People Change the World Diakonia

Edraak Foundation For development and equality

الدليل الإرشادي للحمايـــة مـن العنف الرقمي



الدليل الإرشادي للحمايــــة مــن العنف الرقمي

تم تصميم هذا الدليل في إطار تنفيذ مشروع تعزيز حماية النساء والفتيات من تهديدات العنف الإلكتروني بالتعاون مع هيئة دياكونيا بهدف توفير بيئة آمنه ومستدامة للنساء والفتيات في الفضاء الرقمي، تمكنهن من التعبير عن أنفسهن بحرية وخصوصية، يسعي المشروع إلي تمكين النساء والفتيات من معرفة حقوقهن في الفضاء الرقمي، وتعزيز قدرتهن علي اتخاذ تدابير لحماية أنفسهن من الاعتداءات الرقمية ومكافحة أشكال العنف الإلكتروني التي قد تواجهها النساء والفتيات عبر الإنترنت، من خلال نشر ثقافة الأمان الرقمي وتعزيز الوعي بالتهديدات الرقمية وأساليب الحماية المتاحة، مع التركيز علي تقديم الدعم والمساندة للضحايا وتشجيع ثقافة الإبلاغ عن تلك الجرائم، يركز المشروع علي بناء شراكات منظمات المجتمع المدني والمجموعات النسوية والطلابية والمؤسسات التعليمية بهدف نشر المعرفة والمهارات اللازمة لتعزيز الأمان الرقمي علي مستوي المجتمع ككل.



إعداد
نورهان ثروت

تعريف بالمؤسسة

مؤسسة إدراك للتنمية والمساواة مؤسسة مصرية غير هادفة للربح مشهرة بوزارة التضامن الاجتماعي برقم 11014 لعام 2019، تهتم بدعم وجود النساء ومشاركتهم اجتماعيًا واقتصاديًا وسياسيًا في المجال العام ومناصرة القضايا التي تمكنهن من الحصول على حقوقهن الأساسية كاملة، وتحقيق المساواة في قضايا النوع الاجتماعي ومكافحة أشكال العنف والتمييز في المجالين العام والخاص، من خلال توفير وسائل الدعم والحماية والإرشاد الاجتماعي لضحايا/ الناجيات من العنف وتقديم خدمات التوعية المختلفة.

وتشتبك المؤسسة مع قضايا النساء والفتيات من خلال تصميم حملات المناصرة والدعم، إلى جانب إصدار الدراسات والتقارير الرصدية منذ 2020 من خلال (مرصد جرائم العنف القائم على النوع الاجتماعي ضد النساء والفتيات). وتولى المؤسسة إهتمام بالشراكات متعددة القطاعات مع أصحاب المصالح المعنيين بقضايا النساء وصناع وصانعات القرار والتشريعيين/ات، كما تعمل على دمج وإشراك الرجال في دعم ومناصرة قضايا النساء والفتيات، وتولى المؤسسة اهتمام خاص لبرامج الصحة الجنسية والإنجابية والتنمية المجتمعية والتمكين الاقتصادي للنساء والفئات الأولى بالرعاية في المجتمعات المحلية.

الفهرس

- لمن نوجه هذا الدليل 3
- لماذا دليل جديد عن العنف الرقمي الموجه للنساء 4
- مقدمة عن العنف الرقمي 5
- أشكال العنف الرقمي والتهديدات الرقمية 6
- التشريعات والقوانين المتعلقة بالعنف الرقمي 27
- استراتيجيات الوقاية والدعم 28
- خطوات الإبلاغ عن العنف الرقمي أو الابتزاز الإلكتروني 30
- آليات الإبلاغ عن العنف الرقمي على منصات السوشيال ميديا المختلفة 34
- أهم ممارسات الحماية الرقمية 37
- توصيات ختامية بشأن جرائم العنف الرقمي الموجه للنساء والفتيات: 38
- توصيات بالإجراءات العاجلة للجهات القضائية والمشرّع في قضايا العنف الرقمي الموجه النساء والفتيات في مصر 39



لمن نوجه هذا الدليل؟

يستهدف هذا الدليل جميع النساء والفتيات في مصر ممن يتعاملن مع الفضاء الرقمي، سواء لأغراض شخصية، مهنية، تعليمية أو مجتمعية، مع التركيز على الفئات الأكثر عرضة للعنف الرقمي، مثل الناشطات في الشأن العام، والصحفيات، والمدافعات عن حقوق الإنسان، والمستخدمات الشابات لوسائل التواصل الاجتماعي. كما يوجَّه الدليل إلى النساء من خلفيات مختلفة، بما في ذلك النساء والفتيات ذوات المعرفة التقنية المحدودة وغير المتخصصة، بهدف تمكينهن من أدوات الحماية الرقمية وتعزيز قدراتهن على مواجهة المخاطر الإلكترونية، في ظل ازدياد وتنوع أنماط العنف الرقمي في السنوات الأخيرة.



لماذا دليل جديد عن العنف الرقمي الموجه ضد النساء؟

يركز الدليل على أمثلة مستوحاة من حالات حقيقية تعرضت فيها النساء والفتيات لأنواع متعددة من العنف الرقمي، ويرصد التطورات التي نتجت عن عمل المبادرات والمنظمات النسوية والمعنية بالحقوق الرقمية بالإضافة للتطور فيما يتعلق بالبنية والآليات القانونية في السنوات الأخيرة، نتيجة لإلقاء الضوء الذي قامت به مختلف المبادرات بالتعاون والعمل مع الفتيات والنساء اللاتي قررن مواجهة العنف الرقمي والنضال من أجل جعل المساحات الرقمية أكثر أمانا للجميع.

يتناول الدليل أنواع العنف الرقمي المختلفة والإجراءات وآليات الحماية والإبلاغ المختلفة والتمييز بين الخيارات المتاحة ويركز على الخطوات العملية للحماية القانونية والرقمية، لذلك فإن هذا الدليل لا يتناول السلامة الرقمية في العموم بل يركز على الجوانب ذات الصلة بالعنف الرقمي المبني على النوع الاجتماعي.

مقدمة عن العنف الرقمي :



في عصر تتسارع فيه التكنولوجيا وتتوسع فيه المساحات الرقمية، أصبحت الإنترنت جزءًا لا يتجزأ من حياة النساء والفتيات في مصر. فهي تتيح فرصًا للتعلّم، التعبير، العمل، والتواصل. لكن في الوقت ذاته، فتحت هذه المساحات أبوابًا جديدة لأنماط من العنف لم تكن مألوفة من قبل — عنف رقمي يتسلل خلف الشاشات ويترك أثرًا عميقًا على النفس والجسد والحياة.

العنف الرقمي ضد النساء والفتيات ليس مجرد تهديدات عابرة أو مضايقات "افتراضية"، بل هو شكل حقيقي وخطير من أشكال العنف القائم على النوع الاجتماعي، يتجلى في التحرش، الابتزاز، الملاحقة، انتحال الهوية، والتشهير، ويؤثر على خصوصية النساء وسلامتهن النفسية والجسدية وحتى مشاركتهن العامة.

في مصر، تتزايد حالات العنف الرقمي بشكل ملحوظ، في ظل فجوة كبيرة في الوعي المجتمعي، ونقص في الحماية القانونية، وقلة نسب الإبلاغ عن هذه الانتهاكات. وقد تتعرض النساء من مختلف الأعمار والخلفيات إلى هذا النوع من العنف، خاصة حين يرفعن أصواتهن، أو يظهرن في الفضاء العام، أو يعبّرن عن آرائهن بحرية.

جاء هذا الدليل الإرشادي ليكون أداة توعوية وعملية، تهدف إلى:

- فهم أشكال العنف الرقمي المختلفة الموجهة ضد النساء والفتيات.
- رفع الوعي بالحقوق الرقمية وأهمية حماية البيانات والخصوصية.
- تمكين النساء من استراتيجيات الحماية والاستجابة عند التعرض للعنف الرقمي.
- تعزيز ثقافة التضامن والسلامة الرقمية بين النساء والداعمين لحقوقهن.

نأمل أن يكون هذا الدليل مساحة آمنة ومعرفة مشتركة، تساعد النساء والفتيات في مصر على استعادة السيطرة على حياتهن الرقمية، والمطالبة بحقهن في فضاء إلكتروني آمن.

أشكال العنف الرقمي والتهديدات الرقمية:

في الوقت الذي أصبح فيه الإنترنت جزء أساسي من حياتنا اليومية، ظهرت أنواع جديدة من العنف، عنف غير مرئي في أغلب الحالات. العنف الرقمي هو أي سلوك مؤذي يمارس باستخدام الإنترنت أو الموبايل أو وسائل التواصل الاجتماعي.

في مصر تتعرض الكثير من الفتيات والسيدات لأشكال مختلفة من العنف الرقمي، سواء من معارف/ أصدقاء أو من غرباء. مما قد يسبب لهن ضررًا نفسيًا كبيرًا، ويؤثر على شعورهن بالأمان، وحتى على مشاركتهن في الفضاء الرقمي.

لذلك من المهم فهم ما هي أشكال العنف الرقمي، وكيف يمكن تمييزها، ماذا نفعل إذا تعرضنا لها، حتى نستطيع مساعدة أنفسنا ومساعدة أخريات.

أولا: التحرش الجنسي الإلكتروني



في السنوات الأخيرة، تم رصد العديد من الحالات التي قام فيها أشخاص باختراق حسابات فتيات على وسائل التواصل الاجتماعي مثل "إنستغرام" و"واتساب" وسرقة صور خاصة منهن، ثم استخدام هذه الصور لابتزاز الضحايا ماديًا أو جنسيًا. وصلت بعض هذه القضايا إلى النيابة العامة، في حين امتنعت أخريات عن الإبلاغ خوفًا من الوصم المجتمعي.

أمثلة على أساليب التحرش:

رسائل مباشرة على وسائل التواصل والاتصال المختلفة تتضمن تعليقات أو صور جنسية.

نشر تعليقات جنسية على منشورات النساء.

كيف أحمي نفسي من التحرش الجنسي الإلكتروني؟

1 إرفعي مستوى الخصوصية في حساباتك

- اجعلي حساباتك على وسائل التواصل خاصة (Private).
- حددي من يستطيع إرسال رسائل لك أو الإشارة إليك (Tag).
- لا تشاركي معلومات شخصية مثل رقم الهاتف، العنوان، المدرسة/الجامعة.

2 احظري فورًا أي شخص يرسل محتوى غير لائق

- لا تردي على الرسائل المسيئة، الحظر أفضل رد.
- كل منصات التواصل فيها زر للإبلاغ عن التحرش (Report).

3 استخدمي اسم وصورة غير واضحة إذا لزم الأمر

- خاصة في الحسابات العامة، يمكنك استخدام اسم مستعار وصورة رمزية لتقليل الاستهداف.

4 كوني حذرة من الغرباء

- كثير من المتحرشين يبدؤون بلغة لطيفة ثم تتحول رسائلهم إلى رسائل مسيئة.
- لا تشاركي صورًا أو معلومات خاصة مع أشخاص لا تعرفينهم جيدًا.

5 وثّقي كل حالة تحرش

- التقطي سكرين شوت (صور للشاشة) لأي رسالة أو تعليق مسيء.
- احتفظي بالرابط وتاريخ المحادثة. "هذه الأدلة مهمة إذا قررتِ الإبلاغ لاحقًا"

ماذا أفعل إذا تعرّضتُ لتحرش جنسي إلكتروني خطوات عملية:

1. لا تردي ولا تدخلي في جدال مع المتحرش.
2. احظري الشخص فورًا.
3. أبلغي المنصة (فيسبوك، إنستغرام، تويتر...) – لديهم سياسات واضحة ضد هذا النوع من العنف.
4. احفظي الأدلة (صور، رسائل، روابط).
5. قدّمي بلاغًا رسميًا إذا كان التحرش متكررًا أو يتضمن تهديدات: في مصر، يمكن الإبلاغ عن الجرائم الإلكترونية في أقرب قسم شرطة أو عبر مباحث الإنترنت.
6. تواصلي مع جهة داعمة (مؤسسة حقوقية أو محامية أو مجموعة نسوية).



ثانيا: الابتزاز الجنسي (Sextortion)

- من خلال الحصول على صور شخصية للضحية سواء من خلال نسخها من على أجهزتها كما في حالة بيع الهواتف الذكية بدون محو محتوياتها أو من خلال تبادل الصور مع الأصدقاء والمعارف أو الشركاء العاطفيين والأقارب، أو حتى من خلال إختراق أجهزة الضحية وسرقة المحتوى، يبدأ المبتز بعدها التواصل مع الضحية والضغط عليها بالصور وتهديدها بنشر هذه الصور إذا لم ترسل صورًا أخرى أو أموالًا، أو لقاء للقيام بأفعال جنسية.

كيف احمي نفسي من الابتزاز الجنسي؟

1. لا ترسلي صورًا أو فيديوهات حميمية لأي شخص – حتى لو كان شريك موثوق، لأنه يمكن للعلاقة أن تتغير
2. استخدمي كلمات سر قوية ومختلفة لكل حساب، وفعّلي المصادقة الثنائية (2FA).
3. احذري من الغرباء الذين يطلبون محادثات خاصة أو مكالمات فيديو، خصوصًا لو بدأت بنبرة ودّية وانتهت بطلبات حساسة.
4. راجعي صلاحيات التطبيقات على هاتفك، وتأكدي إنه لا يوجد تطبيق غريب له صلاحية للكاميرا أو الميكروفون.
5. لا تفتحي روابط مجهولة أو ترسلي صور لأي حساب غير موثوق.

ماذا أفعل لو تعرضتِ للابتزاز فعلًا؟

1. لا ترضي بمطالب المبتز أبدًا. الرضوخ لن يوقفه، بل يشجّعه على طلب المزيد.

2. اجمعي الأدلة فورًا (سكرين شوت، روابط، اسم الحساب، أي محادثة).

3. احظري الشخص فورًا على المنصة، ولا تتواصلي معه بعد ذلك.

4. أبلغي إدارة المنصة التي تم فيها الابتزاز (فيسبوك، إنستغرام، إلخ)، غالبًا لديهم سياسات صارمة ضد هذا السلوك.

5. قدّمي بلاغ رسمي: تواصلي مع مباحث الإنترنت من خلال أقرب قسم شرطة أو موقع وزارة الداخلية أو مقر مباحث الانترنت، يمكنك التواصل عبر رقم الخط الساخن على رقم 108
أو اتصلي بالخط الساخن لمركز دعم المرأة: 15115 (تابع للمجلس القومي للمرأة).

6. تواصلي مع جهة دعم نفسي أو قانوني – مثل مؤسسات حقوقية أو مراكز دعم النساء، للمساعدة والتوجيه.



ثالثًا: التنمر الإلكتروني

- في كثير من الحالات تتعرض الفتيات والنساء أثناء البث المباشر على منصات التواصل الاجتماعي، أيا ما كان الموضوع الذي تتناوله لسيل من التعليقات الساخرة سواء على مظهرها، أو لون بشرتها، أو طريقة كلامها، أو مستواها الاجتماعي أو التعليمي. على الأغلب يستمر التنمر حتى بعد انتهاء البث، سواء في التعليقات أو حتى في الرسائل الخاصة، شهدت الكثير من المنصات ردود أفعال لفتيات انسحبن تمامًا وأغلقن حساباتهن بسبب هذه التعليقات، يشمل التنمر:

- إطلاق حملات تشويه أو شائعات عن نساء ناشطات أو إعلاميات.

- السخرية من المظهر أو الصوت أو الخلفية الاجتماعية.

كيف احمي نفسي من التنمر الإلكتروني؟

1 احمي معلوماتك الشخصية

- لا تشاركي معلوماتك الشخصية (مثل عنوانك، رقم هاتفك، صور خاصة، أو تفاصيل حساسة) على الإنترنت أو مع الأشخاص عموما دون ضرورة واضحة.
- استخدمي إعدادات الخصوصية على حساباتك في وسائل التواصل الاجتماعي لتحديد من يمكنه رؤية ما تنشره.

2 تجاهلي، لا تردي

- في كثير من الحالات، التجاهل هو أفضل رد على المتنمر. الرد عليهم قد يعطيهم دافعًا للاستمرار.
- خذي لقطات شاشة (screenshots) إذا لزم الأمر، قبل الحذف أو الحظر.

3 احظري وبلّغي

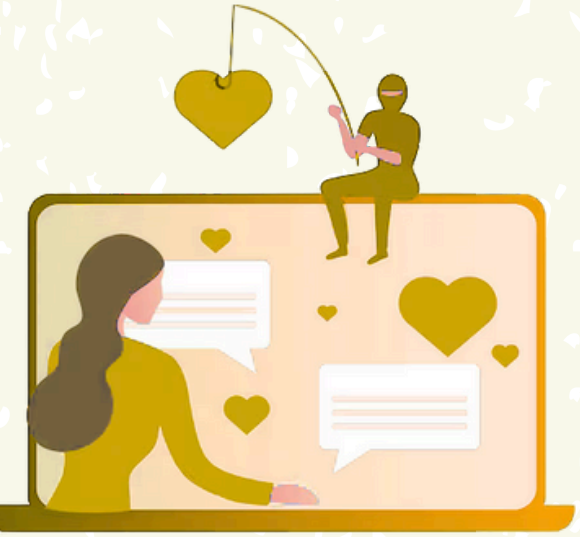
- استخدم خاصية الحظر (block) والإبلاغ (report) على منصات التواصل.
- كل منصة لديها آلية معينة للإبلاغ عن المحتوى المسيء أو المتنمرين.

4 تكلمي مع شخص تثقين فيه

- إذا كنت تشعرين بالأذى أو الضغط، احكي لشخص موثوق مثل أحد أفراد العائلة أو الصديقات المقربات الثقة أو مستشار نفسي.

5 أحتفظي بالأدلة

- احتفظي بالرسائل أو الصور أو أي محتوى فيه تنمر، لأنه ممكن تحتاجه إذا قررتي اتخاذ إجراء قانوني.



رابعًا: الملاحقة الإلكترونية (Cyberstalking)

- تعني تتبع حساباتها، أماكن تواجدها، أو محاولة الاتصال بها بشكل متكرر ومخيف.

كيف أحمي نفسي من الملاحقة الالكترونية؟

قوي إعدادات الخصوصية وممارسات الأمان

- غيّري إعدادات حساباتك لتكون "لأصدقائك فقط".
- اخفِي معلوماتك الشخصية مثل البريد،رقم الهاتف، الموقع، أو المدرسة/العمل.
- تأكدي من الحسابات التي تقومين بقبول صداقتها أو متابعتها.
- لا تقبلي طلبات صداقة من أشخاص غير معروفين.
- لا تتركي اجهزتك مفتوحًا بدون رقابة.
- تأكدي من عدم وجود تطبيقات تجسس أو برامج غير معروفة مثبتة.
- لا تضغطي على روابط مشبوهة حتى لو كانت من شخص تعرفه.
- لا تتفاعلي مع المتحرش
- لا تردي على الرسائل أو الاستفزازات.
- احتفظي بالرسائل، التعليقات، أو أي نشاط مشبوه.
- احظري الحسابات المزعجة من كل حساباتك.
- استخدم خاصية "الإبلاغ" على المنصة نفسها.



خامسًا: نشر الصور أو المعلومات الخاصة دون إذن (الانتقام الإباحي)

- تعني نشر صور خاصة بعد انتهاء علاقة بهدف الانتقام.

كيف أحمي نفسي من الانتقام الإباحي ؟

1 لا تشاركي صورًا خاصة واضحة أبدًا

- لا تشاركي صورًا خاصة واضحة أبدًا، حتى مع من تثقين بهم

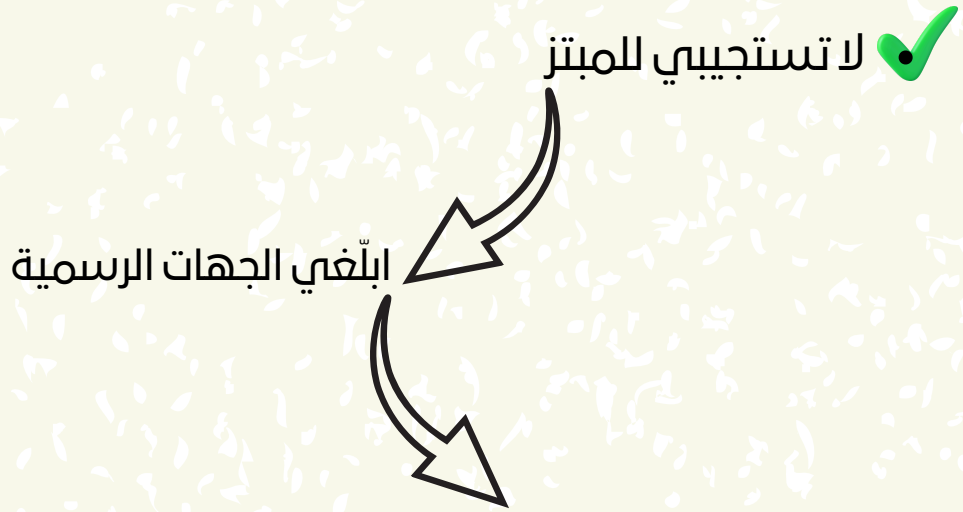
2 احذف الصور الحساسة من أجهزتك

- امسحيها من الهاتف، البريد، السحابة (cloud)، الرسائل، وأي مكان ممكن اختراقه أو تسريب البيانات منه.

3 استخدمي برامج تشفير وحماية

- احمِ هاتفك بكلمة مرور قوية.
- لا تخزن صورًا أو فيديوهات حساسة بدون حماية.

ماذا افعل اذا تعرضت لانتقام إباحي أو تهديد بنشر صور ؟



- قدّمي بلاغ للمنصات إزالة المحتوى أو الإبلاغ عن حساب المبتز، إذا تم نشر شيء على: فيسبوك، إنستغرام، تويتر، تيك توك... إلخ بالطريقة التي سنشرحها لاحقا، هذه المنصات تسمح لك بالإبلاغ عن محتوى حميمي نُشر بدون إذن ويتم حذفه بسرعة، مع ملاحظتك أنك قد تحتاجين هذه المواد كإثبات إذا رغبتي في اللجوء إلى الجهات الرسمية.

سادسًا: التحريض على العنف أو الكراهية

- تغريدات/تدوينات تدعو للعنف ضد النساء بسبب ملابسهن أو آرائهن

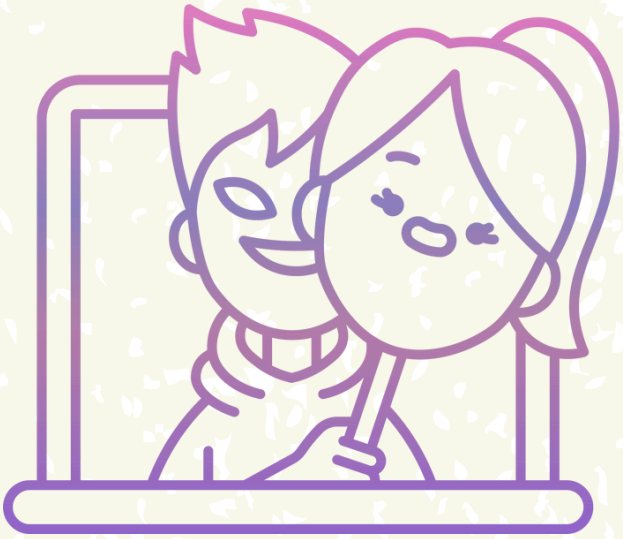
كيف أحمي نفسي من التحريض على العنف والكراهية ؟

- لا تتفاعل/ي مع صفحات أو حسابات تنشر كراهية، عنصرية، طائفية، أو دعوات للعنف.
- إذا تم إضافتك أو علمتي عن مجموعة تنشر محتوى محرض، اخرجي فورًا وبلّغي عنها.
- استخدمي منصات ذات أدوات إبلاغ فعالة.
- قد يحفز التفاعل على الرد ويشعل الموضوع أكثر أو يعرضك للخطر.
- التفاعل مع المحرضين غالبًا يغذيهم.
- استخدمي أدوات المنصات المختلفة للإبلاغ عن أي خطاب كراهية أو تحريض على العنف.
- احتفظي صور شاشة (screenshots) أو روابط المنشورات.



سابعًا: انتحال الشخصية:

- هو نوع من أنواع العنف أو الاحتيال الرقمي، ويقصد به أن يقوم شخص ما باستخدام هوية شخص آخر دون إذنه، بهدف خداع الآخرين، أو الإساءة للشخص المُنتَحل، أو تحقيق مكاسب شخصية.
- حيث ينشئ شخص حسابًا أو يتصرف وكأنه شخص آخر – سواء باستخدام اسمها، أو صورتها، أو معلوماتها الشخصية للإضرار بها.
- يمكن إستخدام انتحال الشخصية في أكثر من سيناريو للعنف ضد النساء مثل:



التشهير والإساءة للسمعة:

يقوم المعتدي بإنشاء حساب مزيف باسم المرأة أو استخدام صورها، وينشر محتوى مسيء لها:

- منشورات جنسية أو عنصرية
- شتائم أو مواقف سياسية لا تعبر عنها
- إشاعات كاذبة على مجموعات أو صفحات عامة

الابتزاز أو النصب:

ينتحل شخص هوية المرأة ويتواصل مع معارفها أو شركائها لجمع معلومات أو أموال:

- يطلب مالًا من أصدقائها أو عائلتها بادعاء أنها في "مشكلة"
- يستخدم حسابها المزيف لإرسال صور أو تهديدات

مكيدة قانونية:

ينشر محتوى مخالف للقانون باسمها (مثل تحريض أو محتوى غير أخلاقي)، مما قد:

- يعرضها للتحقيق أو ملاحقة قانونية
- يؤدي لفقدان عمل أو رفض طلبات عمل أو منحة

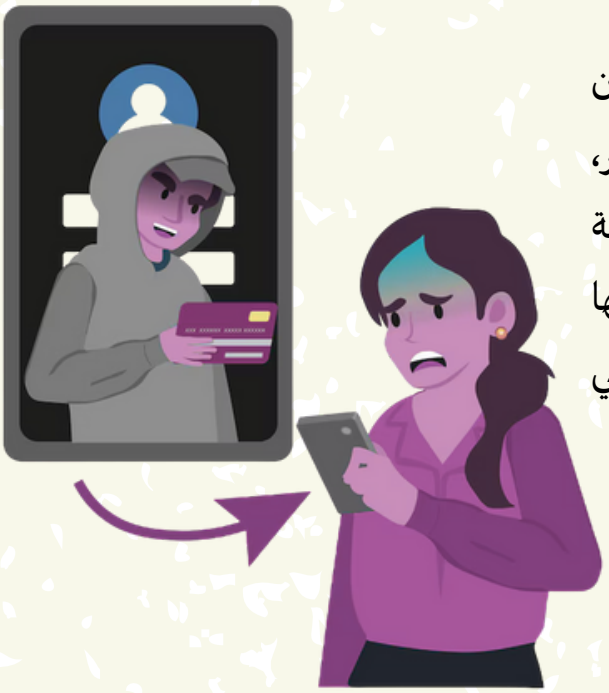
لتحرش بالآخرين باسم الضحية:

التحرش بالآخرين باسم الضحية: يتم استخدام حساب باسم المرأة للتحرش بنساء أخريات.

كيف أحمي نفسي من انتحال الشخصية ؟



ثامنًا: جمع وكشف البيانات الخاصة Doxing:



- من أبرز أدوات العنف الرقمي ضد النساء، وغالبًا ما يكون الخطوة الأولى قبل التحرش أو الابتزاز أو التشهير، ويتضمن تتبع، واستخراج، أو تجميع معلومات شخصية عن امرأة دون إذنها، ثم استخدام هذه البيانات لإيذائها أو تهديدها، وقد يتم كشفها علنًا أو تسريبها في مجموعات مغلقة.

ويمكن أن يستخدم في أكثر من سيناريو عنف ضد النساء:

التجسس والمراقبة

استخدام أدوات تتبع أو الوصول غير المصرح به لحسابات الضحية.
مراقبة نشاط الضحية اليومي (موقع، تفاعل، رسائل).

كشف الهوية الحقيقية

تتبع المرأة التي تستخدم اسماً مستعارًا للكشف عن بياناتها الحقيقية

نشر صور أو وثائق خاصة

صور شخصية، بطاقات هوية، رسائل، إيصالات، أو حتى محادثات خاصة تُنشر علنًا دون إذن.

مضايقتها عبر بيانات الاتصال:

مشاركة رقم هاتفها أو بريدها الإلكتروني أو عنوانها في منصات عامة، مما يؤدي إلى:

- تحرشات جماعية
- تهديدات بالقتل أو الاغتصاب
- اتصالات مزعجة

كيف احمي نفسي من ال Doxing (كشف البيانات الخاصة)؟

1. احمي بياناتك على وسائل التواصل:

- اجعلي حساباتك خاصة (Private)، خصوصًا إنستغرام وفيسبوك.
- لا تنشري معلومات حساسة مثل عنوان السكن أو رقم الهاتف أو المدرسة/الجامعة.
- تجنبي مشاركة صور توضح موقعك الجغرافي أو خلفية تُظهر مكانك

2. قلّلي من البيانات المتاحة عنك عبر البحث:

- ابحثي عن اسمك على جوجل، واكتشفي البيانات المتاحة عنك على الإنترنت.
- إذا وجدت معلومات حساسة، حاولي أن تطلبي إزالتها (من الموقع أو من جوجل مباشرة).

3. لا تستخدمي نفس الاسم أو الإيميل في كل المواقع:

- استخدمي إيميلات مختلفة للحسابات المهمة (مثل العمل أو الدراسة) وحسابات الترفيه.
- تجنّبي استخدام اسمك الحقيقي الكامل في كل مكان.

4. فعّلي المصادقة الثنائية (2FA):

حتى اذا تم تسريب بريدك أو رقمك، المصادقة الثنائية ستمنع دخول أي شخص لحساباتك بدون رمز تأكيد

5. احذري من روابط التصيد (Phishing) مثل روابط الهدايا المجانية أو إعلانات التطبيقات:

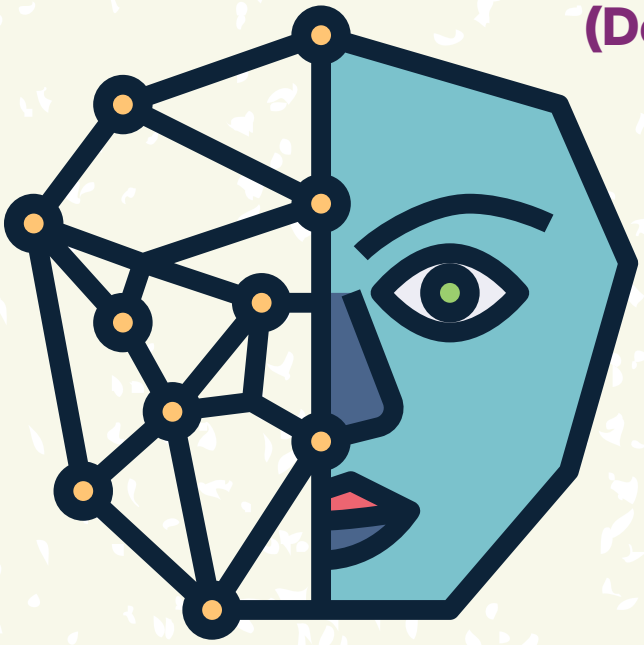
لا تضغطي على روابط مشبوهة أو من أشخاص غرباء.

بعض الجهات تستخدم روابط لخداعك وجمع معلومات عنك

6. احذري من الأشخاص الذين يحاولون تجميع معلومات بهدوء (لا تصدقي أنها أسئلة عادية للتعارف)

- يمكن لأحدهم الدردشة معك بهدف جمع معلومات: "أنتِ ساكنة فين؟"، "اسم مدرستك إيه؟"، "ابعتي صورة قديمة وانتِ في البيت؟"، "ابعتي صورتك وإنتي صغيرة".... إلخ.
- تلك طريقة شائعة في doxing، فكوني واعية لأي فضول زائد.


ماذا أفعل لو تعرضت لـ Doxing؟
1
سجلي كل الأدلة (سكرين شوت، روابط، رسائل).
2
أبلغي المنصة عن الحساب أو الشخص الذي قام بنشر بياناتك.
3
أغلقي أي حساب تم كشفه مؤقتًا أو غيّري بيانات الدخول.
4
تواصلي مع محامٍ أو جهة قانونية إذا تم تهديدك أو استخدام البيانات للإيذاء.
5
في مصر، يمكن التواصل مع مباحث الإنترنت لتقديم بلاغ رسمي



تاسعاً: التزييف العميق (Deepfake)

التزييف العميق (Deepfake) هو تقنية يُستخدم فيها الذكاء الاصطناعي (خاصة تقنيات التعلم العميق مثل **الشبكات التوليدية التنافسية - GANs**) لإنشاء صور أو فيديوهات أو تسجيلات صوتية مزيفة تبدو حقيقية تمامًا، ولكنها مُعدّلة أو مُصنعة بالكامل. يتم ذلك عن طريق استبدال وجه أو صوت شخص بآخر، أو حتى إنشاء شخصيات غير موجودة في الواقع.

التزييف العميق يمثل انتهاكًا خطيرًا للخصوصية والكرامة، ويجب التعامل معه كشكل من أشكال العنف الجندري الذي يتطلب استجابة عاجلة من الحكومات والمجتمعات التقنية.

كيف يُستخدم التزييف العميق كأداة للعنف الرقمي ضد النساء والفتيات؟

يُعد التزييف العميق أحد أخطر الأدوات التي يمكن استخدمها في أنواع متعددة من العنف الرقمي القائم على النوع الاجتماعي، حيث يُستغل بشكل خاص لمهاجمة النساء والفتيات عبر:

الانتقام الإباحي

- يتم إنشاء مقاطع فيديو إباحية مزيفة بوضع وجوه نساء أو فتيات على أجساد ممثلات إباحيات دون موافقتهن.
- يُنشر هذا المحتوى على مواقع إباحية أو وسائل التواصل الاجتماعي لتشويه سمعة الضحايا، ابتزازهن، أو إلحاق ضرر نفسي واجتماعي بهن.

هل يوجد حلول رقمية لإيقاف ذلك؟

نؤكد في البداية إنه في ظل تطور أدوات الذكاء الصناعي المختلفة، فإن كشف زيف المحتوى قد يتطلب قدرات تقنية متقدمة لا تمتلكها أغلب النساء، وننصح دائمًا باللجوء لآليات الإبلاغ والمساندة لتقديم الدعم اللازم، ونقترح هنا أدوات مجانية ومفتوحة المصدر قد تساعد في الكشف عن التزييف العميق (Deepfake) في الفيديوهات والصور، خاصةً تلك ذات المحتوى الإباحي الانتقامي المزيف (Non-Consensual Deepfake Pornography). هذه الأدوات تعتمد على خوارزميات الذكاء الاصطناعي ويمكن استخدامها لتحديد المحتوى المزيف:

Deepware AI Scanner

- **ما هو؟**

أداة مجانية على الإنترنت طورتها شركة Deepware للكشف عن مقاطع الفيديو المزيفة (Deepfake) باستخدام الذكاء الاصطناعي.

- **كيف يعمل؟**

يُحلل الفيديو المُرفق بحثًا عن علامات التلاعب، مثل:

1. عدم تناسق تعابير الوجه.
2. تشوهات في الإضاءة أو الظل.
3. أخطاء في دقة الحركات (مثل رمش العينين أو حركة الشفاه).
4. يُظهر نتيجة تحليله بنسبة احتمالية تشير إلى وجود تزييف.

- **مميزاته:**

يدعم العديد من الصيغ (مثل MP4, MOV).

سريع ولا يتطلب تسجيل دخول.

- **حدوده:**

قد لا يكتشف التزييف عالي الجودة.

لا يُقدم تفسيرًا تفصيليًا للنتيجة.

2. Illuminarty AI

- **ما هو؟**

منصة متقدمة تعتمد على الذكاء الاصطناعي لاكتشاف الصور والفيديوهات المُنشأة بالذكاء الاصطناعي (مثل تلك المُولدة بواسطة DALL·E، MidJourney، Stable Diffusion)، بالإضافة إلى تحليل النصوص.

- **مميزاته:**

يدعم تحليل الصور والنصوص.
واجهة بسيطة مع خيارات تحليل متعددة.

- **كيف يعمل؟**

يُحلل الصور/ النصوص ليكشف ما إذا كانت من إنتاج الذكاء الاصطناعي عبر:

1. فحص الأنماط غير الطبيعية في البكسل.
2. تحليل التوزيع اللوني والإضاءة.
3. يُقدم تقريرًا مفصلاً يبرز المناطق المشبوهة في الصورة.

- **حدوده:**

النسخة المجانية محدودة (قد تتطلب الاشتراك المدفوع لتحليل متقدم).
يركز أكثر على الصور المُنشأة بالذكاء الاصطناعي (مثل AI Art) وليس فيديوهات Deepfake.

3. Forensically

- **ما هو؟**

أداة ويب مجانية لتحليل الصور المُزيفة (مثل تلك المنشأة بـ **GANs**).

- **القيود:**

- يركز على الصور اكثر من الفيديوهات.

- **المميزات:**

- يكشف التلاعب في الصور عبر تحليل الضوضاء والتدرجات اللونية.
- لا يحتاج إلى تثبيت.

كيف تتعرفي على الفيديوهات/الصور المزيفة يدويًا؟

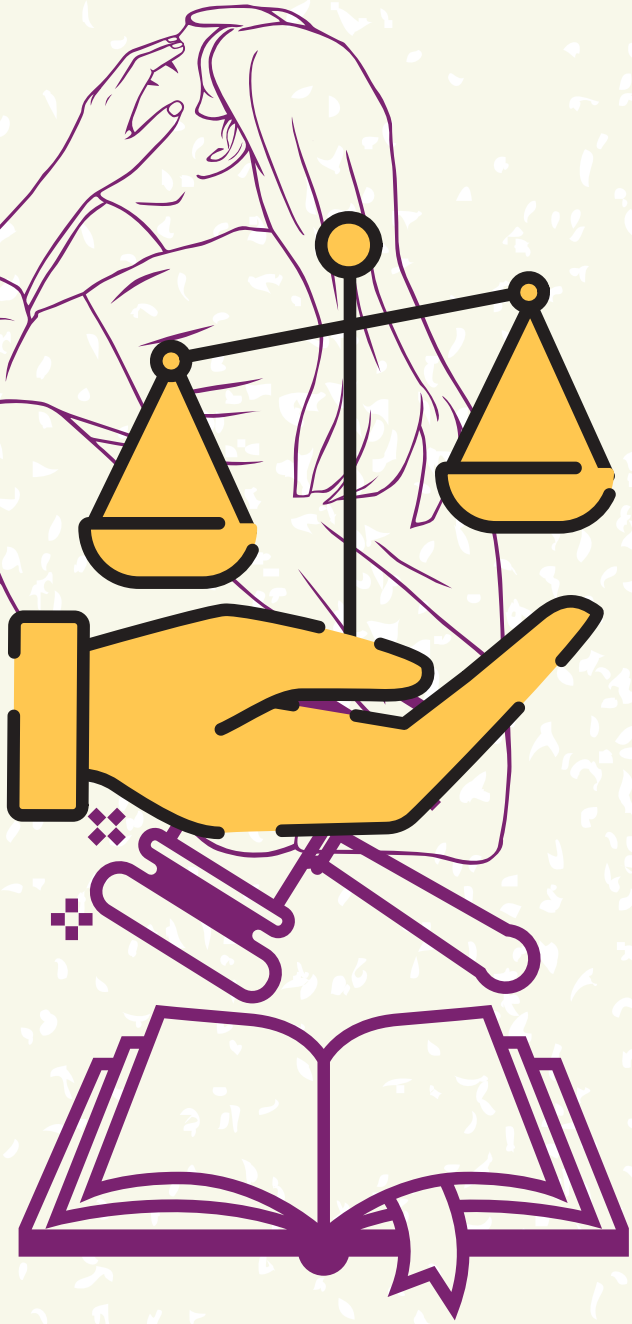
1. الوجه: انتبهي لعدم تناسق العينين، الحركة غير الطبيعية للشفاه.
2. الضوء/الظل: اختلافات غير منطقية في الإضاءة على الوجه مقارنة بالجسم.
3. الخلفية: تشوهات أو أجزاء مشوشة عند حواف الوجه.

إذا كنتِ ضحية لهذا النوع من العنف، تواصلي مع إحدى المنظمات المقترحة سابقًا للحصول على دعم قانوني ونفسي وتقني.

للحماية من العنف الرقمي، دائمًا وثقي المحتوى المشبوه عبر أدوات متعددة، واحفظي الأدلة للإبلاغ عنها على المنصات أو القانون.



التشريعات والقوانين المتعلقة بالعنف الرقمي:



تُعد التشريعات القانونية في مصر واحدة من الأدوات الأساسية لحماية النساء والفتيات في حالات العنف الرقمي الذي يتخذ أشكالًا متعددة كما سردنا، دفعت مجهودات المجموعات والمنظمات النسوية المختلفة الدولة إلى وضع قوانين تنظم الجرائم الإلكترونية وتوفير الحماية للأفراد على الإنترنت، مع التركيز بشكل خاص على حماية حقوق النساء ومكافحة العنف القائم على النوع الاجتماعي.

أبرز هذه التشريعات هو قانون مكافحة جرائم تقنية المعلومات (رقم 175 لسنة 2018)، الذي يعاقب على عدة أنواع من الجرائم الإلكترونية مثل التهديد، الابتزاز، والتشهير، ويشمل العنف الرقمي الموجه ضد النساء. إضافة إلى ذلك، فإن قانون العقوبات المصري يجرم التحرش والتهديد عبر الوسائل الإلكترونية، مما يوفر إطارًا قانونيًا لدعم النساء في مواجهة الاعتداءات الرقمية. وعلى الرغم من ذلك، لا تزال هناك حاجة لتطوير التشريعات وآليات الإبلاغ والشكوى لتواكب تطورات الجرائم الرقمية وبشكل يحافظ على سرية بيانات المبلغات، وتطوير إجراءات التقاضي خاصة في ظل التحديات التي يواجهها المجتمع في التصدي لهذه الأفعال وحماية النساء من آثارها النفسية والاجتماعية.

استراتيجيات الوقاية والدعم:

دعم الفتيات والنساء المعرضات للعنف الرقمي ودور الأسرة والأصدقاء

يُشكّل الدعم المجتمعي والأسري عاملًا أساسيًا في حماية النساء والفتيات من العنف الرقمي والحدّ من آثاره النفسية والاجتماعية. على الأسرة والأصدقاء أن يتبنّوا موقفًا داعمًا وغير مُدين، وأن يصغوا بتعاطف عند تعرض أي فتاة أو امرأة لانتهاك رقمي. يمكنهم استخدام دليل الحماية الرقمية كأداة عملية لفهم طبيعة العنف الرقمي، ومساعدة الضحية على توثيق الانتهاكات، وضبط إعدادات الأمان والخصوصية، والتبليغ للمنصات المعنية. من المهم أيضًا أن يُشجّع المحيطون النساء والفتيات على طلب الدعم القانوني أو النفسي عند الحاجة، وأن يعملوا على نشر الوعي الرقمي في دوائرهم الاجتماعية، مما يعزز بيئة أكثر أمانًا وتضامنًا في مواجهة هذا النوع من العنف.



خطوات
لدعم النساء والفتيات المعرضات للعنف الرقمي:

1. الاستماع بتعاطف دون لوم أو إدانة وتقديم الدعم النفسي الأولي ومراعاة مشاعر الضحية.
2. المساعدة في استخدام دليل الحماية الرقمية واتباع النصائح الواردة هنا لتأمين الحسابات، توثيق الانتهاكات، وضبط الخصوصية.
3. تشجيع الضحية على التبليغ وعدم الصمت إذا كان ذلك مناسبا لها سواء للمنصات الرقمية أو الجهات القانونية المختصة.
4. مرافقتها عند طلب الدعم القانوني أو النفسي لتقليل شعور الوحدة والتهديد.
5. نشر الوعي حول العنف الرقمي في الدائرة المحيطة عبر الحديث عنه، مشاركة مواد توعوية، أو تنظيم لقاءات صغيرة.
6. تفادي إعادة نشر أو تداول محتوى يتضمن عنفًا رقميًا ضد الضحية دون موافقتها وشرح العواقب حتى لو كان بهدف لفت الانتباه، قد يمثل ذلك عبئا إضافيا عليها
7. التحقق من المعلومات قبل تقديم النصائح لتجنّب توجيه الضحية نحو خطوات قد تزيد من الخطر الذي تتعرض له.





آليات الإبلاغ القانونية

يفضل دائما اللجوء لواحدة من المنظمات المعنية بالسلامة الرقمية للنساء والفتيات لتقديم الإرشاد اللازم حين يتعلق الأمر بجرائم العنف الرقمي، وحضور محامي/ة مختص/ة في هذا النوع من البلاغات لضمان استيفاء البلاغ والحصول على الدعم اللازم.

بشكل عام فإن آليات الإبلاغ القانونية التي يمكن للنساء والفتيات اللجوء إليها هي:

1. الإبلاغ عبر قسم الشرطة

يعد التوجه إلى أقرب قسم شرطة أحد الخيارات الرئيسية للإبلاغ عن جرائم العنف الرقمي. يمكن لأي شخص تعرض للعنف الرقمي التوجه للشرطة لتقديم بلاغ رسمي، سواء كان الأمر يتعلق بالتحرش، الابتزاز أو أي جريمة إلكترونية أخرى.

إجراءات الإبلاغ:

- الذهاب إلى أقرب قسم شرطة وتقديم بلاغ مكتوب أو شفوي.
- التوضيح للشرطة نوع الجريمة (مثل التحرش الإلكتروني، الابتزاز، أو التشهير).
- إرفاق الأدلة المتاحة مثل صور الشاشة، الرسائل النصية، أو الروابط التي تحتوي على المحتوى المضر.

2. الإبلاغ عبر الإدارة العامة لتكنولوجيا المعلومات (وزارة الداخلية)

تتولى الإدارة العامة لمكافحة جرائم المعلومات في وزارة الداخلية التعامل مع الجرائم الإلكترونية. يمكن للمواطنين تقديم بلاغات إلكترونية من خلال المنصة الخاصة بهذه الإدارة.

كيفية الإبلاغ:

- الاتصال بالخط الساخن على رقم 108
- التواصل عبر الموقع الالكتروني لوزراة الداخلية https://moi.gov.eg
- من خلال مقر الإدارة بالعباسية بجوار كلية الشرطة القديمة، أو من خلال مكتب مباحث الانترنت داخل كل مديرية امن في المحافظات.

- زيارة صفحة الإدارة العامة لتكنولوجيا المعلومات على فيسبوك أو الموقع الإلكتروني الخاص بالوزارة.
- الإبلاغ عن الجرائم عبر البريد الإلكتروني أو الأرقام الساخنة المخصصة لهذا الغرض. صفحة وزارة الداخلية – الجرائم الإلكترونية

3. الإبلاغ عبر النيابة العامة

تتخذ النيابة العامة دورًا كبيرًا في التحقيق في قضايا العنف الرقمي، خاصة إذا كانت الجريمة تشمل الابتزاز أو التشهير عبر الإنترنت. يمكن للضحايا تقديم بلاغات مباشرة إلى النيابة العامة عبر الإنترنت.

كيفية الإبلاغ:

- التقديم عبر الإنترنت: يمكن تقديم شكوى عبر الموقع الرسمي للنيابة العامة المصرية https://www.pp.gov.eg.
- الإبلاغ الشفوي أو المكتوب: يمكن الذهاب إلى النيابة العامة في المنطقة المحلية وتقديم البلاغ.

4. الإبلاغ عبر المجلس القومي للمرأة

يعد المجلس القومي للمرأة من الجهات الداعمة التي تقدم الدعم القانوني والنفسي للنساء والفتيات المتعرضات للعنف الرقمي. يوفر المجلس خطًا ساخنًا للإبلاغ عن العنف الرقمي ويقوم بالتنسيق مع الجهات المختصة مثل الشرطة والنيابة.

كيفية الإبلاغ:

- الاتصال بالخط الساخن 15115.
- التواصل عبر الموقع الإلكتروني للمجلس: www.ncw.gov.eg.
- يمكن تقديم الشكاوى بشكل سري وبدون الكشف عن هوية المبلغة.

ملاحظات هامة في حالة الإبلاغ القانوني:

خطوات الإبلاغ عن العنف الرقمي أو الابتزاز الإلكتروني:

- **توثيق الرسائل أو التعليقات المسيئة**
- التقاط صورة للشاشة (Screenshot) للرسالة أو التعليق، مع حفظ رابط حساب الشخص المعتدي أو رقم هاتفه إن وُجد.

- **عدم الرد أو نشر بيانات المعتدي**
- تجنّبي التفاعل مع الجاني أو فضحه على مواقع التواصل، حتى لا يؤثر ذلك على سير البلاغ أو يُستخدم ضدك أو ينبه المعتدي.

- **طباعة الأدلة**
- اطبعي صورة للشاشة (Screenshot) وروابط الحساب أو رقم الشخص المعتدي، وارفقي أي معلومات متوفرة عنه.

- **التوجه للإبلاغ شخصيًا**
- توجهي بنفسك إلى أقرب مديرية أمن في محافظتك، أو إلى مقر مباحث الإنترنت في العباسية (القاهرة).

- **الوثائق المطلوبة عند الإبلاغ**
- بطاقة الرقم القومي مع نسخة مصوّرة منها.
- قد يطلب منك فتح الحساب في حال وجود رسائل خاصة بالعنف الرقمي، تأكدي من تذكرك لإسم المستخدم وكلمة المرور (اليوزر والباسوورد).

5. الاستعانة بالمنظمات الحقوقية

هناك العديد من المنظمات الحقوقية في مصر التي تقدم الدعم القانوني والتقني والنفسي للنساء المعرضات للعنف الرقمي، في حال التعرّض لأي شكل من أشكال العنف الرقمي أو الابتزاز أو التهديد، يمكن التوجه إلى عدد من المبادرات والمؤسسات الموثوقة التي تقدم دعمًا قانونيًا أو نفسيًا أو توعويًا، منها:

1. مؤسسة إدراك للتنمية والمساواة – **Edraak Egypt**: مؤسسة نسوية تقدم محتوى توعويًا وداعمًا للنساء والفتيات حول قضايا العنف الرقمي والحقوق الرقمية.
   - وسائل التواصل:

   البريد الالكتروني: info@edraak-eg.org

   واتس آب: +201100703129

2. مؤسسة قضايا المرأة المصرية – **CEWLA**: تقدم دعمًا قانونيًا واستشارات للنساء المتضررات من العنف، ولديها خبرة طويلة في التعامل مع قضايا العنف الإلكتروني.

   البريد الإلكتروني: info@cewla.net

3. مبادرة اتكلمي – **Speak Up**: تعمل على توثيق حوادث العنف والتحرش، وتساعد الناجيات على الإبلاغ والحصول على الدعم الرقمي اللازم عبر إزالة المحتوى الخاص بالانتهاكات التي يتعرضن لها.
   - البريد الإلكتروني: helpline@speakupeg.com
   - لطلب إزالة محتوى عنف رقمي عبر مبادرة إتكلمي توجهي لهذا الرابط

4. مؤسسة جنوبية حرة – **Ganoubia Horra**: تدعم النساء في صعيد مصر، وتعمل على التوعية القانونية والاجتماعية بقضايا العنف ضد المرأة تقدم الدعم التقني والقانوني في حالات العنف الرقمي الموجه للنساء والفتيات.
   - البريد الالكتروني: Ganoubia.hora@gmail.com

5. مبادرة سوبر وومن – **Superwomen**: تركز على تمكين النساء ومشاركة قصص النجاة والمقاومة.
   - البريد الإلكتروني: superwomencontact3@gmail.com

6. براح آمن : مؤسسة نسوية تقاطعية تقدم الدعم الشامل للنساء.
   - البريد الإلكتروني: barahaamen@gmail.com

آليات الإبلاغ عن العنف الرقمي على منصات السوشيال ميديا المختلفة

إذا كنتي:

ترغبين في اللجوء لآليات التقاضي والعدالة يفضل أن لا تقومي بالإبلاغ عن المحتوى لتتمكني من استخدامه كدليل في عملية الإبلاغ والتقاضي.

في عصر السوشيال ميديا، أصبحت وسائل التواصل الاجتماعي أكثر من مجرد مكان للتفاعل الاجتماعي، بل أصبحت أيضًا ساحة رئيسية للعنف الرقمي، بما في ذلك التحرش، التشهير، والتهديدات. ولحماية المستخدمين، تتوفر آليات محددة للإبلاغ عن العنف الرقمي على مختلف المنصات. في حال لم تنجح محاولاتك في إزالة المحتوى عبر الخطوات المذكورة، يمكنك اللجوء لإحدى المنظمات المذكورة سابقا للمساعدة في إزالة المحتوى.

1. فيسبوك (Facebook)

<u>آلية الإبلاغ:</u>

- الإبلاغ عن منشور أو تعليق: يمكن للمستخدم الإبلاغ عن أي منشور أو تعليق يتضمن تحرشًا، تهديدًا، أو محتوى مسيئًا.
- طريقة الإبلاغ: اضغطي على النقاط الثلاث (•••) بجانب المنشور، ثم اختر "الإبلاغ عن المنشور" واختَر السبب المناسب.
- الإبلاغ عن حسابات مزيفة أو انتحال شخصية: يمكنك الإبلاغ عن الحسابات التي تنتحل شخصية مستخدم آخر أو تقوم بنشر محتوى مزعج.
- طريقة الإبلاغ: اضغطي على صورة الحساب أو اسمه، ثم اختر "إبلاغ عن الحساب".
- الإبلاغ عبر مركز المساعدة: Facebook Help Center

2. تويتر (Twitter)

آلية الإبلاغ:

- الإبلاغ عن التغريدات المسيئة: يمكن الإبلاغ عن التغريدات التي تحتوي على تحرش، تهديد، أو محتوى مسيء.
- طريقة الإبلاغ: اضغطي على السهم الموجه لأسفل بجانب التغريدة، ثم اختر "الإبلاغ عن التغريدة" وحدد السبب.
- الإبلاغ عن الحسابات المسيئة: يمكن الإبلاغ عن الحسابات التي تروج للعنف الرقمي أو تتعرض للنساء.
- طريقة الإبلاغ: اذهبي إلى صفحة الحساب، ثم اضغطي على النقاط الثلاث (•••) في أعلى الصفحة واختر "الإبلاغ عن الحساب".

إبلاغ عبر مركز الدعم: Twitter Help Center

3. إنستغرام (Instagram)

آلية الإبلاغ:

- الإبلاغ عن الصور أو الفيديوهات المسيئة: يمكنك الإبلاغ عن الصور أو الفيديوهات التي تحتوي على محتوى مسيء أو تهديدات.
- طريقة الإبلاغ: اضغطي على النقاط الثلاث (•••) في الزاوية العليا للمنشور، ثم اختر "الإبلاغ عن المنشور".
- الإبلاغ عن الحسابات أو التعليقات المسيئة: يمكن الإبلاغ عن الحسابات التي تروج للابتزاز أو التحرش.
- طريقة الإبلاغ: اضغطي على اسم الحساب أو تعليقه، ثم اختر "الإبلاغ عن الحساب" أو "الإبلاغ عن التعليق".
- إبلاغ عبر مركز الدعم: Instagram Help Center

4. تيك توك (TikTok)

آلية الإبلاغ:

- الإبلاغ عن مقاطع الفيديو المسيئة: يمكنك الإبلاغ عن أي فيديو يحتوي على تحرش أو تشهير.
- طريقة الإبلاغ: اضغطي على السهم الموجه لأسفل بجانب الفيديو، ثم اختر "الإبلاغ عن الفيديو".
- الإبلاغ عن الحسابات أو التعليقات المسيئة: يمكن الإبلاغ عن الحسابات أو التعليقات التي تحتوي على محتوى مسيء.
- طريقة الإبلاغ: اضغطي على صورة الحساب أو اسمه، ثم اختر "الإبلاغ عن الحساب".
- إبلاغ عبر مركز الدعم: TikTok Help Center

5. لينكدإن (LinkedIn)

آلية الإبلاغ:

- الإبلاغ عن المحتوى المسيء: يمكنك الإبلاغ عن المنشورات أو الرسائل المزعجة.
- طريقة الإبلاغ: اضغطي على النقاط الثلاث (•••) بجانب المنشور أو الرسالة، ثم اختر "الإبلاغ عن المحتوى".
- الإبلاغ عن الحسابات المزيفة أو المسيئة: يمكن الإبلاغ عن الحسابات التي تنتحل الشخصية أو تنشر محتوى مسيء
- طريقة الإبلاغ: اذهبي إلى صفحة الحساب، ثم اضغطي على النقاط الثلاث (•••) في أعلى الصفحة واختر "الإبلاغ عن الحساب".
- إبلاغ عبر مركز الدعم: LinkedIn Help Center

6. يوتيوب (YouTube)

آلية الإبلاغ:

- الإبلاغ عن الفيديوهات المسيئة: يمكنك الإبلاغ عن الفيديوهات التي تحتوي على محتوى عنيف أو مسيء.
- طريقة الإبلاغ: اضغطي على النقاط الثلاث بجانب الفيديو، ثم اختر "الإبلاغ عن الفيديو".
- الإبلاغ عن التعليقات المسيئة: يمكن الإبلاغ عن التعليقات المسيئة أو التي تحتوي على تهديدات.
- طريقة الإبلاغ: اضغطي على النقاط الثلاث بجانب التعليق واختر "الإبلاغ عن التعليق".
- إبلاغ عبر مركز الدعم: YouTube Help Center

نصائح للإبلاغ

احتفظي بالأدلة: احرصي على حفظ صور الشاشة (Screenshots) للمحتوى المسيء أو المخالف قبل الإبلاغ.

استخدمي الإبلاغ بسرية: معظم المنصات تقدم إمكانية الإبلاغ بشكل سري، بحيث لا يعرف الشخص الذي قمتِ بالإبلاغ عنه.

إطلبي الدعم القانوني: إذا كان العنف الرقمي يتضمن تهديدات أو ابتزازًا، يمكن اللجوء إلى الشرطة أو منظمات الدعم.

أهم ممارسات الحماية الرقمية

أولًا: الحماية الرقمية الأساسية

1. استخدام كلمات مرور قوية ومختلفة
2. تفعيل المصادقة الثنائية (**Two-Factor Authentication**)
3. تحديث البرامج بانتظام
4. تنصيب برامج الحماية من الفيروسات والتجسس
5. مراجعة صلاحيات التطبيقات على الهواتف
6. استخدام شبكة **VPN** لحماية اتصالك بالانترنت
7. تجنبي الروابط المشبوهة وفتح الملفات العشوائية ولا تدخلي بياناتك على أي رابط يصلك عبر تطبيقات التواصل أو المحادثة.

ثانيًا: إدارة الخصوصية على الإنترنت

1. ضبط إعدادات الخصوصية على وسائل التواصل الاجتماعي
   - تحديد من يمكنه رؤية منشوراتك ومعلوماتك الشخصية.
2. عدم مشاركة المعلومات الشخصية أو الصور الحساسة
   - حتى مع من تثقين بهم، خاصة عبر تطبيقات الدردشة غير المؤمنة.
3. تجنب استخدام الحسابات الرسمية أو الشخصية في التفاعل مع المسيئين
   - واستخدام حسابات بديلة عند الحاجة للتبليغ أو المواجهة.



توصيات ختامية
بشأن جرائم العنف الرقمي الموجه للنساء والفتيات:

1. الاعتراف بالعنف الرقمي كجريمة قائمة بذاتها

- الضغط لتعديل القوانين لتشمل صراحة جرائم مثل: الابتزاز الجنسي الإلكتروني، نشر الصور الخاصة دون إذن، المراقبة الرقمية، والتحرش الإلكتروني.
- التعامل مع العنف الرقمي كامتداد للعنف القائم على النوع الاجتماعي.

2. تبني منهج يراعي النوع الاجتماعي في إنفاذ القانون

- تدريب الشرطة والجهات القضائية على التعامل الحساس والفعال مع بلاغات العنف الرقمي ضد النساء.
- ضمان عدم إعادة إيذاء الناجيات أثناء التحقيق أو المحاكمة.
- ضمان سرية بيانات المبلغات لحمايتهن من ردود الفعل الانتقامية.

3. حماية الخصوصية الرقمية للنساء والفتيات

- الضغط على المنصات الرقمية لتعزيز سياسات الحماية والخصوصية، وتوفير أدوات أكثر فاعلية للنساء للتحكم في بياناتهن ومحتواهن.
- تشجيع تطوير منصات إبلاغ باللغة العربية يسهل الوصول إليها.

4. توفير الدعم الشامل للناجيات

- إنشاء مراكز دعم للناجيات من العنف الرقمي خاصة في المناطق المهمشة.

5. التوعية المجتمعية والتثقيف الرقمي

- تنفيذ حملات توعوية حول العنف الرقمي وآثاره وكيفية مواجهته.
- إدماج التربية الرقمية والوعي بالحقوق في المدارس والجامعات.

6. رفض لوم الضحية ومناهضة السرديات الذكورية

- مواجهة الثقافة المجتمعية التي تُحمّل النساء مسؤولية الانتهاك.
- التأكيد على أن المسؤولية تقع على المُعتدي لا على الضحية.

7. تمكين النساء من أدوات الحماية الرقمية

- توفير أدلة ومصادر تدريبية على الأمان الرقمي بلغات مبسطة ومجانية.

توصيات بالإجراءات العاجلة للجهات القضائية والمشرّع في قضايا العنف الرقمي الموجه النساء والفتيات في مصر:

أولًا: للنيابة العامة وجهات التحقيق

1. التعامل الجاد والسريع مع بلاغات العنف الرقمي واعتبار العنف الرقمي جريمة تمس السلامة الجسدية والنفسية، وليس مجرد "خلاف إلكتروني".
2. توفير بيئة آمنة أثناء التحقيق مع الضحايا وضمان الخصوصية، ومنع أي شكل من أشكال التمييز أو اللوم أثناء الاستماع لأقوال النساء أو الفتيات.
3. تفعيل وحدات متخصصة في الجرائم الإلكترونية ذات الطابع الجندري وتدريب الكوادر على التعامل مع قضايا الانتهاك الرقمي ضد النساء من منظور حقوقي ونفسي.
4. طلب الفحص الفني السريع للأجهزة الإلكترونية والتنسيق مع جهات تقنية مختصة لضمان الحفاظ على الأدلة الرقمية.

ثانيًا: للجهات القضائية

1. تسريع الفصل في قضايا العنف الرقمي ضد النساء والفتيات لتقليل الضرر النفسي والاجتماعي، ومنع إفلات الجناة من العقاب.
2. إصدار أحكام تضمن الردع وتراعي الأثر المعنوي على الضحية وعدم الاكتفاء بالغرامات المالية الرمزية في قضايا الابتزاز، التشهير، أو اختراق الخصوصية.
3. السماح للضحايا باستخدام الأسماء المستعارة أثناء المحاكمات خاصة في الحالات التي تمس السمعة أو تتعلق ببيانات حساسة.

ثالثًا: للمشرّع والبرلمان المصري

1. تحديث وتوسيع قانون مكافحة جرائم تقنية المعلومات (القانون رقم 175 لسنة 2018) بإضافة تعريفات واضحة للعنف الرقمي، مثل: الابتزاز الجنسي الإلكتروني، التهديد بالنشر، الملاحقة الرقمية، والتنمر الإلكتروني.
2. إصدار قانون خاص بحماية النساء والفتيات من العنف الرقمي بالاستناد إلى اتفاقية "سيداو" والمعايير الدولية لحقوق الإنسان.
3. إنشاء آلية وطنية للتبليغ والحماية السريعة تتيح للنساء والفتيات الإبلاغ إلكترونيًا وامكانية تجهيل هوية الضحية وتلقي الدعم القانوني والنفسي الفوري.

Edraak
Foundation
For development and equality

www.edraak-eg.org

info@edraak-eg.org

edraakEgypt

edraakEgypt

edraak_egypt

edraak-eg