستناد إلى إطار قانوني متاح للعموم وواضح ودقيق ومستفيض وخال من التمييز، وأن أي مساس بالحق في الخصوصية يجب ألا يكون تعسفيا أو غير قانوني، مع مراعاة ما هو معقول لتحقيق أهداف مشروعة، وإذ تذكِّر بأن الدول الأطراف في العهد الدولي الخاص بالحقوق المدنية والسياسية عليها أن تتخذ الخطوات اللازمة لاعتماد القوانين أو التدابير الأخرى اللازمة لإعمال الحقوق المعترف بها في العهد،

وإذ تؤكد أنه يجب على الدول احترام التزاماتها الدولية في مجال حقوق الإنسان فيما يتعلق بالحق في الخصوصية عندما تعترض الاتصالات الرقمية للأشخاص و/أو

تجمع البيانات الشخصية وعندما تتطلب الإفصاح عن البيانات الشخصية من أطراف ثالثة، بما في ذلك الشركات الخاصة،

وإذ تشير إلى أن مؤسسات الأعمال التجارية تتحمل مسؤولية احترام حقوق الإنسان، على نحو ما هو مبين في مبادئ الأمم المتحدة التوجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون "الحماية والاحترام والانتصاف"، وإذ يساورها بالغ القلق من التداعيات السلبية على ممارسة حقوق الإنسان والتمتع بها من جراء مراقبة الاتصالات و/أو اعتراضها، بما في ذلك مراقبة الاتصالات و/أو اعتراضها خارج إقليم الدولة، وكذلك جمع البيانات الشخصية، ولا سيما عندما تجرى على نطاق واسع،

وإذ تلاحظ مع بالغ القلق أنه في العديد من البلدان كثيرا ما يواجه العاملون في مجال تعزيز حقوق الإنسان والحريات الأساسية والدفاع عنها، من أشخاص ومنظمات، تهديدات ومضايقات ويعانون من انعدام الأمن، فضلا عن المساس بشكل تعسفي أو غير قانوني بحقهم في الخصوصية، بسبب أنشطتهم،

وإذ تلاحظ أن الشواغل المتصلة بالأمن العام قد تبرر جمع وحماية بعض المعلومات الحساسة، ولكن يجب على الدول ضمان التقيد التام بالتزاماتها بموجب القانون الدولي لحقوق الإنسان،

وإذ تلاحظ أيضا في هذا الصدد أن منع وقمع الإرهاب هو مصلحة عامة ذات أهمية كبيرة، مع التأكيد مجددا على أن الدول يجب أن تكفل توافق أي تدابير تتخذها لمكافحة الإرهاب مع التزاماتها بموجب القانون الدولي، ولا سيما القانون الدولي لحقوق الإنسان والقانون الدولي للاجئين والقانون الدولي الإنساني،

١ - تؤكد من جديد الحق في الخصوصية، الذي لا يسمح بتعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصياته أو في شؤون أسرته أو بيته أو مراسلاته، وحقه في التمتع بحماية القانون من مثل هذا التدخل على النحو المبين في المادة ١٢ من الإعلان العالمي لحقوق الإنسان والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية؛

٢ - تسلم بالطبيعة العالمية والمفتوحة للإنترنت وبالتقدم السريع في مجال تكنولوجيا المعلومات والاتصالات كقوة دافعة لتسريع خطى التقدم على طريق التنمية بمختلف أشكالها؛

٣ - تؤكد أن الحقوق نفسها التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحظى بالحماية أيضا على الإنترنت، بما في ذلك الحق في الخصوصية؛

٤ – تهيب بالدول كافة القيام بما يلي:

(أ) أن تحترم وتحمي الحق في الخصوصية، بما في ذلك في سياق الاتصالات الرقمية؛

(ب) أن تتخذ ما يلزم من تدابير لوضع حد لانتهاكات تلك الحقوق، وأن تعمل على تهيئة الظروف الكفيلة بالحيلولة دون حدوث هذه الانتهاكات، بطرق منها ضمان توافق تشريعاتها الوطنية في هذا الصدد مع التزاماتها بموجب القانون الدولي لحقوق الإنسان؛

(ج) أن تعيد النظر في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجمع البيانات الشخصية، بما في ذلك مراقبة الاتصالات واعتراضها وجمع البيانات على نطاق واسع، وذلك بهدف تأكيد الحق في الخصوصية عن طريق ضمان تنفيذ جميع الالتزامات المترتبة عليها بموجب القانون الدولي لحقوق الإنسان تنفيذا كاملا وفعليا؛

(د) أن تنشئ آليات رقابة محلية قضائية و/أو إدارية و/أو برلمانية نزيهة ومستقلة وفعالة ومزودة بموارد كافية وقادرة على ضمان الشفافية، حسب الاقتضاء، والمساءلة بشأن مراقبة الدولة للاتصالات واعتراضها وجمع البيانات الشخصية، أو أن تقوم بتعهد آليات الرقابة القائمة؛

(هـ) أن تتيح للأشخاص الذين انتُهكت حقوقهم في الخصوصية نتيجة المراقبة التعسفية أو غير القانونية سبل الانتصاف الفعالة بما يتسق مع الالتزامات الدولية في مجال حقوق الإنسان؛

٥ – تشجع مجلس حقوق الإنسان على أن يُبقي باب المناقشة مفتوحا بهدف تحديد وتوضيح المبادئ والمعايير وأفضل الممارسات فيما يتعلق بتعزيز وحماية الحق في الخصوصية، وأن ينظر في إمكانية وضع إجراء خاص لهذا الغرض؛

٦ – تقرر أن تُبقي هذه المسألة قيد نظرها."

• كيف تحظى بخدمة آمنة من خلال بعض الخطوات !

الحديث عن الأمن الرقمي خاصة حينما نخاطب نشطاء وصحفيين ومدافعين عن حقوق الإنسان، ليس فقط حديثا دوليا ووطنيا عن إلتزام الدولة والوصول لقواعد دولية تحد من انتهاك الحقوق الرقمية والأمن الرقمي ومعايير الخصوصية، بل يأتي معه على التوازي نصائح بأهم الإجراءات الواجب اتباعها عند استخدام الوسيط الرقمي أو شبكة الإنترنت للتمتع بخدمة آمنة ومعايير خصوصية أعلى..وهنا نورد بعض الخطوات الأساسية لتأمين استخدام خدمة الإنترنت.

كيف تنشئ كلمة مرور قوية

١. تحتوي على ما لا يقل عن عشرة أحرف.
٢. تتضمن حرفاً واحداً على الأقل من كل فئة من الفئات التالية:
   – الأحرف الكبيرة
   – الأحرف الصغيرة
   – الأرقام
   – الأحرف الخاصة (مثل ! و@ و&)
٣. ليست أبداً هي نفسها – أو تحتوي على أي جزء من – اسم المستخدم الخاص بك.
٤. لا تحتوي أبداً على معلومات شخصية عنك أو عن أقاربك أو حيواناتك الأليفة.
٥. لا تحتوى أبداً على تسلسلات مفهومة من الأحرف أو الأرقام (على سبيل المثال "١ ٢ ٣ ..." أو "A B C").
٦. لا تحتوي على أجزاء كبيرة كتلك الموجودة بالقاموس.
٧. إحدى الطرق لجعل كلمة المرور الحالية أقوى – وخاصةً لمقاومة برامج التخمين الآلي – هو جعلها أطول.

- **تطبيقات ينصح باستخدامها للصحفيين والمدافعين عن حقوق الإنسان للتمتع بمستوى حماية أفضل:**

١. أونيون شير - OnionShare

والذي تتيح لأي شخص المشاركة الآمنة للملفات من أي حجم. وعوضاً عن نقل المعلومات الحساسة التي تقدمها المصادر في أجهزة التخزين (يو إس بي) أو أجهزة محمولة، يمكن للصحفيين مشاركتها في هذا الموقع المؤقت الذي لا يمكن تعقبه.

هذه الأداة مثل دروب بوكس ولكن مشفرة وموثوق بها. وبمجرد أن يقوم الشخص بتحميل الملف، يمكن محوه من الخادم ولا يصبح من الممكن لأي شخص الوصول له"، كما أوضح لي. إذا أراد مراسل أو مصدر إرسال ملفات، تنشئ الأداة عنوان **URL** وكلمة مرور يمكن مشاركتها عبر رسائل مشفرة. ويمكن أن تكون هذه الأداة مفيدة للصحفيين المستقلّين في التواصل مع المبلغين عن المخالفات.

٢.تور ماسنجر - Tor Messenger

إذا كنت معتاداً على مشروع تور وهو أفضل وسيلة حالياً للتنقل عبر الإنترنت دون ترك أثر، ستكون سعيد بمعرفة أنه دشن مؤخراً تور ماسنجر. تسهّل الأداة العابرة للمنصات الدردشة المشفرة على مجموعة متنوعة من الشبكات مثل فيس بوك وجي تشات. وأوصى لي بتشغيله مع جابر أو زمب وهي "خوادم لامركزية مملوكة من قبل منظمات غير ربحية في مجال الخصوصية مهتمة أكثر من الشركات العملاقة بحفظ البيانات الخاصة بك آمنة".

٣. أوبن أركيف - OpenArchive

أوبن أركيف هو تطبيق على الهاتف المحمول، يسعى للحفاظ على وسائل الإعلام السمعي البصري المدنية بطريقة آمنة. يلتقط الكثير من المواطنين والصحفيين صوراً لانتهاكات حقوق الإنسان أو مشاهد فيديو لوحشية الشرطة، ويترددون في وضعها على وسائل التواصل الاجتماعي على الفور"، كما أوضحت مؤسسة أوبن أركيف. "هم يريدون إعطائها لشخص يثقون به، لذلك يمكنهم تحميله على أوبن أركيف باستخدام اسم مستعار إذا لزم الأمر، ويجعله التطبيق متاحاً على نطاق واسع لفترة طويلة".

التطبيق، حالياً في مرحلة الاختبار للأندرويد، يستخدم تكنولوجيا تور للهواتف المحمولة للسماح للأشخاص على الأرض بإرسال الصور الحساسة دون الخوف من التعقب. ويحصل كل المحتوى الذي يتم تحميله على أوبن أركيف على رخصة المشاع الإبداعي. ومن المخطط أن يكون بالإمكان البحث في هذا المحتوى في المستقبل.

٤. كي بايز - Keybase

كي بايز هو دليل مفتوح للمفاتيح العامة التي يمكنك التحقق منها من خلال حسابات وسائل التواصل الاجتماعي. ويمكن استخدام مفتاح عام جنباً إلى جنب مع مفتاح خاص لتشفير الرسائل بشكل فعّال. إذا كان هناك مصدر يرسل لك بريد إلكتروني مشفّر وتريد أن تتحقق من أن هذا الشخص موثوق به، فدليل كي بايز يمكن أن يخبرك لمن هذا المفتاح، اعتماداً على ملفه أو ملفها الشخصي على تويتر، ورديت، وجيثب، وبيتكوين، وأسماء النطاقات. "هذه الأداة هي نسخة تجريبية، لذلك فهي تحتاج للمزيد من التطوير ليتم التحقق منها من خلال فيس بوك أو إينستجرام"، كما يقول جيرمي ستريبلينج، أحد مؤسسي كي بايز.

يستطيع الصحفيون إنشاء حساب كي بايز ومشاركة المفتاح العام الخاص بهم. بهذه الطريقة، يمكن للمصادر التحقق ممن يتبادلون معهم المعلومات. إنه

نموذج للثقة يسعى لتجنب انتحال شخصيات الغير. "إذا وضعت رابط على حساب كي بايز الخاص بك في نهاية مقالاتك، يستطيع أي شخص البحث عن ملفك الشخصي والتحقق منك من خلال حساباتك على وسائل التواصل الاجتماعي".

٥.سيجنال - Signal

لا تخلط بين هذه الأداة وتطبيقات سيجنال على فيس بوك أو لينكدإن. هذه الأداة، التي طورتها أوبن ويسبر سيستم، تسمح بإجراء مكالمات صوتية مشفرة، فضلاً عن إرسال رسائل نصية مشفرة. المشكلة الوحيدة في قيام المصادر بالتحدث مع الصحفيين أو النشطاء الحوقيين من خلال سيجنال، هي أنه في حالة حصول السلطات على الهاتف فستعرف أن هناك اتصالاً بينهم، إلا أنها لن تصل لمحتوى المحادثات.

• نصائح لاستخدام هواتف ذكية آمنة:

أولاً : استعمال الخدمات السحابية

بمعنى استخدام خدمات التخزين على الانترنت، بما أنها تساعد على حفظ البيانات سواء كانت صورًا أم مقاطع فيديو أو مقالات على شبكة الانترنت، بحيث تستطيع الوصول إليها في أيّ وقت تريد وفي أي مكان تشاء وحتى استرجاعها بحال ضياعها. إلاّ أنه يُنصح عند استخدام مثل هذه الخدمات باختيار خدمات مواقع تتيح إمكانية عدم تسريب البيانات أو بيعها لجهات أخرى، وغالباً ما تكون الخدمات المدفوعة هي الأكثر حماية وأفضل من نظيراتها المجانية.

ثانياً: تجنّب تنصيب التطبيقات الخارجية

كلنا نعلم أنه للبحث عن تطبيق في منصتي Android أو iOS، يتم الدخول إلى متجري التطبيقات الخاصين بهاتين الخدمتين، غير أن بعض الناس يبحثون عن مثل هذه التطبيقات في مواقع أخرى، ممّا يشكّل خطر احتواء التطبيق على فيروس أو فخ إلكتروني يتيح التجسس على الصحفي وحتى العبث بهاتفه وسرقة بياناته.

ثالثًا: تفعيل خدمة تحديد الموقع

أصبحت غالبية أنظمة الهواتف الذكية توفر هذه الخدمة وحتى بعض التطبيقات التي تمكن من تحديد هوية سارق هاتف الصحفي إن وقعت مثل هذه الحادثة، أو حتى تحديد الموقع الذي يوجد فيه الهاتف إذا تم ربطه بالانترنت، وهو ما تقدمه مثلًا خدمة icloud بالنسبة لهواتف آيفون.

رابعًا: غلق إشارة البلوتوث

في حالة عدم استعمالها وذلك لعدم إتاحة دخول أي مخترق إلى هاتفك المحمول عبر إرسال ملفات أو تطبيقات خبيثة قد تعمل كوسائل تجسس.

خامسا: برامج الحذف عن بعد

استخدام برنامج على الحاسوب يتيح للصحفي حذف كل المعلومات الموجودة في هاتفه عن بعد إذا ما سُرق أو ضاع الهاتف الذكي، بما أن أكبر تهديد أمني يمكن أن يقع لهاتف الصحفي هو سرقته أو ضياعه.

سادسا:الحذر من الشبكات المفتوحة

الحذر عن استخدام شبكات الانترنت المفتوحة للعموم (free wireless)، إذ يمكن للهاكرز دخولها بسهولة ومعرفة الأجهزة الإلكترونية التي تلج الانترنت عبر هذه الشبكات، وبالتالي إذا ما اضطريت إلى استخدام هذه الشبكات، عليك أن تحاول ما أمكن استخدام ال VPN، أي شبكة خاصة افتراضية، وهي خدمة تتيحها بعض المواقع والبرامج، كي يتم الربط بين حواسيب معيّنة عن بعد بشكل آمن، أو كي يتم تشفير بيانات الجهاز الإلكتروني عند استخدام الشبكات المفتوحة.

سابعا : صلاحيات التطبيقات المنزلة

قبل تنصيب أيّ تطبيق على الهاتف الذكي، يجب عليك أن تتأكد من من الصلاحيات التي يطلب هذا التطبيق الولوج إليها كمعرفة نوعية الكاميرا، ونوعية اتصال الانترنت، أو استخدام الإسم الموجود على الشبكات الاجتماعية. غير أن هناك بعض التطبيقات التي تطلب استخدام الكاميرا أو الولوج إلى دليل الهاتف، وهو أمر غير مقبول ويجب على الصحفي الحذر من استخدام هذا التطبيق.

ثامنا: عدم استخدام كلمة سر واحدة

عدم استخدام كلمة السر نفسها في جميع التطبيقات والمواقع التي تلجها، فاستخدام هذه الكلمة في شبكة غير محمية، قد يتيح للهاكر معرفتها وبالتالي استخدامها في بقية حسابات الصحفي على المواقع الاجتماعية مثلًا.

فضلًا عن ضرورة تعقيد هذه الكلمة، واستخدام تقنية التثبت من حقيقة المستخدم بإرسال كود في رسالة قصيرة على رقم الهاتف إن تم ولوج البريد من جهاز غير معروف، وهي التقنية التي تتيحها مثلًا خدمة البريد الإلكتروني من جوجل.

ويلاحظ أن الكثيرون يعتمدون على مكافحة الفيروسات بالكامل في حماية هواتفهم، معتقدين أن ذلك لا يمنعهم من اتباع ما سبق من نصائح، بينما توجد الكثير من الثغرات في هذه البرامج، خاصة منها النسخ المجانية، ممّا قد يجعل الهواتف عرضة للاختراق والتجسس.

• بعض الخطوات الأساسية لتشفير الأجهزة الذكية:

١. تأكد من أن بطاقة SIM الخاصة بك مقفولة بكلمة السر وتفادى أن تزيل هذه الخاصية كما يفعل العديد منا.

٢. تأكد كذلك من وضع تشفير لقفل الشاشة سواء برمز PIN أو بالوسائل المتعددة الأخرى لتفادي التطفل على جهازك، مع تحديد وقت الإقفال الذي يستحسن ضبطه كذلك.

٣. ينصح الأخصائيون في الأمان الرقمي بتشفير إعدادات الشبكة عن طريق إيقاف الإشتغال الإفتراضي "بالوايفاي" أو بالبلوثوث أو حتى بتقنية NFC.

٤. عدم استخدام إعدادات الموقع GPS إلاّ في حالة الحاجة إليها. و ألا تكون هذه الخاصية تعمل افتراضياً مما يقلص من مخاطر تعقب المستخدمين وكذلك لما توفره من استهلاك البطارية.

• خمس أدوات لحماية حساباتك على وسائل التواصل الاجتماعي

من ضمن التدابير الفعالة للحفاظ على الأمان على الإنترنت، إعدادات الخصوصية المعدّلة حسب الطلب، وتبادل البيانات الشخصية بيقظة، وسياسة "فكر قبل أن تنقر"، ولكن يمكن لهذه الأدوات البرمجية الخمسة أيضاً المساعدة على تحسين الحماية الخاصة بك على وسائل التواصل الاجتماعي:

لاست باس - LastPass

الخطأ الأكثر شيوعاً الذي يمكن أن يرتكبه الشخص هو أن يكون لديه كلمة مرور بسيطة وواضحة أو أن يستخدم كلمة مرور واحدة لجميع الحسابات – من الخدمات المصرفية عبر الإنترنت إلى البريد الإلكتروني. وتجمع القائمة السنوية لسبلاش داتا ملايين كلمات السر المسروقة وتصنفهم في قوائم حسب الشعبية. وتتضمن

الخمس الأولى "١٢٣٤٥٦"، و"كلمة المرور"، و"١٢٣٤٥"، و"١٢٣٤٥٦٧٨"، و"كويرتي" (الست حروف الأولى على لوحة المفاتيح الإنجليزية).

لاست باس هي خدمة لإدارة كلمات المرور بنظام فريميوم تخزن كلمات المرور المشفرة في السحابة. والخدمة قادرة على حفظ كلمات المرور الموجودة وكذلك توليد كلمات مرور جديدة. وتوفر مصادقة مزدوجة، وكلمة المرور الوحيدة التي يجب على المستخدم تذكرها وألا يفقدها أبداً هي كلمة مرور رئيسية للاست باس نفسه. وبشكل مثالي فكلمة المرور الخاصة بك يجب أن تكون مكونة من ١٦ حرفاً، وتحتوي على رقم واحد على الأقل، وحرف كبير واحد، وحرف صغير واحد ورمز خاص واحد. ويمكن قياس قوة كلمة المرور عن طريق باسوورد ميتر. ويوصي الخبراء بتغيير كلمة المرور الرئيسية مرة كل ١٠ أسابيع.

لوج دوج - LogDog

لوج دوج هو منتج مجاني مصمم لتعقب أي نشاط مشبوه متعلق بحسابات وسائل التواصل الاجتماعي. ويقوم النظام بمسح مستمر لمؤشرات مختلفة للوصول غير المصرح به. عندما يتم الكشف عن هجوم، يرسل لوج دوج تنبيهات بوجود تسلل ويتيح للمستخدمين استعادة السيطرة على حساباتهم. حالياً، هو متاح فقط للأجهزة التي تعمل بنظام تشغيل أندرويد. أيضاً، فبعض الشبكات الاجتماعية مثل فيس بوك تسمح لك بتلقي تنبيه عندما يسجل أي شخص دخول للحساب من جهاز أو متصفح جديد. ويجب أن يتم تشغيل هذه الخاصية.

إتش تي تي بي إس في كل مكان - HTTPS

إذا كانت الأجهزة التي يتم استخدامها للوصول إلى وسائل التواصل الاجتماعي تُشارك مع آخرين أو يتم اصطحابها في كثير من الأحيان إلى أماكن عامة، فمن الأفضل حمايتها بطبقة أمنية إضافية من خلال تشفير حركة المرور من المتصفح لشبكة إجتماعية. إتش تي تي بي إس في كل مكان هو امتداد مجاني لمتصفح يحّول المواقع من إتش تي تي بي (غير آمنة) إلى إتش تي تي بي إس (آمنة).

أيه في جي بريفيسي فيكس - AVG Privacy Fix

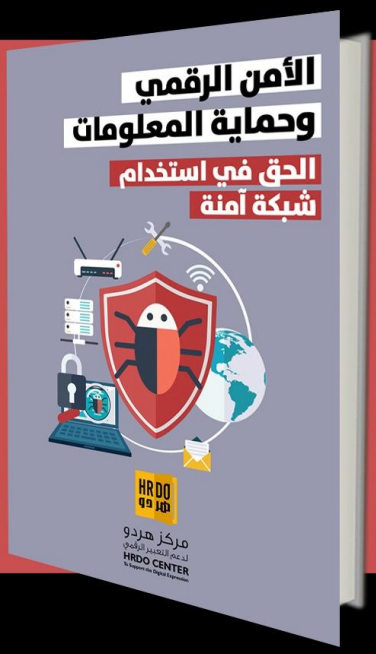
أيه في جي بريفيسي فيكس هو تطبيق مجاني يساعد المستخدمين على ضبط إعدادات الخصوصية لفيس بوك، وجوجل بلس، ولينكد إن، وتويتر، وكذلك يمنع التتبع غير المرغوب فيه. وهو متوفر حاليا للكروم، والأندرويد، والآي أو إس.

ديجي دوت مي (سويشال سيف سابقاً) - digi.me

هي أداة أخرى بنظام فريميوم، وتم تصميم ديجي دوت مي لتخزين بيانات وسائل التواصل الاجتماعي في حال فقدان جميع المعلومات نتيجة للقرصنة. وهي تسمح لك بعمل نسخة احتياطية وعرض المحتوى إلى ما يصل إلى أربعة من حسابات وسائل التواصل الاجتماعي الخاصة بك.

إشارات مرجعية:

١. القمة العالمية لمجتمع المعلومات، الوسيط، ١٦ نوفمبر ٢٠٠٥.
https://goo.gl/BCf7qb
٢. الوثائق الصادرة عن القمة العالمية لمجتمع المعلومات، ديسمبر ٢٠٠٥.
https://goo.gl/ShH4eY
٣. خمس أدوات لحماية الصحفيين وسلامتهم، شبكة الصحفيين الدوليين، ٢٦يناير ٢٠١٦.
https://goo.gl/X9f9n3
٤. الأمن الرقمي كأداة لحماية المدافعات والمدافعين عن حقوق الإنسان، سبتمبر ٢٠١٤.
https://goo.gl/fFA4mm
٥. ٨نصائح لاستخدام آمن لهواتفكم الذكية ، شبكة الصحفيين الدوليين، ٣٠ يوليو ٢٠١٧.
https://goo.gl/8vA6cI
٦. كيف تحول هاتفك الذكي لهاتف آمن، شبكة الصحفيين الدوليين، ١٦يوليو ٢٠١٥.
https://goo.gl/lffpU8
٧. خمس أدوات لحماية حسابك على مواقع التواصل الاجتماعي، شبكة الصحفيين الدوليين.
https://goo.gl/qu49IX
٨. الأمن الرقمي لصحفيي حقوق الإنسان، Speak up-speak out.
https://goo.gl/4SKRJR



الأمن الرقمي وحماية المعلومات

الحق في استخدام شبكة آمنة

برنامج الحريات الرقمية

ناضل المدافعون عن حقوق الإنسان في مصر لسنوات طوال من أجل التأكيد على حرية الرأي والتعبير كمدخل رئيسي لبناء حياة ديمقراطية ومجتمع متطور، ولا شك أن بعد ثورة يناير أصبح الاهتمام بالحريات الرقمية ضرورة ملحة لما شكلته مواقع التواصل الاجتماعي من ساحات واسعة للمشاركة والتواصل والتعبير عن لمختلف الفئات والأعمار.

وفي إطار الاهتمام بالحريات الرقمية فإننا نأخذ على عاتقنا عدة مهام، رفع الوعي بمسألة الحريات الرقمية، ومناقشة وتوثيق انتهاكات الحريات الرقمية في مصر، والضغط في اتجاه التأكيد عليها وتوفير مناخ تشريعي وتنفيذي يضمنها ويرعاها.