GANOUBIA HORA FOUNDATION
مؤسسة جنوبية حرة

السلامة الرقمية

صادر عن مؤسسة جنوبية حرة

الفهرس

مُقدمة

حاولت النساء منذ قرون الدخول للمجال العام، ونجحن في ذلك، ولكن في كل مرة، يضع المجتمع أمامهن عوائق مضاعفة، عوائق يجب عليهن خوضها بشكل يومي حتى يثبتن أنهن جديرات بالتواجد في هذه المساحات، ومنذ الثورة التكنولوجية وإتاحتها أمام الجميع، إلا أنه مع تطورها السريع فإن النساء يعانين من آثارها عليهن، حيث يتم استهدافهن وممارسة كافة أشكال العنف ضدهن، بداية من التعليقات المسيئة، الإبتزاز الإلكتروني، الإستغلال الجنسي، التهديد، مشاركة بيانات النساء دون رضائهن، المراقبة والتتبع، سرقة الهوية، التحرش الجنسي، وحتى تصل حد هذه الجرائم للقتل على أساس النوع، وهو ما يجعل تواجدهن في المجال العام العالمي الجديد «الإنترنت» أكثر صعوبة، ويحرمهن من التعبير عن أنفسهن، مشاعرهن، معرفتهن، وكذلك أيضا يحرمهن من الفرص الاقتصادية التي يمكن استغلالها لرأب الصدع في الفجوة الاقتصادية بين الجنسين.

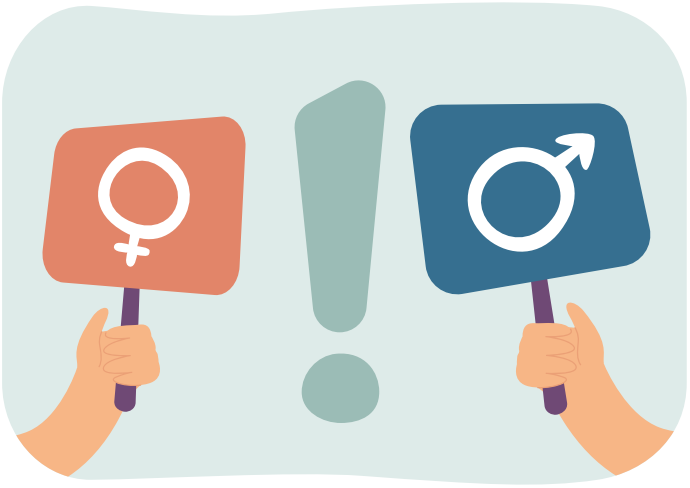
مؤسسة جنوبية حرة، هي مؤسسة نسوية شابة تدير عملها من محافظة أسوان –جنوب مصر- ، مُشهرة برقم ١٤٥٠ لسنة٢٠١٥م، تؤمن مؤسستنا بالمساواة بين الجنسين، ونظرية التقاطعية، وتسعى إلى تفكيك كافة أشكال السلطة الأبوية والقبلية التي تقف عائقا امام النساء لتحقيق أنفسهن، وتدعم المؤسسة النساء في كافة المساحات التي يحاولن التواجد فيها دون التعرض لـ تمييز أو عنف بناءا على نوعهن كأقرانهن من الرجال.

كما تؤمن مؤسسة جنوبية حرة «بالتاريخ البديل» وهو التاريخ الذى نرى أنه أكثر إنصافا واعترافا بمنجزات النساء، حيث عادة ما تكون السير والأحداث التاريخية التي نشأنا عليها تصب لمصلحة إظهار ما فعله الرجال عبر القرون الماضية دونا عن النساء، ولكن عندما نبحث في التاريخ البديل، سنعرف على سبيل المثال لا الحصر بأن «آدا لوفيلاس – Lovelace Ada» هي أول مبرمجة في التاريخ عندما كتبت خوارزميات، أو التي يعتبرها الكثيرين بأنها مجموعة التعليمات الأساسية الأولية لأول جهاز حوسبة في العام ١٨٣٣، وهي عنصر أساسي في برمجة الكمبيوتر اليوم. سنكتشف ايضا أن الممثلة «هيدي لامارر – Lamarr Hedy» هي من قدمت لنا ما يعرف بـ «القفز الترددي» وهو حجر الأساس لـ (وواي فاي – WIFI، تحديد المواقع – GPS، البلوتوث – Bluetooth).

إيماناً بمؤسسة جنوبية حرة بالقيم والمبادئ الحاكمة لها في مناهضة كافة أشكال العنف والتمييز الذي تتعرض له النساء في المجتمع المحلي –محافظة أسوان- وكافة مناطق جمهورية مصر العربية، فإن المؤسسة تقدم لكن/م هذا الكتيب كـ جزء من مسؤوليتها ودورها في تقديم كافة الوسائل، والأدوات، والمعرفة التي تُمكن النساء إليكترونيا في زيادة معارفهن وقدراتهن على مناهضة كافة أشكال العنف والتمييز التي تقع عليهن كونهن فقط نساء. ينقسم هذا الكتيب لتغطية ثلاث مناطق أساسية للمعرفة لمناهضة العنف الرقمي الذي تتعرض له النساء في فضاء الإنترنت، الجزء الأول؛ يرتبط بتعريفات ومصطلحات أساسية لماهية العنف وأشكاله حتى نستطيع تسمية ما نتعرض له كـ نساء ليكن جزء من حل المشكلة، أما الجزء الثاني؛ يرتبط بالأدوات الرقمية اللازمة التي نستطيع تعلمها لحماية أنفسنا تكنولوجياً وتخفيف حدة الآثار المرتبطة بالجرائم الإلكترونية ضد النساء، أما الجزء الثالث؛ للحديث عن الآليات القانونية اللازمة التي نستطيع اتخاذها في حالة قررنا التصدي ومواجهة مانتعرض له كـ نساء من عنف إليكتروني قانونيا.

الجـزء الأول

(مصطلحات وتعريفات)



ماهو النوع الإجتماعي؟

مفهوم النوع الاجتماعي (الجندر)

مصطلح النوع الاجتماعي (الجندر) يطلق على العلاقات والأدوار الاجتماعية والقيم التي يحددها المجتمع لكل من الجنسين (النساء والرجال)، وهذه الأدوار والعلاقات والقيم تتغير وفقا لتغير المكان والزمان، وذلك لتداخلها وتشابكها مع العلاقات الاجتماعية الأخرى، مثل الدين، الطبقة االجتماعية، العرق.

وتعرفه منظمة «الصحة العالمية» على أنه «المصطلح الذي يفيد استعماله وصف الخصائص التي يحملها كل من الرجل والمرأة كصفات مركبة اجتماعية، لا علاقة لها بالاختلافات العضوية». وأيضاً قد عرفته وثيقة صادرة عن برنامج الأمم المتحدة الإنمائي بأن «مصطلح النوع الاجتماعي (الجندر) يشير إلى الخواص الاجتماعية والمشاركة في النشاطات الاجتماعية كفرد في جماعة محددة. ولأن هذه الخواص هي سلوك وتصرفات يتم تعلمها، فهي قابلة للتغير وتتغير بالفعل عبر الزمن وتختلف باختلاف الثقافات والعلاقات المرتبطة بالنوع الاجتماعي (الجندر)، هي علاقات قائمة بين الرجال والنساء كجنسين مختلفين، تنشأ مترتبة على الأدوار والمسؤوليات المتبادلة بينهما، وتحدد القيم المتعلقة بها، وقد تكون علاقات داعمة للتعاون والتواصل والمساواة، أو قد تكون علاقات تصادم وانفصال وتنافس واختلاف وعدم مساواة. فهي دائما ما تشير إلى كيفية تعامل النساء والرجال بعضهم مع بعض في المجتمع، ودائماً ما تختلف باختلاف الزمان والمكان والعلاقات الاجتماعية الأخرى، مثل الطبقة والعرق وغيرها.

وهناك فرق بين النوع الاجتماعي (الجندر) والنوع البيولوجي.

فالنوع البيولوجي (الجنسي) يصف الاختلافات البيولوجية في جسم المرأة وجسم الرجل. أما النوع الاجتماعي (الجندر) فإنه يصف الأدوار الاجتماعية لكل نوع – أي ما هو متصور ومتوقع بخصوص طبيعة المرأة أو الرجل، أو كيف يجب أن تكون - مع ملاحظة أن الأدوار النسائية والذكورية تتغير مع مرور الوقت، كما أنها تختلف كثيراً، سواء داخل الثقافات أو فيما بينها.

الأدوار الاجتماعية

إن إعادة تشكيل العلاقة بين الجنسين بحسب المبادئ الأساسية القائمة على المساواة والديمقراطية وحقوق الإنسان والعدالة الاجتماعية هي أمر ممكن لأن أدوار الرجال والنساء هي من صنع المجتمع.

فالدور هو نموذج سلوك الفرد في المجتمع، حيث يرتبط بتوقعات المجتمع من الأفراد، وهذه التوقعات يبنيها على أساس الجنس، فهناك أدوار خاصة بالذكور وأخرى بالإناث، كما يقيم المجتمع الرجال والنساء وفقاً لنجاحهم/ن في تأدية الأدوار التي يحددها لكل منهما.

ماهو العنف المبني على النوع الإجتماعي؟

تُستخدم مصطلحات «العنف الجندريّ» أو «العنف القائم على النوع الاجتماعيّ» للإشارة إلى مجموعة من الانتهاكات التي ترتكب ضد جندر النساء، والتي تنبع من عدم المساواة بين الجنسين.

وهو: (أي عمل من أعمال العنف البدنيّ أو النفسيّ أو الاجتماعيّ بما في ذلك العنف الجنسيّ والذي يتم ممارسته أو التهديد بممارسته) مثل العنف، أو التهديد، أو القسر، أو الاستغلال، أو الخداع، أو التلاعب بالمفاهيم الثقافيّة، أو استخدام الأسلحة، أو استغلال الظروف الاقتصاديّة).

و عرفه الإعلان العالمي للقضاء على العنف ضد المرأة والذي تبنته الجمعية العامة في ديسمبر ١٩٩٣م ، ووافقت عليه جميع الدول في الأمم المتحدة فقد حددته كالأتي: «هو أي فعل عنيف قائم على أساس الجنس ينجم عنه أو يحتمل أن ينجم عنه أذى أو معاناة جسمية أو جنسية أو نفسية للمرأة، بما في ذلك التهديد باقتراف مثل هذا الفعل أو الإكراه أو الحرمان التعسفي من الحرية سواء أوقع ذلك في الحياة العامة أو الخاصة « .

لا ينحصر العنف ضد النساء في شكل واحد، بل يأخذ عدة أشكال، منها:

- العنف الجسدي: يُعدّ العنف الجسديّ من أكثر أنواع العنف انتشارًا ضد المرأة، وعادةً ما يتسبّب به

زوجها أو أحد أفراد عائلتها من الذكور، ويشمل هذا النوع من العنف أيّ أذى جسدي يَلحق بالمرأة و أي إساءة موجهة لجسدها ، سواء كان اعتداءً بالضرب او لكم و صفع وركل أو باستخدام آلة ورمي بالأجساد الصلبة واستخدام لبعض الآلات الحادة بما في ذلك التلويح بها للتهديد باستخدامها . وتترتب على العنف الجسديّ مخاطر صحيّة ونفسيّة كبيرة للمعتدى عليها، وقد يتسبّب في بعض الأحيان بوفاة المعتدى عليها.

- العنف اللفظي والنفسي: هو العنف المُمارَس ضد النساء من خلال ألفاظ مُهينة أو شتائم تنتقص من قدرِهن، بالإضافة إلى التهديد اللفظي وسوء المعاملة، ويشمل ذلك التهديد بالطلاق. للعنف النفسيّ آثار سلبية تنعكس على نفسية النساء، بالرغم من عدم وجود آثار واضحة، إلا أنه يؤدّي إلى إصابة النساء بأمراض نفسيّة حادة كالاكتئاب.
- العنف الجنسي : يأخذ هذا العنف أشكالاً عديدة منها التحرّش الجنسيّ أو أي تهديد جنسيّ، أو أي علاقة تُفرض بالإكراه، أو الاغتصاب.
- العنف الاقتصادي : هو العنف الذي يمنع النساء من الحصول على استقلاليتها الاقتصاديّة، وإبقائها كتابِع لأحد أفراد أُسرتها، ويشمل هذا النوع من العنف حرمان النساء من التعليم والعمل والتدريب مما يؤهلها لدخول سوق العمل، وحصر مجال عملها داخل المنزل فقط، بما فيه من انتهاك لحقّ النساء بالعمل والحدّ من حريتها في اختيار عمل ما تُحب.
- العنف الرقميّ : لا يوجد تعريف واحد متفق عليه. لكن يستمد العنف الجندريّ الرقميّ أصوله من الاختلال الاجتماعيّ في الأدوار بين الرجل والمرأة وتدعمه المفاهيم الاجتماعيّة الأبويّة والسلطويّة في أي مجتمع، وينعكس في العالم الرقميّ وتكون له أبعاد وعواقب في العالم غير الافتراضي.

من المؤكد أن إعطاء تعريف دقيق للعنف الرقمي، مسألة مرتبطة بمعرفة جيدة للظاهرة، وفهم عميق لآلياتها، الشيء الذي لازال قيد التبلور، نظرا للطبيعة الديناميكية لهذا الشكل من العنف والذي، كما سبقت الإشارة، لديه قدرة كبيرة على أن يتطور ويطور آلياته باستمرار

يعرف تقرير المقررة الخاصة المعنية بمسألة العنف ضد النساء وأسبابه وعواقبه ، العنف الرقمي، على أنه «أي عمل من أعمال العنف ضد النساء الذي تستخدم في ارتكابه او تساعد عليه، أو تزيد من حدته جزئيا أو كليا تكنولوجيا المعلومات والاتصالات، كالهواتف المحمولة والهواتف الذكية، أو الإنترنت، أو منصات وسائل التواصل الاجتماعي، أو البريد الإلكتروني، والذي يستهدف المرأة لأنها امرأة أو يؤثر في النساء بشكل متناسب ». و يمكن تعريفه بالعنف المتصل بالتقنية وهو جزءٌ من العنف الموجه ضدَّ النساء في الواقع.

ويعرف أيضا بـ «المضايقات الإلكترونية» ضد النساء وأنها من أشكال العنف الأخرى التي يمكن أن تكون مؤلمة بنفس قدر العنف الجسدي في بعض الأحيان أو أكثر، وهو نوع ظهر مع تطور وسائل التواصل الاجتماعي، و ينضاف إلى أساليب التعنيف على أساس النوع، ويأتي على شكل إهانة أو إساءة أو تهديد أو ابتزاز مباشر أو عبر استخدام صور أو مقاطع فيديو ضد رغبة صاحبتها.

مما تقدم فإن التطور التكنولوجي وفضاء الإنترنت ومنصات التواصل الاجتماعي أصبحت تعمل بشكل سلبي تجاه النساء، وجعل منها البعض فضاءً للتحرش والتنمر والعنف عن طريق التشهير وتشويه السمعة والابتزاز

المالي أو الجنسي .الإنترنت ومنصات التواصل جعل منها البعض فضاء للتحرش والتنمر والعنف. إن العنف الرقمي يهدد النساء بشكل مضاعف فهو عنف ممتد في الزمن وينتشر أكثر وأحيانا يمسّ دائرة الثقة والمحيط المفروض فيه الحماية وله مضاعفات نفسية خطيرة . فالخطورة تشمل الطرد والتعنيف المضاعف وفقدان الشغل في بعض الحالات، وتصل حدّ انتحار الضحية أحيانا.

أشكال العنف الرقمي ومظاهره

أما عن أشكاله تقول منظمة العفو الدولية في تقريرها عن العنف ضد النساء عبر الإنترنت، إن العنف الإلكتروني: « يتخذ أشكالا متعددة، منها التهديدات المباشرة أو غيرالمباشرة باستخدام العنف الجسدي أو الجنسي؛ والإساءة التي تستهدف جانبا أو أكثر من جوانب هوية النساء»

يأخذ العنف الموجه عن طريق الإنترنت أشكالا عديدة حصرتها حملة استعيدى التقنية Take Back The Tech:

- الوصول غير المسموح/ السيطرة غير المسموحة : هو الهجوم على الحسابات الإلكترونية أو الأجهزة الشخصية ما يعني الحصول على المعلومات والبيانات الخاصة أو حجب وصول المستخدمين إلى حساباتهم الشخصية .
- السيطرة والتلاعب بالمعلومات : فقدان السيطرة على المعلومات من قبل أصحابها و/أو إمكانية تغييرها والعبث بها.
- تقليد أو سرقة الهوية : استخدام المعلومات الشخصية في تقليد أو الانتحال او سرقة الهوية بهدف الاستغلال والابتزاز او التصيد.
- المراقبة والتتبع : الملاحقة الالكترونية بشكل مستمر، سواء بالتواصل أو بالمراقبة من بعيد، في الكثير من الأحيان تنتقل إلى أرض الواقع و قد يصاحبها تهديد أو ابتزاز.
- خلق بيئة معادية للنساء : خطابٌ يكرّس النظرة السائدة عن النساء، وحصرهن في أشكال جنسية و/ أو أدوار جندرية او إنجابية صارمة، يصاحبه هجوم و تعليقات ساخرة بهدف التقليل أو الاستهداف،

يمكن أن يحدث في المجال الالكتروني العام او في مساحات العمل أو مساحات خاصة.

- التحرش : أي صيغة من الكلمات غيرمرغوب بها و/أو الأفعال ذات الطابع الجنسي والتي تنتهك جسد أو خصوصية أو مشاعر شخص ما وتجعله يشعر بعدم الارتياح، أو التهديد، أو عدم الأمان، أو الخوف، أو عدم الاحترام، أو الترويع، أو الإهانة، أو الإساءة، أو الترهيب، أو الانتهاك أو أنه مجرد جسد.
* تعريف خريطة التحرش

- التهديد : هو الخطاب أو المحتوى العنيف سواء كان(كتابة، صورة، شفويا ، أو أي شكل آخر)، للتهديد بالعنف أو الاعتداء الجنسي بحيث يعبر عن نوايا صاحب التهديد على إيقاع الضرر بالشخص نفسه أو عائلته أو أصدقائه أو ممتلكاته.

- المشاركة غير الرضائية للمعلومات الخاصة : نشر أو مشاركة أي نوع من المعلومات أو البيانات الخاصة دون موافقة المستخدمين في تلك المعلومات أو المواد المرئية مثل مشاركة الصور الخاصة بدون موافقة. قد يصاحب اعادة مشاركة الصور التهديد أو الابتزاز من شخص او عدة اشخاص. علي سبيل المثال ما لم توافق الضحية على القيام بشيء ما في المقابل مثل المشاركة بنشاط جنسي أو إرسال صور خاصة أكثر، فإن هذا الأمر يتم تصنيفه بصفته ابتزاز جنسي.

كان يشار إلى المشاركة غير الرضائية للمعلومات الخاصة بالمصطلح «الإنتقام الإباحي» لكنه مصطلح غير دقيق.

- الابتزاز : إجبار الشخص على القيام بتصرفاتٍ ضدَّ رغبته، عن طريق التهديد والتخويف

- الذم : الاعتداء على كرامة وشرف الأشخاص و توجيه السباب أو أن يحط من قدر الأشخاص وشرفهم\ن واعتبارهم\ن الاجتماعي، وذلك بإسناد صفة او ان تنسب أمر ما لشخص سواء كان في موضع استفهام او شك كقول ان شخص مريض مرض معدي او ان هذا الشخص سرق , دون يكون هناك دليل وركن مادي للتحقق و سواء كانت تلك المادة او الامر جريمة تستلزم العقاب أم لا

- التشهير : السبّ والقذف والتشهير في مصداقيةٍ أو مهنيةٍ أو عمل أو في الصورة العامة أو الخاصة للشخص عن طريق نشر أخبارٍ كاذبة عنه او مشاركة معلومات خاصة حقيقية، أو التلاعب بالحقائق.

- الانتهاك والاستغلال الجنسي المرتبط بالتقنية : هو ممارسة القوة على الضحية بهدف الاستغلال الجنسي عن طريق التهديد بنشر المعلومات الشخصية أو المواد المرئية (صور او فيديو) على غير إرادتهم.

- الهجوم على قنوات الاتصال : الهجوم الدائم على قنوات التواصل، بحيث يبقى الشخص المستهدف خارج دائرة التواصل .

- تجاهل أو إغفال الجهات المنظمة للانتهاك : تجاهل أو عدم اهتمام أو قلة معرفة الأشخاص الفاعلين (السلطات، مقدمي الخدمة الذين لديهم لديها القدرة على التنظيم أو حل المشكلة ورفع الانتهاك، أو معاقبة المنتهك)

دراسات واحصائيات عن العنف الرقمي ضد النساء

ولفهم هذا الشكل الناشئ للعنف بشكل أفضل، بادر المكتب الإقليمي لهيئة الأمم المتحدة للمرأة للدول العربية بإجراء مشروع بحثي استكشاف مدى انتشار العنف على الإنترنت وتأثيره وعواقبه على النساء والفتيات في الدول العربية، والحواجز التي تواجه الناجيات في الحصول على الخدمات والتمكن من الإبلاغ.

وكان حجم العينة المستهدفة ١٠٠٠ مستطلعا ومستطلعة في كل بلد من فئتين تتكون من عدد ٥٠٠ رجل و٥٠٠ امرأة كحد أدنى: مع مستوى ثقة بنسبة ٩٥ في المائة وأقل من ٥ في المائة هامش خطأ. وشارك ما مجموعه ١١,٤٩٧ مستطلعا ومستطلعة في الاستقصاء، بما في ذلك ٤,١٨٧ امراة (٣٦,٤ في المائة) وتضمن الاستبيان ٢٢ سؤالا لجميع المستطلعين والمستطلعات، وتم عرضه باللغات العربية والإنجليزية والفرنسية وفقا لتفضيل المستطلعين والمستطلعات، وتم جمع البيانات في الفترة بين ٢٦ يوليو و٢ سبتمبر ٢٠٢١، وقامت شركة RIWI بتحليل البيانات.

وثبت أن في منطقة الشرق الأوسط وشمال أفريقيا، ملكية هاتف محمول واستخدام الإنترنت أقل من المتوسط العالمي بنسبة ١ في المائة و٥ في المائة على التوالي، واحتمال امتلاك النساء في المنطقة شبكة متنقلة تقل بنسبة ٨,٩ في المائة من الرجال، واستخدام شبكة الإنترنت المتنقلة أقل احتمالا بنسبة ٢٠ في المائة من الرجال.

(لا يعتبر الفضاء الرقمي آمنا بالنسبة للنساء في العالم العربي)

أبلغ ما يقرب من نصف مستخدمات الإنترنت في الدول العربية (٤٩ في المائة) عن عدم شعورهن بالآمان بسبب التحرش عبر الإنترنت، وكان هذا الشعور بعدم الأمان أكثر خطورة بين الناشطات و المدافعات عن حقوق الإنسان (٧٠ في المائة).

أبلغت نسبة ١٦ في المائة من النساء في الدول العربية عن تعرضهن للعنف على الإنترنت على الأقل مرة واحدة في حياتهن، ونسبة ٦٠ في المائة من النساء اللاتي تعرضن للعنف على الإنترنت في المطلق، تعرضن له خلال العام الماضي، وكانت هذه هي المرة الوحيدة بالنسبة لنصفهن تقريبا التي تعرضن فيها للعنف على الإنترنت.

٧٠ ٪ نسبة الناشطات والمدافعات عن حقوق الإنسان اللواتي أبلغن عن شعورهن بعدم الأمان في الحيز الالكتروني نسبة النساء اللاتي تعرضن للعنف على الإنترنت واللائي أبلغن عن ذلك في السنة الماضية.

عادة لا يقتصر التعرض للعنف على الإنترنت على حادث واحد فقط، فنسبة ٤٤ في المائة من النساء اللاتي تعرضن للعنف عبر الإنترنت، تعرضن له أكثر من مرة.

ويظهر العنف ضد النساء في الفضاء الرقمي بأشكال مختلفة، وأكثرها شيوعا هو تلقي «صور أو رموز غير مرغوب فيها ذات محتوى جنسي» (٤٣ في المائة)؛ تليها «مكالمات هاتفية_مضايقة أو اتصالات غير لائقة أو غير مرحب بها» (٣٨ في المائة) و»تلقي رسائل مهينة و/أو مفعمة بالكراهية» (٣٥ في المائة)، وتعاني نسبة ٢٢ في المائة من النساء اللاتي تعرضن للعنف عبر الإنترنت من «الابتزاز الجنسي المباشر». ولوحظت اتجاهات مماثلة بين الناشطات و المدافعات عن حقوق الإنسان، حيث أفادت نسبة ٧٠ في المائة منهن

بتلقيها رموزا غير مرغوب فيها ذات محتوى جنسي، ونسبة صور ٦٢ في المائة بتلقي رسائل مهينة و/أو مفعمة بالكراهية، بينما أفادت نسبة ٥٨ في المائة منهن بتلقي مكالمات هاتفية_مضايقة، واتصالات غير لائقة أو غير مرغوب فيها.

أبلغ النصيب الأكبر من النساء اللاتي تعرضن للعنف على الإنترنت عن تعرضهن له على موقع فيسبوك (٤٣ في المائة) يليه إنستغرام (١٦ في المائة) وواتساب (١١ في المائة).

وأقر ٢٧ في المائة من الرجال الذين أجابوا على الاستقصاء بارتكاب أعمال عنف على الإنترنت. ومن الأرجح أن يرتكب الأشخاص الأصغر سنا أعمال عنف على الإنترنت، و لا سيما الشباب. يقر أكثر من ١ من بين كل ٣ رجال في السن بين ١٨ و٢٤ سنة بارتكاب بعض من العنف على الإنترنت، حيث الطالب والعاطلون من الرجال هم أغلب من يقر بارتكاب عنف على الإنترنت (٣٠ في المائة)، والرجال الذين لم يكملوا سوى التعليم الابتدائي هم غالبا من يرتكبونه في حين أن الرجال الذين أكملوا الجامعة/الكلية هم الأقل احتمالا.

(يمثل العنف على الإنترنت تهديدا لسلامة النساء البدنية وصحتها النفسية)

يمثل العنف على الإنترنت تهديدا خطير لسلامة النساء البدنية وصحتها النفسية، وبالنسبة ١ في كل ٣ نساء، لم يمكث العنف عبر الإنترنت في الحيز الرقمي، حيث أبلغت نسبة ٣٣ في المائة من النساء اللاتي تعرضن للعنف على الإنترنت أن بعض أو كل تجاربهن في العنف على الإنترنت انتقلت خارجه، وتفيد غالبية النساء اللاتي تعرضن للعنف على الإنترنت على يد شخص يعرفونه خارج إطار الإنترنت بأن واقعة العنف انتقلت إلى خارج هذا الإطار (٥١ في المائة).

وعلاوة على ذلك، أفادت نسبة ١٢ في المائة من النساء اللاتي تعرضن للعنف على الإنترنت بتعرضهن للعنف البدني بعد إبلاغ أفراد الأسرة بالواقعة.

وكانت الصلة بين العنف على الإنترنت والعنف خارج الإنترنت ذات أهمية خاصة بالنساء اللاتي تعرضن للعنف على الإنترنت في فترة جائحة كوفيد-١٩ ،حيث أبلغت ٤٤ في المائة من النساء اللاتي تعرضن للعنف على الإنترنت في العام الماضي أن الحادث انتقل إلى خارج نطاق الإنترنت، مقارنة بنسبة ١٥ في المائة من النساء اللاتي لم تكن تجربتهن في هذا العام. وتعكس هذه الإشارة تفاقم الضرر الملموس في السنة الماضية، مما يوحي بتفاقم آثار العنف على الإنترنت في أثناء جائحة كوفيد-١٩.

نسبة النساء اللائي تعرضن للعنف على الإنترنت في العام الماضي وأبلغن أن الحادث انتقل إلى خارج نطاق الإنترنت بنسبة ٤٤ في المائة

ولوحظت اتجاهات مماثلة من خلال الدراسة الاستقصائية مع الناشطات والمدافعات عن حقوق الإنسان، حيث صرحت ٣٥ في المائة من المستطلعات بالمعاناة من تواصل العنف على الإنترنت وخارجه، بينما قالت ٦ في المائة من المستطلعات إن جميع حوادث العنف على الإنترنت ضدهن تواصلت خارجه.

وللعنف على الإنترنت أثر أيضا على صحة النساء النفسية، حيث أبلغت ٣٥ في المائة من النساء اللاتي تعرضن للعنف على الإنترنت في الدول العربية عن شعورهن «بالحزن/الاكتئاب»، وأبلغت ٣٥ في المائة منهن أنهن «فقدن الثقة في الأشخاص من حولهن»، وأبلغت

١٢ في المائة من النساء أنه قد راودتهن أفكار انتحارية نتيجة واقعة عنف على الإنترنت.
«يعرقل العنف على الإنترنت في الدول العربية المشاركة الكاملة للنساء في المجتمع ويسهم في إسكات أصواتهن»

أفادت النساء اللاتي تعرضن للعنف عبر الانترنت أنهن لم يحصلن على دعم ، وهناك أدلة على أن ذلك ساهم في فرضهن ّرقابة ذاتية أو استبعاد أنفسهن كليا من الفضاء الإلكتروني، فقد قامت أكثر من ١ من كل ٥ نساء(٢٢ في المائة) ممن تعرضن للعنف على الإنترنت بحذف أو وقف حسابها، وأفادت أكثر من ١ من كل ٤ نساء (٢٦ في المائة) ممن تعرضن للعنف على الإنترنت بأنهن كن حذرات بشأن ما ينشرونه على الإنترنت.

وكان ذلك الأمر ذا أهمية خاصة فيما يتعلق بالعنف على الإنترنت الذي شوهد خلال العام الماضي، حيث كانت النساء اللاتي تعرضن للعنف على الإنترنت هذا العام أكثر ميّلا (٢٧ في المائة) للابلاغ عن وقف أو حذف حساباتهن أو التغيب عن الدراسة أو العمل نتيجة واقعة العنف، مقارنة بالنساء اللاتي لم تقع حادثة العنف على الإنترنت لهن هذا العام.

تتعرض النساء للاعتداء بسبب تزايد وجودهن في الفضاء الإلكتروني, وقد يثير تواجد النساء على الإنترنت، ولا سيما النساء التي يعتقد أنها تتطاول على العادات المجتمعية شعوراً بالغضب والأحقية في إسكات النساء والفتيات أو حتى استبعادهن من الفضاء الإلكتروني. وصرحت منظمات المجتمع المدني بارتباط ذلك بالأفكار الثقافية المتعلقة بالذكورة والسلوك التحكمي. إذن، يسعى مرتكبو الجرائم إلى السيطرة على تلك النساء والتحكم فيهن، ويشمل ذلك الجناة الذين لديهم آراء دينية مختلفة، وغير قادرين على مواجهة ّالناجيات شخصيا والذين يفضلون الاختباء وعدم الكشف عن هويتهم، وإحساس الجناة بالأحقية، أي الجناة الذين يعتقدون أن هذا من حقهم، والنظرة إلى أن النساء على أنها «تستحق ذلك».

وقد تستجيب الأسر أيضا عن طريق تقييد أو منع حصول النساء والفتيات على الأجهزة الرقمية، مما يؤدي إلى زيادة عزل النساء والفتيات وحرمانهن من حقهن في الحصول على المعلومات والتقدم التكنولوجي فضّل عن حرية التعبير.

وعلاوة على ذلك،ونظراً لأن القوانين المتعلقة بجرائم الإنترنت لا تولي في الغالب اهتماما كافيا للعنف ضد النساء والفتيات ُعلى الإنترنت، فإنها تستخدم أحيانا لمقاضاة الناجيات أو لقمع آرائهن السياسية، و بدل من التركيز على معاقبة أفعال مثل نشر الصور الحميمة دون موافقة، قد يتم مقاضاة الناجيات بتهمة الفجور أو ارتكاب جرائم ضد الأخلاق أو المشاعر العامة.

تشكل معايير اجتماعية مختلفة العنف على الإنترنت ولكنه يعتبر في معظمه «قضية نسائية» لا ينبغي أخذها على محمل الجد، يتم بسببه إلقاء اللوم على النساء. يعتقد معظم ّالمستطلعين والمستطلعات أن «النساء يتعرضن للعنف على الإنترنت أكثر من الرجال» (٦٦ في المائة من النساء مقارنة بنسبة ٦٠ في المائة من الرجال). وعلى غرار أشكال العنف ُالأخرى ضد النساء ، تأمل المرأة عليه ويُتوقع منها أن تقبله، حيث ُطلب من ٣٦ في المائة من النساء اللاتي تعرضن للعنف على الإنترنت تجاهل الأمر، وألقي اللوم على ٢٣ في المائة منهن، وطلب من ٢١ في المائة منهن حذف حساباتهن على مواقع التواصل الاجتماعي، وتفيد نسبة ٢٠ في المائة فقط بأن أسرتها كانت تدعمها، وتفيد نسبة ٣٢ في المائة من الضحايا الإناث بأن أصدقائهن كانوا داعمين لهن.

العوامل المؤدية إلى تزايد العنف الرقمي

- الامتيازات المادية (تكلفة عالية + سوء الخدمات) وأثرها على عدم مقدرة الكثير من النساء خارج القاهرة من الوصول للإنترنت. - مجال التقنية والبرمجة مهيمن عليه من قِبلَ الرجال، ويتم إعطاء النساء المشتغلات بالتقنية أدوار محددة لا تشمل كتابة الأكواد.
- الرقابة الأسرية/ العائلية على وجود النساء على الإنترنت وما يمُكن أن يترتب عليه من تضييق أو عنف مبني على أساس الجندر. - حظر استخدام أجهزة الكمبيوتر (الحاسوب) أو الولوج للإنترنت على النساء، واتاحته للذكور في بعض السياقات الاجتماعية.
- الإرهاق النفسي وأثره على قدرتنا على التواجد أونلاين. - مطالبتنا بتلبية توقعات اجتماعية معينة مبنية على نوعنا الاجتماعي وما يترتب عليه من ضغط نفسي.
- طريقة وحجم تواجدنا على الإنترنت يعكس اختلاف هوياتنا وتقاطعها وأوجه الامتيازات والقهر التي نختبرها (أصحاب الهويات المهمشة أكثر عرضة للعنف الإلكتروني).
- عدم وجود وعي كافي بسياسات الخصوصية والأمان الرقمي وأهميته وكيفية تطبيقه.
- قدرة الدولة على منع الإنترنت (قطع الإنترنت في الثورة السودانية، حجب المواقع في مصر.. إلخ) يعكس الإنترنت أيضًا فجوة جندرية كبيرة فيما يتعلق بمسألة الوصول للتقنية من الأساس، أو فيما يتعلق بحجم الوقت الذي تقضيه نساء مستخدمة أجهزة تقنية، ففي الكثير من الأسر يُحظر الولوج على أجهزة الحاسوب أو الهواتف الذكية على النساء بينما تكون متاحة للاستخدام من قبل الذكور فقط، أو تُخصص أوقات معينة في اليوم تستطيع فيها النساء استخدام أجهزة الحاسوب والولوج على الإنترنت، في حين يستطيع الذكور استخدامها وقتما شاءوا.

ويرتبط هذا بالرقابة الأسرية المفروضة على النساء في الواقع الافتراضي، بداية من تحديد مواعيد لتواجد النساء أونلاين أو منعهن من التواجد الإلكتروني من الأساس وصولًا لمراقبة ما تنشره النساء على حساباتهن على منصات التواصل الاجتماعي، فلا تشعر كل النساء بالراحة والأمان الكافيين لنشر صور شخصية لهن أو مشاركة منشورات (بوستات) مرتبطة بموضوعات محظور الكلام عنها اجتماعياً، خاصة الموضوعات المرتبطة بالجسد والجنسانية والحريات الفردية والسياسة، تمتد الرقابة الأسرية حتى عدم السماح للنساء بوضع صورهن الشخصية و/أو أسمائهن الحقيقية على حساباتهن على منصات التواصل الاجتماعي، وتدخل الأسرة في بعض الأحيان في قرارات النساء المرتبطة بالإضافات على قائمة الأصدقاء و/أو السؤال حول الأصدقاء الذين يقومون بكتابة تعليقات أو إعجاب بالمنشورات التي تقوم المستخدمات بنشرها، وكثيراً ما يترتب ممارسة عنف أسري سواء بالتهديد أو بمنع استخدام الأجهزة وقد يصل لممارسة العنف الجسدي (الضرب أو الحبس) في المنزل إذا ما اكتشف أحد أفراد الأسرة أو العائلة أن إحداهن قامت بمخالفة القواعد الأخلاقية التي على النساء الالتزام بها.

لا تتوقف الرقابة الإلكترونية على الأسرة أو العائلة فقط، ولكنها تمتد لتكون رقابة اجتماعية تتضمن المحيطين من الأصدقاء والجيران وزملاء العمل، فيتحول الإنترنت لمساحة مراقبة مدى التزام النساء

بالقواعد الأخلاقية المرتبطة بطريقة اللبس والاحتكاك الجسدي بالرجال واللغة المسُتخَدَمَة في الكتابة أو التعليق والسلوك العام وموضوعات اهتمام المسُتخَدِمَة، وإذا خالفت الكود الأخلاقي يشعر المحيطين بالأحقية و يتهمن في إعطائها نصائح حول ما تقوم بنشره، وفي بعض الأحيان يلجأ البعض لتبليغ الأسرة حول السلوك المرصود، في مطالبة مبطنة أحياناً وصريحة أحياناً أخرى لقيام الأسرة بدورها في تقويم سلوك نسائها، وهو امتداد لمركزية دور الأسرة كمؤسسة تنشئة اجتماعية للأفراد في إطار الثنائية الجندرية وما تمثله من محددات لصفات الأفراد و اختياراتهن وسلوكياتهن، حيث تمتلك الأسرة كامل الحق اجتماعياً في تقويمهن إذا ما حادوا عن المحددات الاجتماعية المرتبطة بجندرهن، وفي أغلب الحالات يقوم أفراد الأسرة بفرض إجراءات عقابية لتقويم السلوك الإلكتروني للمستخدمة. فلا يشعرن بأريحية كاملة في تواجدهن الإلكتروني.

الآثار والانعكاسات على النساء من العنف الرقمي

في دراسة نشرتها شبكة «Learning VAW» حول العنف الالكتروني ضد المرأة قالت الشبكة إن العنف ضد المرأة يمكن أيضًا أن يكون امتدادًا لتجربة العنف التي تعيشها النساء في علاقتها العاطفية، حيث يمكن استخدامه من قبل شريك المرأة كوسيلة للحفاظ على سيطرته وسلطته عليها.

- آثار النفسية : وأشارت الدراسة إلى أن العنف الإلكتروني ضد المرأة له آثار نفسية واجتماعية ومادية واقتصادية، ولكن الآثار الأكثر انتشارًا هي النفسية التي تشعر بها معظم لنساء اللاتي يتعرضن للعنف الإلكتروني، ومن أكثر هذه الآثار النفسية شيوعًا القلق وتشوه الصورة الذاتية، وأحيانا تصل ثار النفسية إلى حد أكثر تطرفاً كالأفكار الانتحارية، أو الانخراط في سلوك إيذاء النفس. ومن آثار العنف الإلكترونى على النساء أيضًا الأرق ونوبات الهلع والخوف الشديد من مغادرة المنزل بالإضافة إلى الشعور بالإذلال.
- أما الآثار الاقتصادية للعنف الإلكتروني ضد المرأة فهي الأخرى خطيرة، فأحيانا تكون نتيجته فقدان وظائفهن بسبب التشهير أو نشر صور إباحية انتقامية، أو فقدانهن لصفحاتهن على مواقع التواصل الإجتماعي إذا ما كن يعملن اونلاين «عن بعد». وهي كلها آثار تزيد من نسبة الفجوة ما بين الجنسين.

الجـزء الثاني

(السلامة الرقمية)

السلامة الرقمية

يشير مصطلح «الأمان الرقمي » إلى كل الوسائل التي تضمن استخدام شبكة الإنترنت استخدام فعال بدون التعرض لأي تهديدات أو مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات. وإن تواجد الفتيات والنساء على الإنترنت ومواقع التواصل الاجتماعي واستخدامهن لتطبيقات الهاتف التي تسهل أمور حياتهن اليومية، أصبح يفرض عليهن أن يكُن أكثر معرفة بحقوقهن الرقمية خاصة في ظل انتشار حالات كثير من الجرائم المتعلقة في انتهاك خصوصيتهن. ويتضمن الأمان الرقمي كذلك كيفية استخدام شبكة الإنترنت استخدام فعال بدون التعرض لأي تهديدات أو مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات.

يؤكد مجلس حقوق الإنسان التابع للأمم المتّحدة، وهو الهيئة الرائدة عالميا المنوطة بتعزيز حقوق الإنسان وحمايتها، على أنّ «الحقوق الّتي يتمتّع بها الناس خارج نطاق الإنترنت هي ذات الحقوق التي يجب حمايتها داخل نطاق الإنترنت»

والحقوق الرقميّة هي من ضمن حقوق الإنسان التي نتمتّع بها في عالم الإنترنت، ولا بد أن تعترف الدّول بهذه، الحقوق، وأن تحترمها، وتحميها، وتعزّزها بما يتسق مع التزاماتها بموجب القانون الدوليّ لحقوق الإنسان.

- الحق في الوصول للإنترنت : يحظى الحقّ في الوصول للإنترنت، باعتراف واسع النّطاق بكونه حقّ من حقوق الإنسان وأحد الوسائل الأساسيّة للتمتّع بحقوق الإنسان خارج نطاق الإنترنت كما داخله. إذ أصبح الإنترنت ركنا يمكّننا من تشارك المعرفة واكتسابها عبر منصاته المختلفة، والتّشبيك الاجتماعيّ، والتّنظيم السياسيّ، والمشاركة في الاقتصاد والتنمية.
- الحقّ في حريّة التّعبير والرأي والمعلومات : يشمل هذا الحق، حقّ التماس المعلومات وجميع أنواع الأفكار، وتلقيها وتناقلها دون تدخل أو اعتبار للحدود، وضمان التّنوع الواسع للمصادر، وتمكين الجميع من الوصول لمجتمع المعلومات.
- الحق في التّجمّع السّلميّ وتكوين الجمعيات والمشاركة: يشمل ذلك الحقّ في ممارسة حريّة التّجمّع وتكوين الجمعيات مع آخرين في العصر الرقمي المبني على نهج تشاركيّ في مشاركة المعلومات، إذ لا يقتصر دورنا على تلقّي المعلومات فقط، بل بمقدورنا أن نساهم بفاعليّة في عمليّة إنشاء المحتوى.
- الحقّ في الخصوصيّة وحماية البيانات : يعد الحقّ في الخصوصية حقّا إنسانيّا راسخًا ومحميًا بموجب القانون الدوليّ لحقوق الإنسان. وتتزايد أهميّة الحقّ في الخصوصيّة، والّذي يشمل حماية البيانات، كقاعدة أساسيّة لممارسة حقوق الإنسان ذات الصّلة عبر الإنترنت.

مفهوم الخصوصية

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.

وعلى هذا النحو فالخصوصية في مواقع التواصل الاجتماعي وفي أبسط معانيها ترتبط بسرية الحياة الخاصة لمستخدمي تلك المواقع والحديث هنا عن الحياة الخاصة للنساء، سواء كانت وقائع أو معلومات في الحاسب الآلي الشخصي أو الهاتف الذكي، أو تم تخزينها في إحدى مواقع التواصل الاجتماعي التي يشترك فيها المستخدم والتي قد يتم اختراقها حيث أن سرقتها أو الاعتداء عليها يعد إنتهاكاً للخصوصية، كذلك التجسس الإلكتروني، أو اعتراض الرسائل البريدية المرسلة بغرض الإطلاع عليها أو معرفة محتوياتها، ومن ثم إفشاء الأسرار التي قد تحتويها تلك الرسائل ومن قبيل ذلك الأسرار الاقتصادية والسياسية والاجتماعية والصحية والعلمية وغيرها من الانتهاكات والاختراقات.

معايير ضمان المعلومات

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

الأمان الرقمي في الدستور المصري

مادة (٥٧): «للحياة الخاصة حرمة، وهى مصونة لا تمس، و للمراسلات 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، و في 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 تعسفى، 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

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

- **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.

- **قرار الجمعية العمومية للأمم المتحدة بشأن حماية الحق في الخصوصية الرقمية**
القرار ٢٦ 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.
والإقرار بالوارد في المادة ١٢ من الإعلان العالمي لحقوق الإنسان والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية؛ ومنها، التأكيد على أن الحقوق نفسها التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحظى بالحماية أيضا على الإنترنت، بما في ذلك الحق في الخصوصية.

مصطلحات متعلقة بالإنترنت

الهجمات الإلكترونية: وهو الاستغلال المتعمد لأنظمة الحاسوب، والشركات والشبكات المعتمدة على التكنولوجيا. تستخدم الهجمات الإلكترونيّة الشيفرات الخبيثة لتغيير شيفرة الكمبيوتر أو المنطق أو البيانات، مما يؤدي إلى عواقب مخلة يمكن أن تضر بالبيانات

برامج التجسس: وهي البرامج التي تسجّل سرًا أنشطتك على جهاز الكمبيوتر الخاص بك هي برامج التجسس. ويمكن استخدامها لبعض الأغراض المشروعة تماما، ولكن غالبية برامج التجسس الخبيثة. هدفها هو عادة التقاط كلمات السر، وبيانات الاعتماد المصرفيّة وإرسالها عبر الإنترنت إلى مبتكريها. تُنكَّر أحصنة طروادة في شكل دعابات برمجيّة، أو موسيقى أو مقاطع فيديو أو عروضا ذات مشغلات مرفقة بها، كما تشيع في مولدات الأرقام التسلسليّة للبرمجيات التجارية المقرصنة.

مدير كلمة السر: يساعد في توليد واسترجاع كلمات السرّ المعقدة، يحتمل تخزين كلمات السرّ في قاعدة بيانات مشفرّة أو استخراجها على الطلب. هناك أنواع مختلفة من مديري كلمة السر المتاحة ولكن الذي نوصي به يسمى كيباسكس. هو مصدر مفتوح، مما يعني أنه مجاني للاستخدام ويمكن التحقق من التعليمات البرمجيّة للحصول على الثغرات الأمنيّة

برمجيات الفدية: هو نوع من البرمجيات الخبيثة التي تمنع أو تحدّ المستخدمين من الوصول إلى معلوماتهم الشخصية او محتوى أجهزتهم عن طريق التشفير أو العزل، إما عن طريق قفل شاشة النظام أو عن طريق قفل ملفات المستخدمين ما لم يتم دفع فدية.

الحسابات المخترقة والمسروقة: مخترقو الحسابات على الانترنت Hackers -والذين يمكنهم الحصول على دخول غير مفوض إلى حساب المستخدم، وغالبا ما يتم ذلك عن طريق معرفة أو تخمين كلمة السر الخاصة بالمستخدم. لذا تقوم شركة فيسبوك بمحاولة إقصاء القراصنة، وكذلك على المستخدمين أيضا اتخاذ الاحتياطات الضرورية لحماية كلمات السر الخاصة بهم وحساباتهم.

الهندسة الاجتماعية: هي عملية تلاعب بشخص ما للقيام بعمل معين، أو الكشف عن معلومات شخصية غالبًا ما تكون حساسة. يقوم القراصنة في الغالب بإنشاء صداقات أو استخدام حيل نفسية لإقناع شخص ما لمشاركتهم بالصور، مشاركة كلمات السر... الخ. بدلا من العثور على ثغرة أمنية في البرنامج، يمكن للمهاجم أن يتظاهر زُورًا أنه شخص يقدّم الدعم الفني وأن لديه هدفا نبيلا لمساعدة المستخدمين ودعمهم عن طريق حماية حساباتهم، ويطلب منهم معرفة كلمات السر الخاصة بهم للسير لتحقيق هذا الهدف.

هجمات التصيد: التصيد يتمثل عندما تتنكر جهة وتظهر بأنها جهة موثوق بها ويحاول الحصول على معلومات حساسة من مستخدم آخر ككلمات السر الخاصة به أو معلومات عن بطاقة الائتمان. على سبيل المثال، يتظاهر شخص ما بكونه يعمل في محل تجاري، يرسل لك رسالة تعلمك بأن لديهم خصم على البضاعة في ذلك المحل. يطلب منك بعدها بالقيام بعملية الشراء عبر واتساب، و ارسال رقم بطاقة الائتمان الخاصة بك، تاريخ الانتهاء، والرمز الأمني من أجل تكملة عملية البيع لك. مثال آخر، أن تستلم رسالة الكترونية تظهر انها من موقع فيسبوك. تنص الرسالة على تعرُّض الحساب الخاص بك للتهديد وأن عليك الدخول فورا على حسابك لحل المشكلة. تقوم بالضغط على إشارة تسجيل الدخول من الرسالة وإضافة كلمة السر الخاصة بك. في هذه الحالة فإنك تزوّد بيانات الدخول هذه إلى القراصنة.

روابط خبيثة: يمكن للمستخدم أن يستلم روابط بواسطة رسائل أو تعليقات تبدو وكأنها تروج لشيء حقيقي ولكن في الحقيقة تكون روابط خبيثة و تهدف إلى التصيد والاحتيال. في حال الضغط على الرابط، يتم تنزيل فيروس أو برنامج خبيث على جهاز المستخدم. الفيروس المستخدم في الغالب يعمل على سرقة البيانات الشخصية. للكشف فيما إذا كان الرابط خبيثًا، انسخ الرابط وألصقه في COM.VIRUSTOTAL الضغط عليه ، انتقل إلى موقع صندوق البحث. يقوم الموقع بالتأكد من الرابط ويطلعك فيما إذا كان الرابط غير صحيح، أو ليس جديرا بالثقة.

انتحال الشخصية والحسابات المزورة: غالبًا ما يكتشف المستخدمون حسابات تبدو بأنها تخص شخصًا يعرفونه، أو تظهر بمعلومات، أو تبدو ببساطة بأنها مزورة. هذه الحسابات المزورة قد تكون تهديدا حيث أنها غالبا ما تكون مستخدمة لاكتساب ثقة مستخدمين آخرين وإضافة تابعين وأصدقاء، وقد تستخدم هذه الحسابات المزورة بعدها لتهديد المستخدم الذي ينتحلون شخصيته أو ابتزازه.

كيف تحظى بالخصوصية والسلامة الرقمية

كلمات السر القوية واستخدام التحقق بخطوتين تعد خطوات أساسية لا غنى عنها لتأمين اي حساب اونلاين.

تأمين الفيسبوك:

حماية كلمة السر

يجب أن تكون كلمة السر الخاصة بحسابك على فيسبوك فريدة وآمنة ولم تتم مشاركتها مع أي شخص أو في أي مكان. تشتمل المعلومات الرئيسية التي يجب تجنّب تضمينها في كلمة السر أي معلومات تحدد الشخصية مثل اسمك ورقم هاتفك وتاريخ ميلادك وعنوان المراسلة. يمكنك الاستعانة بنصيحة واحدة ألا وهي استخدام برنامج مدير كلمات السر، الذي يحفظ كلمات السر بأمان، وكذلك يساعدك على إنشاء كلمات سر قوية لكل حساباتكم.

نصائح انشاء كلمات سر قوية

الكثير من القراصنة يتحسسون كلمات المرور بواسطة برامج حاسوبية تقوم بشكل آلي كامل بتجريب عدد غير محدود من توليفات الحروف والأرقام والرموز، كما تجرب كلمات قواميس ومعاجم بأكملها بشكل آلي تام، بهدف التمكن من سرقة كلمات المرور للمستخدمين وحساباتهم الإلكترونية.

أولا : استخدام كلمة مرور مختلفة عن غيرها

استخدام كلمة مرور مختلفة لكل حساب من حساباتك المهمة، مثل بريدك الإلكتروني والخدمات المصرفية على الإنترنت. إعادة استخدام كلمات المرور في حساباتك المهمة أمر خطير. فإذا حصل أحدهم على كلمة مرور أحد حساباتك، قد يتمكن من الوصول إلى بريدك الإلكتروني وحتى حسابك المصرفي.

- **كلمة السر القوية**

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) ABC أو ١٢٣
٦. لا تحتوي على أجزاء كبيرة كتلك الموجودة بالقاموس.
٧. إحدى الطرق لجعل كلمة المرور الحالية أقوى
   وخاصة لمقاومة برامج التخمين الآلي - هو جعلها أطول.

ثانيا : الحفاظ على أمان كلمات المرور بعد إنشاء كلمة مرور قوية، ننصحكِ بالخطوات التالية للحفاظ على أمانها.

- إخفاء كلمات المرور المكتوبة إذا أردت\ي تدوين كلمة مرورك، فلا تضع على جهاز الكمبيوتر أو مكتبك. تأكّدي من حفظ أي كلمات مرور مكتوبة في مكان سرّي أو مؤمّن.
- إدارة كلمات مرورك باستخدام أداة رقمية إذا واجهت/ي صعوبة في تذكّر كلمات مرور متعددة، ننصحكِ باستخدام أداة موثوق بها لإدارة كلمات المرور نرشح تطبيق. Bitwarden

خصّص/ي بعض الوقت للاطّلاع على آراء المستخدمين بهذه الخدمات ومدى ثقتهم بها.

- تفعيل المصادقة الثنائية

المصادقة الثنائية يمكن تفعيلها من خلال تطبيقات المصادقة او ارقام الهاتف، لكن الآمن أكثر هو استخدام تطبيقات المصادقة. هي خطوة اساسية لضمان أمان حسابك. يمكن العثور على ذلك في قسم الأمان وتسجيل الدخول تحت «الإعدادات».عند تفعّيل ميزة المصادقة الثنائية، سيُطلب إدخال رمز أمان خاص في كل مرة تتم محاولة الدخول إلى حسابك على الفيسبوك من كمبيوتر أو هاتف أو متصفّح جديد.

أمثلة لتطبيقات المصادقة: Authenticator Microsoft أو Authenticator Google أو Mobile Duo او Authy

- تلقّي تنبيهات بشأن الأجهزة غير المعروفة

• يمكنك استخدام تنبيهات تسجيل الدخول لتلقي إشعارات عندما يحاول أي شخص الوصول إلى حسابك من جهاز جديد أو جهاز غير معروف.

• يمكنك تشغيل التنبيهات الخاصة بعمليات تسجيل الدخول غير المعروفة بزيارة قسم الأمان وتسجيل الدخول تحت «الإعدادات». عند تشغيل التنبيهات، ستصل رسالة بريد إلكتروني أو إشعارًا في أي وقت يحاول فيه شخص ما تسجيل الدخول إلى حسابك من جهاز أو متصفح غير معروف.

- استخدام أدوات التحقق في فيسبوك

يمكنك استخدام فحص الأمان الخاص بفيسبوك من خلال الحصول على تنبيهات عندما يحاول أحد الأشخاص تسجيل الدخول إلى حسابك من كمبيوتر أو هاتف محمول غير معروف.

• التعرف على كيفية حماية كلمة السر الخاصة بك.

• فعّل/ي ميزة المصادقة الثنائية، وهي ميزة اختيارية تضيف المزيد من الأمان إلى حساب فيسبوك الخاص بكم.

• استخدم/ي فحص الخصوصية للتأكد من أن الأشخاص الذين تثقون فيهم فقط يستطيع مشاهدة معلوماتك ومنشوراتك، لأنك في بعض الأحيان قد تود/ي أن تكون المشاركة بشكل عام وفي أحيان أخرى تريد/ي المشاركة مع الأصدقاء فقط.

يمكنك مراجعة من يمكنه مشاهدة منشوراتك ومعلوماتك من ملفك الشخصي، كرقم هاتفك وعنوان بريدك الإلكتروني. كما تُظهر أيضًا إعداداتك للتطبيقات التي سجلتم الدخول إليها باستخدام فيسبوك. يمكنك استخدام ميزة التحقق من الخصوصية لمراجعة وضبط إعدادات

الخصوصية المتعلقة بك للتأكد من مشاركتك القصص مع الأشخاص الذين تود/ي منهم/ن رؤيتها.

- إدارة تواجدك على الملفات الشخصية والصفحات
يمكنك التعامل بشكلٍ عام أو خاص بالقدر الذي ترغب/ي فيه مع جمهورك على فيسبوك. إليك نصيحة حول كيفية إدارة ما تقوم\ي بإرساله.

الملف الشخصي:

ا. استخدم/ي أداة تحديد الجمهور للتحكّم بمن يمكنه رؤية منشوراتك. يمكنك اختيار المشاركة مع الجميع، أو مع الأصدقاء فقط، أو حتى مع جمهور مُخصص حسب الرغبة. عندما تقوم/ي بإنشاء جمهور مُخصص حسب الرغبة، يمكنك المشاركة انتقائيًا مع أشخاص مُحددين.

ب. تحكّم/ي في من يشاهد ما ترسلونه عبر تحديث «الإعدادات» في شاشة «اليوميات» و»الإشارات». يمكنكم الموافقة على الإشارات التي يضيفها الأصدقاء لمنشوراتكم أو رفضها. بمجرد موافقتك على وسمٍ ما، يمكن للشخص الموسوم وأصدقائه رؤية منشورك. يمكن العثور على مُراجعة الإشارات في «الإعدادات» تحت «اليوميات والإشارات».

ت. استخدم/ي مراجعة «اليوميات» لتقرير ما إذا كانت المنشورات التي تمت الإشارة إليك/ي

فيها تظهر على يومياتك. عندما يقوم أشخاص ليسوا أصدقاءك بالإشارة إليك/ي في منشور، فإنه يذهب تلقائيًا إلى مراجعة يومياتك. إذا كنتم تودّ/ي أيضًا مراجعة الإشارات من قِبل الأصدقاء، يمكنك تشغيل مُراجعة «اليوميات» للإشارات من أي شخص. يمكن العثور على مُراجعة اليوميات في «الإعدادات» تحت «اليوميات والإشارات».

ث. للتحكم في كيفية ظهور ملفك الشخصي للآخرين باستخدام أداة «عرض كما يظهر للآخرين». ببساطة، انتقل/ي إلى ملفك الشخصي، انقر/ي على «عرض كما يظهر للآخرين» وشاهد/ي كيف يظهر ملفك الشخصي للعامة أو لشخصٍ مُحدد.

- الصفحة:

ا. سواءً كنت/ي مُحرري وسائط تواصل اجتماعي، أو تستخدم/ي صفحة للوصول إلى قرائكم أو مشاهديكم، أو مُدراء صفحة، هناك خيارات متعددة للحفاظ على أمان صفحتك. إن اختيار وتعيين الأدوار الصحيحة للمدير سيساعد في إدارة صفحتك دون أن تُعرّض/ي كلمات السر للخطر. سيدخل كل شخص إلى حسابه الشخصي ويعمل على الصفحة من هناك. من المهم تعيين وظائف الصفحة وفقًا لذلك لأن التحكم الإداري الكامل في صفحةٍ ما ليس مسألة يحتاجها الجميع؛ فبعض الأشخاص يحتاجون فقط مسؤوليات تحريرية أو إعلانية.

ب. تأكد/ي من أن المسؤولين عن الصفحة يستخدمون حسابات حقيقية ومن تفعيلهم/ن المصادقة الثنائية حتى لا يخسروا الدخول إلى حساباتهم/ن. يحذف فيسبوك الحسابات المزيفة والانتحارية عندما

نُصبح على علمٍ بها.

ت. استخدم/ي أدوات الفلتر والإشراف، والموجودة تحت إعدادات «الصفحة» من أجل الإشراف على التعليقات والمنشورات من قِبل الزوار. ستقوم هذه الأدوات أيضًا بحجب الكلمات وتفعيل فلتر «الكلمات البذيئة» لصفحتك. لا تَنس/ي فلترة النسخ المُختلفة من الكلمات المحظورة. يمكنك إضافة نقاط وقف أو مسافات بينية ووسومات هاشتاغ. على سبيل المثال، لفلترة الكلمة «مسدس»، قوم/ي أيضًا بفلترة «م.س.د.س»، و «#مسدس»، و «م س د س». في حين أنه لا يمكنك تعطيل التعليقات على منشورات صفحتك، يمكنك إخفاء أو حذف التعليقات الفردية. عندما تقوم/ي بإخفاء تعليق، لن يعرف الشخص الذي أرسله أنه كان مخفيًا.

ث. يمكنك اختيار حظر الأشخاص الذين ينشرون محتوى احتياليًا على صفحتك باستمرار. يمكنك ازالة الحظر في أي وقت. عندما تحظر/ي شخصًا ما من صفحتك، سيتمكّن من مشاركة المُحتوى من صفحتك إلى أماكن أخرى على فيسبوك، ولكنه لن يستطيع النشر على صفحتك، أو وضع إعجاب أو التعليق على منشورات صفحتك أو إرسال رسائل إلى صفحتك أو الإعجاب بصفحتك.

ج. إذا كنتم تودّ/ي أن يقوم شخصٌ ما في موقع مُختلف ببث مباشر من صفحة فيسبوك الخاصة بك، ضع/ي في اعتبارك منحه دور «المساهم المباشر». سيعطيه ذلك القدرة على بدء بث مباشر، ولكن سيحد وصوله إلى مزايا أخرى على صفحتك.

ح. يسمح لك فيسبوك أيضًا بحذف أي تعليقات ترغب/ي في حذفها من ملفك الشخصي أو صفحتك، سواء كانت ضد معايير المجتمع الخاصة بنا أم لا.

- التحكّم في موقعكم بالمنشورات

يقدّم لكم فيسبوك خيار تضمين موقعك في منشوراتك. لا يُشارك فيسبوك الموقع بشكلٍ افتراضي، ولكن من الجيد دومًا تحديث أو إيقاف تشغيل خدمات الموقع الخاص بهاتفك قبل الإرسال من مناطق حساسة. يمكنك تحديث إعدادات الموقع الخاصة بكم على جهاز iOS أو Android الخاص بك.

يمكن أيضًا استخدام فيسبوك بمتصفح Tor كي يساعد على إخفاء عنوان بروتوكول الإنترنت الخاص بك بحيث لن يتمكن فيسبوك والمُعلنين وشبكات الهاتف المحلية ومزودي خدمات الإنترنت من مشاهدة المكان الذي تسجل/ي دخولك منه. و بذلك يحمي بشكلٍ أكبر أمن موقعكم واتصالك بفيسبوك

خطوات لحماية الحساب على الانستغرام والواتساب من الهجوم

على انستجرام، ادخل/ي على «الإعدادات» ثم "الأمان" ثم اضغط على "المصادقة الثنائية" و من هنا يمكن ربط الحساب بأحد تطبيقات المصادقة التي تم تثبيتها على الهاتف او استخدام رقم الهاتف.

على واتساب، ادخل/ي على "الإعدادات» ثم "الحساب" ثم "المصادقة الثنائية" ثم "تمكين"

فعّل/ي تنبيهات تسجيل الدخول حتى يتم إشعارك بوجود نشاط غير معتاد على حسابك.

على انستجرام، ادخل/ي على الإعدادات < الأمان < نشاط تسجيل الدخول

تذكر/ي دائما بالتحقق من مصدر رسائل البريد الإلكتروني , لتكن من عاداتك التحقق مما إذا كانت الرسالة الإلكترونية حقيقية أم آتية من أحد تطبيقات فيسبوك أو من مخترق يحاول تصيد معلوماتك الشخصية.

للتحقق من مصدر رسائل البريد الإلكتروني:

على فيسبوك، انقر/ي على الإعدادات والخصوصية < الإعدادات < الأمان وتسجيل الدخول < عرض أحدث رسائل البريد الإلكتروني من فيسبوك

على انستجرام، انقر/ي على الإعدادات < الأمان < رسائل البريد الإلكتروني الواردة من انستجرام

إذا كنت تعتقد/ى أن حسابك تعرض للهجوم، قم بالخطوات التالية:

١. سجلي الخروج من جميع الجلسات الفعالة:

على فيسبوك، انقر على: الإعدادات والخصوصية < الإعدادات < الأمان وتسجيل الدخول < المكان الذي سجلت دخولك منه.

على انستجرام، انقر على: الإعدادات < نشاط تسجيل الدخول.

على واتساب، انقر على: واتساب ويب < تسجيل الخروج من جميع أجهزة الحاسب.

٢. غيري كلمة المرور.

على فيسبوك، انقر على: الإعدادات < الأمان وتسجيل الدخول < تغيير كلمة السر.

على انستجرام، انقر على: الإعدادات < الأمان < كلمة السر.

على واتساب، انقر على: الإعدادات < الحساب < التحقق بخطوتين < تغيير رقم التعريف.

٣. فعل المصادقة الثنائية.

على انستجرام: الإعدادات < الأمان < المصادقة الثنائية.

على واتساب: الحساب < التحقق بخطوتين < تمكين.

توخى الحذر حيال ما تقوم بمشاركته

١. حافظ على خصوصية بياناتك الخاصة.
٢. تحكم بمسألة من يمكنه العثور عليك على الانترنت.
٣. شارك ما يهم مع من يهمون

قومي بمراجعة إعدادات الخصوصية لديك.

- على فيسبوك، انقر على: الإعدادات والخصوصية < اختصارات الخصوصية.
- على انستجرام، انقر على: الإعدادات < الخصوصية.
- على مسنجر، انقر على: الإعدادات < الخصوصية
- على واتساب، انقر على: الإعدادات < الحساب < الخصوصية

كيفية تأمين الهواتف والأجهزة الإلكترونية

نصائح لاستخدام هواتف ذكية آمنة:

أولا : استعمال الخدمات السحابية :

بمعنى استخدام خدمات التخزين على الإنترنت، 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. إلّا 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.

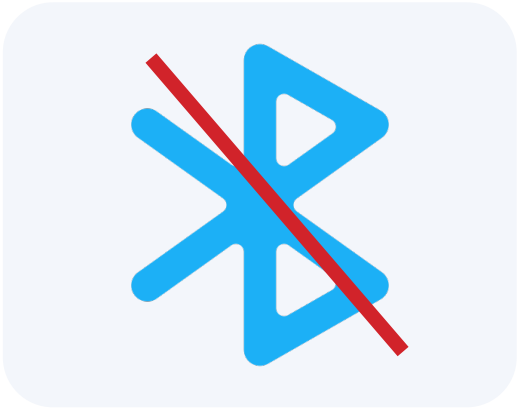
ثانياً: تجنّب/ي تنصيب/تحميل التطبيقات الخارجية :

يتم الدخول إلى iOS، أو Android كلنا نعلم أنه للبحث عن تطبيق في منصتي متجري التطبيقات الخاصين بـ هاتين 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 وحتى العبث بهاتفك وسرقة بياناتك.

ثالثًا: تفعيل خدمة تحديد الموقع :

أصبحت غالبية أنظمة الهواتف الذكية توفر هذه الخدمة وحتى بعض التطبيقات التي تمكن من تحديد هوية سارق الهاتف إن وقعت مثل هذه الحادثة، أو حتى تحديد الموقع الذي يوجد فيه الهاتف إذا تم ربطه بالانترنت.

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 حذف كل المعلومات الموجودة في الهاتف عن بعد إذا ما سُرق أو ضاع الهاتف الذكي، بما أن أكبر تهديد أمني يمكن أن يقع للهاتف هو سرقته أو ضياعه.

سادسا:الحذر من الشبكات المفتوحة :

الحذر عن استخدام شبكات الانترنت المفتوحة للعموم(wireless free) إذ يمكن للهاكرز دخولها بسهولة ومعرفة الأجهزة الإلكترونية التي تلج الانترنت عبر هذه الشبكات، وبالتالي إذا ما اضطريت إلى استخدام هذه الشبكات، عليك أن أي شبكة خاصة افتراضية، وهي خدمة تتيحها VPN، تحاول ما أمكن استخدام البعض المواقع والبرامج، كي يتم الربط بين حواسيب معيّنة عن بعد بشكل آمن، أو كي يتم تعمية 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 لمعرفة نوعية الكاميرا، ونوعية اتصال الإنترنت، أو استخدام الاسم الموجود على الشبكات الاجتماعية. غير أن هناك بعض التطبيقات التي تطلب استخدام الكاميرا أو الولوج إلى دليل الهاتف، وهو أمر غير مقبول ويجب الحذر من استخدام هذا التطبيق.

ثامنا: عدم استخدام كلمة سر واحدة :

عدم استخدام كلمة السر نفسها في جميع التطبيقات والمواقع التي تدخلينها، فاستخدام هذه الكلمة في شبكة غير محمية، قد يتيح للهاكر معرفتها وبالتالي استخدامها في بقية الحسابات على المواقع الاجتماعية مثلًا. فضلًا عن ضرورة تعقيد هذه الكلمة، واستخدام تقنية التثبت من حقيقة المستخدم بإرسال كود في رسالة قصيرة على رقم الهاتف أن 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.

الخطوات الأساسية لتعمية الأجهزة

١. تأكد من أن بطاقة SIM الخاصة بك مقفلة بكلمة السر وتفادى ان تزيلي هذه الخاصية كما يفعل العديد منا.
٢. تأكد كذلك من وضع تعمية لقفل الشاشة سواء برمز أو PIN بالوسائل المتعددة الأخرى لتفادي التطفل على جهازك، مع تحديد وقت الإقفال الذي يستحسن ضبطه كذلك.
٣. ينصح الأخصائيون في الأمان الرقمي بتعمية إعدادات الشبكة عن طريق إيقاف الإشتغال الإفتراضي «بالواي فاي» أو البلوتوث أو حتى NFC بتقنية .
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.

تطبيقات آمنة للتمتع بمستوى حماية أفضل

هنا سرد ملخص لبعض تطبيقات المحادثات و ننصح المستفيدات دائماً بالبحث عن ما يناسبهن عند استخدام تطبيقات المحادثات.

سيجنال (Signal)

(سيجنال هو خدمة مراسلة مشفرة عبر مختلف المنصات، وتركِّز على المكالمات الصوتية المشفرة بين الأطراف والرسائل النصية المشفرة، ويُعد هذا التطبيق أحد أقوى تطبيقات المراسلة أمانًا في السوق.

تطبيق المراسلة سيجنال مجاني الاستخدام ومتوفِّر على كلٍ من نظامي التشغيل Android وiOS، كما يوجد منه إصدار للحاسوب لأنظمة Windows وMac وLinux، لكنك ستحتاج إلى رقم هاتف من أجل استخدامه.

تجربة المستخدم مشابهة لتطبيقات المحادثة الشهيرة الأخرى مثل واتس آب وفيسبوك ماسنجر، ومزاياه تشمل الرسائل بين شخصين اثنين والرسائل الجماعية والملصقات والصور ونقل الملفات والمكالمات الصوتية ومكالمات الفيديو.

ظهر تطبيق سيجنال عام ٢٠١٣ تقريبًا، لكن ازدادت شعبيته كثيرًا في ٢٠٢٠ و٢٠٢١).

ما مدى أمان تطبيق سيجنال؟

- تطبيق سيجنال ليس مملوكًا لإحدى شركات التقنية الكبيرة، بل إنه مشروع مفتوح المصدر يدعمه منح وتبرعات، وهذا يعني أنه لا يوجد به إعلانات أو شركات تابعة أو تعقب سري.
- المحادثات على سيجنال مشفرة بين الأطراف، وهذا يعني أن الأشخاص في المحادثة فقط هم من يمكنهم رؤية الرسائل ولا يراها أحد غيرهم (ولا مالكو تطبيق سيجنال أنفسهم).
- توفِّر التطبيقات الأخرى التعمية بين الأطراف كخيار، لكنه هو الاختيار الافتراضي في تطبيق سيجنال.
- يوفِّر سيجنال رسائل ذاتية التدمير ومختفية، أي رسائل يتم حذفها تلقائيًا بعد وقت محدد.
- يحاول سيجنال عدم جمع الكثير من المعلومات عن مستخدميه، ويتم تخزين كل شيء في تطبيق المراسلة سيجنال، بما في ذلك الرسائل والصور والملفات، محليًا على جهازك فقط.
- تستخدم التطبيقات الأخرى بروتوكول رسائل سيجنال في أنظمتها الأكثر أمانًا، ومن بين تلك التطبيقات واتس آب وواير.

وایر (Wire)

(یروج تطبیق وایر لنفسه على أنه تطبیق مراسلة آمن منذ أن صدر في ٢٠١٤، والشركة التي أسست هذا التطبیق تقع في سویسرا وتُعد واحدة من أفضل الشركات والسلطات في العالم لأي نوع من الخدمات الأونلاین الآمنة أو تطبیقات المحادثة الآمنة. یمكن استخدام تطبیق وایر على أنظمة Android و iOS و OS mac و Windows وكذلك المتصفحات المشهورة)

ما مدى أمان وایر؟

- وایر من التطبیقات التي تستخدم التعمیة بین الأطراف، وتعمیة وایر یعمل بشفافیة وسلاسة في الخلفیة ولا یحتاج إلى أن یتم تنشیطه بنفسك لأنه دائمًا ما یكون نشطًا.
- وایر لا یبیع تحلیلات البیانات أو استخدامها إلى أطراف خارجیة.
- تطبیق وایر یشبه تطبیق سیجنال في أنه مفتوح المصدر، وهذا یعني أنه برمجته متاحة كي یتفحصها المستخدمون و یتأكدون منها ویعملون على تحسینها (عبر GitHub في هذه الحالة).
- قام بعض الخبراء من خارج تطبیق وایر بتدقیقه، لذلك إذا لم یكن لدیك الخبرة الكافیة أو الوقت الكافي لعرض برمجته ومصدره بنفسك، یمكنك قراءة النتائج الموجودة على الإنترنت بالفعل.
- یمكنك التسجیل بالبرید الإلكتروني فقط، ولن تحتاج إلى رقم هاتف.
- التطبیق متوافق مع النظام الأوروبي العام لحمایة البیانات بشكل كامل.

ثریما (Threema)

(ثریما تطبیق تبادل رسائل مشفرة بین الأطراف، ویختلف عن كثیر من التطبیقات الأخرى في أنه لا یتطلب منك إدخال عنوان بریدك الإلكتروني أو رقم هاتفك من أجل فتح حساب، وهذا یوفّر للمستخدمین مستوى عالیًا من السریة والخصوصیة. من مزایا هذا التطبیق الرسائل النصیة والصوتیة ومكالمات الفیدیو والمكالمات الجماعیة وقوائم التوزیع. تطبیق ثریما لیس مجانیًا، بل یدفع المستخدمون مقابل استخدامه، والشركة التي أسسته تقع في سویسرا).

ما مدى أمان ثريما؟

- المبدأ الأساسي لعمل تطبيق ثريما هو السيطرة على البيانات الوصفية. لضمان عدم استغلال أي بيانات بطريقة خاطئة، تعمل خوادم ثريما على حذف الرسائل إلى الأبد بعد توصيلها إلى المستلم.
- عادةً ما يتم إدارة المعلومات على خادم يتم إدارته محليًا على جهاز المستخدم، وهذا يعني أن أي محادثة تكون محمية من التنصت، وبالتالي لا يمكن أن تكون الاتصالات غير مشفرة، ومن ثم لا يمكن لأي شخص أن يقرأ رسائل ثريما إلا الشخص المرسل إليه الرسائل.
- ثريما تطبيق مفتوح المصدر، لذلك يمكن للمستخدمين التأكد بأنفسهم من مدى تعمية التطبيق.
- المشكلة أن التطبيق لا يدعم المصادقة ثنائية العوامل.

Me Wickr

(تأسس Wickr في ٢٠١٢ على أيدي مجموعة من خبراء الأمان وأنصار الخصوصية، وهو واحد من تطبيقات المراسلة التي يمكن استخدامها بكل سرية فعلاً. يتفرع من هذا التطبيقات عدة إصدارات مختلفة كل منها مخصص لمجموعة مستخدمين معينة: Me Wickr وPro Wickr وRAM Wickr وEnterprise Wickr. يستهدف Me Wickr المستخدمين الأفراد).
Me Wickr لا يتطلب عنوان بريد إلكتروني أو رقم هاتف عند التسجيل، وهذا يضمن عدم جمع بيانات المستخدم وبالتالي لا يكون للتطبيق أي وصول إليها من الأساس. يمكن النظر إلى Wickr على أنه أداة تعاون أكثر من مجرد تطبيق مراسلة حيث يوجد به القدرة على مشاركة الشاشة والمواقع الجغرافية والحالات عبر الإنترنت.

ما مدى أمان Me Wickr؟

- يستخدم التطبيق التعمية بين الأطراف لجميع الرسائل والملفات، بما في ذلك الصور ومقاطع الفيديو، وهذا يضمن أنه لا يوجد أي أطراف خارجية تقدر على الوصول إلى البيانات وهو ينقلها من جهاز إلى جهاز آخر.
- جميع الرسائل المتبادلة على تطبيق Wickr مشفرة بشكل محلي على كل جهاز مع إنشاء مفتاح جديد لكل رسالة جديدة، وهذا يعني أن فقط مستخدمي Wickr هم من يملكون مفاتيح فك تعمية محتوى الرسائل. وبالإضافة إلى تعمية بيانات المستخدم ومحادثاته، يجرِّد تطبيق Wickr البيانات الوصفية من أي محتوى يتم نقله عبر الشبكة.

- التعمية مفعل بشكل افتراضي، وتقارير الشفافية متوفرة لأي شخص يستخدم Wickr.
- يدعم التطبيق المصادقة ثنائية العوامل.
- لا يقوم Wickr بتسجيل عناوين IP والبيانات الوصفية الأخرى.
- هذا التطبيق مفتوح المصدر ويوفِّر الرسائل ذاتية التدمير.
- يوفِّر Wickr ميزة تسمح للمستخدمين باكتشاف التقاط لقطة شاشة لهم، وهذا يعني أنك ستتلقى إشعارًا إذا ما قام شخص ما بأخذ لقطة شاشة لرسالة أرسلتها.

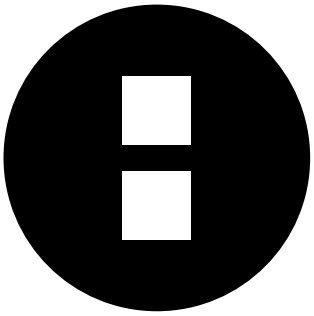
فايبر (Viber)

(فايبر هو تطبيق لتبادل الرسائل النصية والصوتية عبر مختلف المنصات، وهو من إدارة الشركة اليابانية المتعددة الجنسيات Ratuken. تنزيل هذا التطبيق مجاني، ويتيح للمستخدمين إجراء مكالمات مجانية وإرسال رسائل نصية وصور ومقاطع فيديو إلى مستخدمي فايبر الآخرين. يمكنك استخدام فايبر في إنشاء محادثات جماعية تضم حتى ٢٥٠ شخصًا وإجراء مكالمات صوتية مع ما يصل إلى ٢٠ شخصًا مرة واحدة).

ما مدى أمان فايبر؟

- فايبر أحد تطبيقات تعمية المحادثات لكنه لا يعتبر الاختيار الاول للكثير من المهتمين بالسلامة الرقمية
- في حال اختيار المستخدمين لطريقة المشاركة الصحيحة، يوفِّر فايبر محادثات صوتية وفيديو على أنظمة التشغيل المشهورة لأجهزة الهواتف المحمولة والكمبيوتر.
- فيما سبق كانت الحماية متوفرة للمحادثات بين فردين فقط، لكنها الآن متوفرة للمحادثات الجماعية كذلك بالتعمية بين الأطراف.
- كل محادثة في تطبيق فايبر محددة بلون حسب درجة تعميتها:
- الأخضر يعني أن المحادثة مشفرة، وبالتالي الشخص الذي تتواصل معه موثوق به.
- الرمادي يعني أن المحادثة مشفرة لكن الشخص الذي تتحدث معه ليس موثوقًا به.
- الأحمر يعني أنه يوجد مشكلة في التأكد من الشخص الذي تتواصل معه.

داست (Dust)



(داست كان معروفًا فيما سبق باسم سايبر داست (Cyber Dust)، وهو تطبيق مراسلة خاص يستخدم التعمية بين الأطراف للتواصل الآمن. وكما يقول موقعه الرسمي، «يمكنك حذف الرسائل من على هواتف الآخرين، فلا يوجد رسائل مخزنة دائمًا على الهواتف أو الخوادم، كما يتم تعمية الرسائل بشدة ولا ترتبط بأي شخص، ولا حتى نحن).»

ما مدى أمان داست؟

- يمكنك إرسال رسائل خاصة اسمها «Dusts» إلى الأسماء المسجلة عندك، ويمكنك تحديد تدمير الرسائل ذاتيًا خلال ٢٤ ساعة أو بعد قراءتها مباشرةً.
- يمكنك كذلك إرسال رسائل تحمل اسم «Blasts»، وهي رسائل يمكنك إرسالها إلى أكثر من شخص لكن كل شخص يقرأها على حدة.
- أيضًا إعدادات تطبيق داست لا تعرض أسماء المستخدمين في الرسائل، ويخبرك التطبيق إذا ما أخذ شخصٌ ما لقطة شاشة لك من داخل التطبيق.
- بالإضافة إلى كونه تطبيق تبادل رسائل آمن، يوجد كذلك ميزة لمراقبة الخصوصية وأداة للبحث الآمن بهدف المحافظة على الخصوصية أثناء البحث على الإنترنت.

آي مسج (iMessage)

(آي مسج هو تطبيق يقدم خدمة الرسائل الفورية من تطوير شركة آبل، وتم إصداره في ٢٠١١، ويوفِّر هذا التطبيق خدماته على منصات آبل حصريًا: iOS وmacOS وiPadOS وwatchOS.

ما مدى أمان آي مسج؟

- يوفِّر آي مسج التعمية بين الأطراف بين المستخدمين.
- من المشكلات الأمنية المحتملة هي خيار النسخ الاحتياطي لرسائلك على التطبيق إلى خدمة التخزين السحابي آي كلاود، وبالتالي الرسائل المخزنة على السحابة تكون مشفرة بمفاتيح تتحكم فيها آبل؛ وهذا يعني أنه إذا ما تم اختراق حسابك على آي كلاود، يمكن الكشف عن هذه الرسائل.
- الحل هنا بسيط، وهو تجنب تخزين الرسائل الخاصة على المنصات التي المبنية على الويب مثل آي كلاود من أجل زيادة إجراءات الأمان المتبعة.

- يتيح آي مسج للمستخدمين التحكم في مدة ظهور صورهم أو مقاطع الفيديو أو الرسائل قبل أن تختفي. يمكنك كذلك اختيار عدد المرات قدرة الشخص المرسل إليه على رؤية الرسالة، لكن هذه الميزة غير متوفرة إلا على نظام iOS ١٠ فما أعلى.

لاين (Line)

(لاين هو تطبيق مراسلة آمن ومجاني تم إنشاؤه في أعقاب كارثة تسونامي اليابان عام ٢٠١١، فلقد تعطلت الكثير من وسائل التواصل المعتادة بسبب الكارثة، ومن ثم عملت شركة الإنترنت Naver على تطوير تطبيق لاين كوسيلة تواصل عبر الإنترنت لموظفيها.
بعدها أتاحت الشركة التطبيق للعامة في اليابان في العام نفسه، وقد نال شهرة واسعة محليًا بسرعة قبل أن ينتشر في باقي أرجاء آسيا).

ما مدى أمان لاين؟

- يوفِّر لاين التعمية بين الأطراف، لكن على المستخدمين اختيار هذه الميزة بأنفسهم، والتطبيق يسميها «Sealing Letter».
- يمكنك تسجيل التطبيق باستخدام رقم هاتفك أو تسجيل الدخول عبر فيسبوك.
- التأكد من استخدام تطبيق محادثة آمن للتواصل مع الآخرين يحميك من الجهات الخبيثة التي تحاول سرقة بياناتك، ولكل تطبيق مزايا أمنية مختلفة ووظائف مختلفة، لذلك اختيار التطبيق الذي تستخدمه يعتمد على المزايا الأكثر أهمية لك أنت/ي.

التصفح الامن للانترنت

تعدّ متصفّحات الإنترنت البوابة التي يَعبرُ من خلالها المستخدم إلى الشبكة العنكبوتية، ليتصفّح كل ما قد تمّ تحميله على هذه الشبكة الواسعة. فالغرض الأساسي من متصفّح الإنترنت هو جلب موارد المعلومات وتقديمها للمستخدم بشكلٍ سهلٍ ومباشرٍ.

ومن أبرز المتصفّحات وأقدمها متصفّح **(مايكروسوفت إيدج)** (Edge Microsoft) الذي يُنصَّب بشكلٍ تلقائي مع نظام التشغيل (ويندوز)، وكذلك متصفّحا **(جوجل كروم)** (Chrome Google) و **(موزيلا فايرفوكس** Firefox Mozilla) (واسعة الانتشار) ، بالإضافة لمتصفّح **(أوبرا)** (Opera) **وسفاري** (Safari) وهما الأقل رواجاً.

ينصح فريقنا باستخدام متصفحات مثل Brave , focus firefox و DuckDuckGo لأنهم من أفضل المتصفحات التي تحافظ على خصوصية المستخدمين.

عند تصفّح الإنترنت، فإننا بشكل من الأشكال مرَاقَبون. فلأن كثيراً من المواقع الإلكترونية ترغب في الحصول على أكبر قدرٍ ممكنٍ من المعلومات عنا وحولنا، فإنها – أي المواقع – تُثبتُ برمجيات بأحجام صغيرة جداً تدعى ملفات تعريف الإرتباط أو (Cookies) في المتصفّح الخاص بنا، تساعدها في معرفة ما هي أكثر المواقع التي نرتادها ونتنقل بين صفحاتها كما أن هناك طريقةً أخرى شائعةً للتعقب تعتمد على تثبيت برنامج في المتصفّح يدعى (Adware) وهو نوع من البرامج يراجع المواقع الإلكترونية التي نزورها بشكلٍ دوريٍّ، ليقوم بعد ذلك تلقائياً بإظهار الإعلانات أمامنا بما يتناسب مع محتوى تلك المواقع. كما أن هناك مواقع إلكترونية قادرة على تحديد موقعنا الجغرافي من خلال عنوان «بروتوكول الإنترنت IP.

يُمكن لأيّ موقع إلكتروني تعقب نشاط المستخدم على الإنترنت وانتهاك خصوصيته، وذلك عند استخدام المتصفّحات العادية مثل «مايكروسوفت إيدج » و »فايرفوكس » و »جوجل كروم » و »سفاري »، في

المقابل يُمكن للمستخدمين تجربة بعض المتصفّحات التي توّفر حمايةً للخصوصية وتعميةً لبيانات المستخدم، وتمنع كذلك خاصية التعقب.

تُعرّف المتتبِعات (Trackers)، وتُدعى كذلك «تقنيات الطرف الثالث »، بأنها ملفات تتعقب متصفّح الإنترنت، لتقوم بجمع المعلومات حول المواقع التي تزورها وبيانات أجهزة المستخدمين. وتشمل المتتبعات ملفات «الكوكيز » (ملفات تعريف الارتباط) ومنارات الشبكة و »كوكي ف اش » وعلامة «البيكر » وعنوان «بروتوكول الإنترنت IP » الخاص بنا. تجمع هذه المتتبِعات معلومات حول تاريخ التصفح، وحجم الشاشة، والمنطقة الزمنية، والمكونات الإضافية، ونظام التشغيل، كل هذه الأشياء تُشلُ بصمةً فريدةً لكل واحد منا، وبالتالي تتمكن المتصفّحات بسهولة من التعرّف علينا بوساطة هذه البصمة.

قد تتواجد المتتبِعات في المواقع الإلكترونية على شكل متعقبٍ واحدٍ فقط أو قد تصل ل (٦٠ متعقباً للموقع الواحد) ، وقد لا يكون هناك أي متعقّبٍ في الموقع الإلكتروني. بعض هذه المتتبِعات (Trackers) ضرورية تقنياً لعمل الموقع الإلكتروني بالشكل الصحيح، كالمتعقِبات الخاصة بإعطاء صاحب الموقع فكرة حول حركة المرور (أي نشاط المستخدمين على موقعه، والوقت الذي يقضونه فيه، وغير ذلك)، إلا أن هناك معلومات حول العمر ومكان السكن والأشياء التي تهمّنا والمواضيع التي نقرأ، كل هذه المعلومات يتم تصديرها لشركات الإعلانات أو الحكومات.

عند قبول هذه المتَتبِعات (قنيات الطرف الثالث) نكون قد سمحنا لجميع المتعقِبَات الموجودة بالوصول إلى معلوماتنا. ومن بينها بعض المتعقِبَات المرئية كزر الإعجاب على «فيسبوك » وطائر «تويتر » وزر «جوجل+ (G+) .

يمكننا فحص درجة الأمان في المتصفّح الخاصّ بنا من خلال خدمة (panopticlick) التي تُبينّ إذا ما كان متصفّحنا متصفحاً آمناً من متتبعات الإعلانات والمتتبعين غير المرئيين وبصمات التصفح. كما يمكننا مشاهدة المتعقبات على متصفّح «فايرفوكس » من خلال أداة (Lightbeam) وملاحظة كيف تؤدي المتعقِبَات دورَها في التواصل والترابط فيما بينها.

محاولة للحدّ من تلك السلبيات، يمكنك استخدام أداة (Badger Privacy) التي تقوم بتحديد الإعلانات التي تتجسس علينا عبر الإنترنت وحجبها تلقائياً، كما تقوم بحجب كافة أنواع المتتبعات. تعدّ هذه الأداة مُركّباً إضافياً للمتصفّح، تحلّلُ المواقع الإلكترونية للكشف عن المحتوى الذي يتتبّع نشاطاتنا وتحجبه. فحينما نزور موقعاً ما، فإن هذه الأداة ترصد كذلك المحتوى الذي تم تضمينه من مواقع أخرى، أو ما يُعرَف بمواقع «الطرف الثالث » كالصور والبرمجيات الصغيرة والإعلانات. وفي حال كانت إحدى تلك المواقع من النوع الذي يتتبع، فإن هذه الأداة ستمنع ظهور أي محتوى يتضمن أوامر برمجية للتتبع.

كما تمكن الاستفادة من أداة (Ghostery) التي تمنع المواقع والشركات من تعقب خصوصية الزائر،وذلك عبر منع وصولها إلى بيانات الشخص المستخدم، وتتيح الأداة لمستخدميها درجة تحكم كبيرة تمكنهم من تحديد المواقع التي تتعقب خصوصيتهم وتستهدف بياناتهم، وهي متوفرة لجميع أنواع المتصفّحات.

الجزء الثالث

(الوسائل الإجرائية القانونية للتعامل مع العنف الرقمي)

تسعى الدول الى إيجاد أطر قانونية للحد من جرائم العنف , من خلال إصدار التشريعات والقوانين المتعاقبة للحد من تلك الجريمة ونجد أن المشرع لم يغفل اى بند , وقد يعتقد البعض أن جرائم لم يصدر لها قانون ولكن المشرع اكتفى إذا وجد فى قانون آخر .ومعرفتنا بالقوانين

ونستعرض القوانين المترابطة للجرائم الإلكترونية بداية من الدستور نهاية إلى آخر قانون صدر بهذا الشأن

الدستور المصرى ٢٠١٤

المادة ٥٧

(للحياة الخاصة حرمة, وهى مصونة لا تمس. و للمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها , ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك).

قانون الإجراءات الجنائية

المادة (٣) :

(لا يجوز أن ترفع الدعوى الجنائية إلا بناء على شكوى شفهية أو كتابية من المجني عليه، أو من وكيله الخاص، إلى النيابة العامة، أو إلى أحد مأموري الضبط القضائي في الجرائم المنصوص عليها في المواد ١٨٥ و ٢٧٤ و ٢٧٧ و ٢٧٩ و ٢٩٢ و ٢٩٣ و٣٠٣ و٣٠٦ و٣٠٧ و٣٠٨ من قانون العقوبات، وكذلك فى الأحوال الأخرى التي ينص عليها القانون. ولا تقبل الشكوى بعد ثلاثة أشهر من يوم علم المجني عليه بالجريمة وبمرتكبها ما لم ينص القانون على خلاف ذلك).

قانون العقوبات

المادة ١٦٦ مكرر

(كل من تسبب عمداً في إزعاج غيره بإساءة استعمال أجهزة المواصلات التليفونية يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تزيد على مائة جنيه أو بإحدى هاتين العقوبتين).

المادة ٣٠٩ مكرر

(يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

(أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

(ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً.

ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما تحكم بمحو التسجيلات المتحصلة عنها أو إعدامها).

المادة ٣٢٦

(كل من حصل بالتهديد على إعطائه مبلغا من النقود أو أي شيء آخر يعاقب بالحبس. ويعاقب الشروع في ذلك بالحبس مدة لا تتجاوز سنتين).

المادة ٣٢٧

(كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو السجن المؤبد أو المشدد أو بإفشاء أمور أو نسبة أمور مخدشة بالشرف وكان التهديد مصحوبا بطلب أو بتكليف بأمر يعاقب بالسجن.

ويعاقب بالحبس إذا لم يكن التهديد مصحوبا بطلب أو بتكليف بأمر.

وكل من هدد غيره شفهياً بواسطة شخص آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوباً بتكليف بأمر أم لا.

وكل تهديد سواء أكان بالكتابة أم شفهياً بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه).

قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣

المادة ٧٦

(تنص المادة ٢/٧٦ من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ على أنه أن مع عدم الإخلال بالحق في التعويض المناسب يعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من: ..... ٢- تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات).

وتنص المادة ١٦٦ مكرراً من قانون العقوبات على أنه "كل من تسبب عمداً في إزعاج غيره بإساءة استعمال أجهزة المواصلات التليفونية يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تزيد على مائة جنيه أو بإحدى هاتين العقوبتين".

قانون رقم قانون ١٧٥ لسنة ٢٠١٨

المادة ١٨

(يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه, أو بإحدى هاتين العقوبتين, كل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بأحد الناس.

فإذا وقعت الجريمة على بريد إلكترونى أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه, أو بإحدى هاتين العقوبتين).

مادة ٢٤

(يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر, وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا ونسبه زورًا إلى شخص طبيعى أو اعتبارى.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع فى أمر يسيء إلى من نُسب إليه، تكون العقوبة الحبس الذى لا تقل مدته عن سنة والغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه, أو بإحدى هاتين العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة, تكون العقوبة السجن, والغرامة التى لا تقل عن مائة ألف جنيه, ولا تزيد على ثلاثمائة ألف جنيه).

المادة ٢٥

(يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته, أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة).

المادة ٢٦

(يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ٣٠٠ ألف جنيه أو بإحدى العقوبتين كل من تعمد استعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها لابمحتوى مناف للآداب العامة أو لاظهارها بطريقة من شأنها المساس باعتباره أو شرفه).

كيفية الإبلاغ

التوجه إلى الشرطة ويجب معرفة هذه الجريمة تتبع أي جهة هل هي مباحث الانترنت , أم مباحث الاتصال إذا كانت الجريمة متعلقة بالهاتف الأرضي , الهاتف المحمول , او رسائل الهواتف الجهة المختصة مباحث الاتصالات

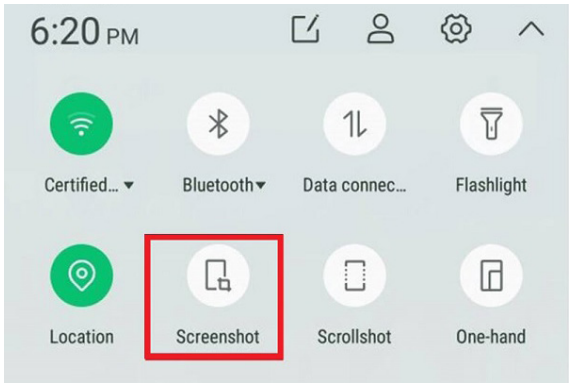
الواتساب whatsapp

حسم محكمة النقض هذا الجدل بشأن الواتساب لانه مرتبط بين أرقام الهواتف والانترنت

- مباحث الانترنت مختصة بجميع التطبيقات أو المواقع والبريد الالكتروني سواء على اجهزة الحاسب او اجهزة الهواتف المحمول.

- يجب عدم مسح أو محاولة اغلاق الصفحات او حسابات مرتكبي الجريمة حتى لا نتسبب فى ضياع الأدلة ونخسر حقوقنا تجاه الجاني .

- عمل لقطة شاشة « اسكرين شوت » مع حفظ اللينك و الاحتفاظ بالرسائل حتى تتمكن الجهة المعنية من الوصول للجاني .



- فثم يجب علينا سرعة التوجه إلى مباحث الإنترنت المتواجد داخل مديريات الأمن بالمحافظات , ثم تقوم بتحرير المحضر وتأخذ رقم سؤال , ثم انتظار التقرير الفني لفحص الايميلات او الاجهزة من قبل الشرطة تتبع الجانى حيث أنهم يتوصلون الى الجانى من خلال « الاي بي IP «الخاص بالهواتف الأرضية أو شبكات المحمول حيث انه الان جميع الارقام تم ربطها من قبل جهاز الاتصالات بالرقم القومى .

- ومن ثم يجب متابعة المحضر بالنيابة العامة والتأكد من القيد والوصف لذا يجب أن نطلب مساعدة المحامى /ة حتى يتمكن من متابعة سير المحضر حتى وصولها للمحكمة.

يجب علينا تطمئنة المجنى عليه/ا حتى يتحقق العدالة ويكون هناك رادع لكل من يسول له نفسه فى انتهاك خصوصية الآخرين .

من هنا يجب علينا أن نسلك ثلاث طرق فقط لا رابع لهم حتى لا نقع تحت ابتزاز اخر مع اشخاص مجهولين الهوية

- ابلاغ الاهل
- منظمات المجتمع المدنى
- الشرطة

ونحن بدورنا كمؤسسة جنوبية نصدق الناجيات من هذه الجريمة ونتعاون معهن لتجاوز هذه المشكلة التى قد تسبب فى خسارة فتيات حياتهن سواء بالانتحار او القتل والوصم . ولكن لا نأخذ بادراتهم فى الابلاغ من عدمه دورنا المساعدة وليس اخذ اجراء دون طلبها بمحض ارادتهن .

يجب علينا ألا نثق فى الصفحات الكبيرة ونعطيهم معلومات حتى لا نقع تحت دائرة اخرى من العنف مع اشخاص مجهولين .

ارقام مكافحة الابتزاز في مصر وطرق الإبلاغ .

أقرت الجهات الرسمية لمكافحة الجرائم الإلكترونية بعض الأرقام للتواصل في حالة التعرض لعنف رقمي

أولها الاتصال بالخط الساخن للابتزاز ١٠٨ أو الاتصال على الأرض ٠٢٢٤٠٦٥٠٥٢. أو الاتصال على ٠٢٢٤٠٦٥٠٥١ للتواصل مباشرة مع إدارة تكنولوجيا المعلومات.

أو عن طريق القيام بتقديم بلاغ عن طريق استخدام الموقع المخصص لوزارة الداخلية.

التواصل على رقم المباحث للابتزاز الإلكتروني وهو ١٢٢.

كما يمكنك التوجه إلى الإدارة العامة لمكافحة جرائم الحاسبات والمعلومات بالمقر الخاص بوزارة الداخلية

نتائج مترتبة على النساء جراء تعرضهن لـ تجربة عنف على الإنترنت

١٢٪ تعرضن للعنف البدني من قبل العائلة

٣٦٪ طلب منهن تجاهله

٢٣٪ تم إلقاء اللوم عليهن

٢١٪ طلب منهن حذف حساباتهن على مواقع التواصل الاجتماعي

وطبقا لنتائج الدراسة، يتفق ١ من بين كل رجلين و ٤ من كل ١٠ نساء (٤١ في المائة) من الدول المشاركة الثمانية على أن «النساء اللاتي يعرضن الصور ومقاطع الفيديو الخاصة بهن يجب أن يتقبلن إمكانية استخدام تلك المواد ضدهن من قبل من يشاهدها».
ويتفق ما يقرب من نصف الرجال (٤٨ في المائة) و٤١ في المائة من النساء على أن العنف على الإنترنت ليس بالأمر الخطير إذا بقي على الإنترنت.

وتقول غالبية النساء الالتي تعرضن للعنف على الإنترنت أن الهجوم كان «بلا سبب محدد» (٥١ في المائة)، ويعتقد النصيب الأكبر من النساء اللاتي يعتقدن معرفة السبب وراء تعرضهن للعنف على الإنترنت (٢٣ في المائة) أنه كان بسبب مظهرهن الخارجي، ويلي ذلك أن مناصرة حقوق المرأة (١٦ في المائة)، الأمر الذي يشير إلى السمة القائمة على النوع الاجتماعي للهجمات على الإنترنت

ويقول النصيب الأكبر من الجناة إن السبب الرئيسي وراء ارتكابهم العنف على الإنترنت هو «لأنه حقهم» (٢٦ في المائة)، ويتبع ذلك ٢٣ في المائة من الذين يقولون إنهم ارتكبوا العنف على الإنترنت « لأنه كان ممتعا».
أبلغت أقل من ١ من بين كل ٣(٣١ في المائة) من النساء اللاتي تعرضن للعنف على الإنترنت عن الحادث، وأغلب النساء أبلغن عن العنف على الإنترنت، فعلن ذلك من خلال المنصة ذاتها (٥٥ في المائة)، وأبلغت ٢٣ في المائة منهن الشرطة بالحادث.

والسبب الأكثر شيوعا لعدم الإبلاغ عن واقعة العنف على الإنترنت بحسب قول النساء هو «لم أظن الإبلاغ أنه سيحدث أي فرق» (٤١ في المائة)، ويتبع ذلك ٢٧ في المائة من النساء اللاتي قلن «لم أعرف ما الجهة التي كان ينبغي إبلاغها بالواقعة».

أسباب عدم الإبلاغ عن العنف على الإنترنت

٤١٪ لم أظن أن الإبلاغ سيحدث أي فرق

١٥٪ لم أثق بالإبلاغ بالواقعة

١٧٪ شعرت بالخوف

٢٧٪ لم أعرف ما الجهة التي كان ينبغي إبلاغها بالواقعة

إن أغلب النساء الالتي أبلغن عن العنف على الإنترنت، قمنا بذلك ذلك على المنصة ذاتها (٥٥ في المائة)، وأبلغت ٢٣ في المائة منهن الشرطة بالواقعة، و١٤ في المائة قمن بإبلاغ منظمة غير حكومية.

جهات الإبلاغ من جانب النساء اللاتي تعرضن للعنف على الإنترنت

١٤٪ منظمات المجتمع المدني

٢٣٪ منظمات المجتمع المدني الشرطة والسلطات المعنية

٥٥٪ المنصة الإلكترونية

ومن خلال النتائج النوعية، اعتبرت منظمات المجتمع المدني أن إلقاء اللوم على الضحايا سبب أساسي لعدم طلب النساء المساعدة، حيث تخشى الناجيات من التعرض للتوبيخ واللوم نتيجة مشاركة صورهن أو الإفصاح عن كونهن ناشطات. ويشمل ذلك الخوف من أن تقوم الشرطة أيضا بإلقاء اللوم عليهن أو إبلاغ أسرهن بما تعرضن له. وهذه المعايير والمواقف الاجتماعية مجتمعة تخلق عقبات شبه مستعصية أمام المرأة التي تلتمس المساعدة. وحددت الدراسة الاستقصائية التي أجريت مع منظمات المجتمع المدني لأسباب المتعلقة بالخصوصية والسرية باعتبارها السبب الرئيسي لعدم قيام الناجيات بالإبلاغ عن العنف ويعقب ذلك الخوف من انتقام الجاني .

معاقبة الجناة هي أفضل إجراء اقترحته النساء للتصدي للعنف على الإنترنت تعتقد النساء أن أفضل وسيلة للتصدي للعنف عبر الإنترنت هي «اتخاذ الشرطة الإجراءات ضد مرتكبي العنف على الإنترنت» (٣٦ في المائة من النساء مقارنة بنسبة ٢٨ في المائة من الرجال)، وخاصة في العراق والأردن والمغرب وفلسطين، وغالبا ما يعتقد الرجال بدورهم أنه يتعين على المنصات الإلكترونية أن تعمل على تحسين سياسات حماية المستخدمين والمستخدمات (٤٠ في المائة من الرجال مقارنة بنسبة ٣٥ في المائة من النساء)

المصادر والمراجع

- أمان تطبيقات المراسلة: ما هي أفضل التطبيقات في الخصوصية؟ (موقع kaspersky)
- مجموعة أدوات الأمن الرقمي (موقع CPJ)
- دليل ورشات مناهضة العنف الجندري الرقمي (حملة- المركز العربي لتطوير الإعلام الاجتماعي)
- دليل سلامة الصحفيين ٢٠٢١
- العنف الرقمي في المغرب (جمعية التحدي للمساواة والمواطنة)
- العنف الرقمي ضد المرأة... إمتداد الظاهرة وتمدد الأشكال (مجلة الرواق للدراسات الاجتماعية والإنسانية)
- التقنية وتقاطعها مع الجندر والنسوية (برنامج نون تك، أحد برامج مؤسسة متون)
- الأمن الرقمي وحماية المعلومات والحق في استخدام شبكة آمنة (مركز هردو لدعم التعبير الرقمي)
- دليل الأمان الرقمي (مركز الإعلام المجتمعي CMC)
- تعميم منظور النوع الإجتماعي في العالم الرقميّ: سلامة النساء والفتيات عبر الإنترنت (مؤسسة male-fe)
- أدوات السلامة الرقمية (source open jordan)
- دليل الأمان الرقمي)حملة المركز العربي لتطوير الإعلام الاجتماعي)
- العنف ضد المرأة في الفضاء الرقمي (رؤى من دراسة متعددة الأقطار في الدول العربية)
- الدليل التدريبي للمدربين والمدربات على التعريف والتوعية بمفاهيم وقضايا النوع الاجتماعي