الابتزاز الإلكتروني

ما هو الابتزاز الإلكتروني؟

الابتزاز الإلكتروني هو سلوك إجرامي يعتمد على التهديد والسيطرة النفسية، حيث يقوم المعتدي باستغلال محتوى خاص أو معلومات شخصية تعود للضحية، ويستخدمها كورقة ضغط لإجبارها على القيام بأفعال لا ترغب بها. هذا النوع من العنف لا يرتبط فقط بالمحتوى الجنسي، بل يشمل أي مادة يمكن أن تُستخدم للإحراج أو التخويف أو الإضرار بالسمعة.

السياق الذي يحدث فيه الابتزاز:

يحدث الابتزاز غالباً في بيئات رقمية يفترض فيها الأمان، مثل المحادثات الخاصة أو العلاقات التي تبدأ بدافع الصداقة أو الدعم العاطفي. في كثير من الحالات، لا يكون المعتدي غريبًا تمامًا، بل شخصًا بنى علاقة ثقة مع الضحية قبل أن يتحول إلى مصدر تهديد.

الأساليب النفسية التي يستخدمها المبتز:

يعتمد المبتز على إثارة الخوف والشعور بالذنب والضغط الزمني. قد يوهم الضحية بأن الاستجابة ستُنهي المشكلة، أو بأن الصمت سيحميها، بينما الهدف الحقيقي هو إحكام السيطرة وإطالة أمد الابتزاز.

الأثر طويل الأمد على الضحية:

الابتزاز لا ينتهي بانتهاء التهديد، بل يترك أثراً نفسياً عميقاً، مثل فقدان الشعور بالأمان، القلق المستمر، وصعوبة الثقة بالآخرين أو بالفضاء الرقمي عموماً.

الابتزاز الإلكتروني – كيف يعمل ولماذا هو خطير جداً؟

الابتزاز الإلكتروني يعتمد على دائرة خوف متصاعدة. يبدأ المبتز غالباً برسالة واحدة تحمل تهديداً مبهماً، ثم ينتقل إلى طلب صغير لا يبدو خطيراً، ليختبر قابلية الضحية للاستجابة، عند أي استجابة، تتوسع المطالب وتتحول السيطرة إلى نمط دائم.

خطورة الابتزاز لا تكمن فقط في نشر المحتوى، بل في الاستنزاف النفسي المستمر، وفقدان الإحساس بالأمان، وتحويل حياة الضحية إلى حالة ترقّب دائم. في السياق المحلي، تُستغل الوصمة الاجتماعية ومفهوم "السمعة" كأداة ضغط رئيسية، ما يجعل كثيراً من الضحايا يلتزمن الصمت رغم الأذى.

أنواع الابتزاز الإلكتروني:

- **ابتزاز جنسي (Sextortion):** باستخدام صور أو فيديوهات خاصة.
- **ابتزاز عاطفي:** استغلال المشاعر للسيطرة النفسية.
- **ابتزاز مالي:** تهديد مباشر مقابل المال.
- **ابتزاز مهني:** التهديد بتشويه السمعة المهنية أو فقدان العمل.

كيف يحدث الابتزاز؟

- بناء علاقة وهمية عبر وسائل التواصل يظهر المبتز كشخص داعم أو مهتم عاطفياً.
- ثم ينتقل إلى جمع المعلومات أو المحتوى الحساس واختراق حسابات أو سرقة صور ومحادثات.
- استخدام محتوى مفبرك أو معدل (وأحياناً ديب فيك).
- التهديد المتدرّج، حيث تبدأ المطالب بسيطة ثم تتصاعد.

أخطاء شائعة يجب تجنبها:

- الاستجابة لمطالب المبتز.
- حذف الأدلة بدافع الخوف.
- مواجهة المبتز وحدك أو تهديده.

ماذا تفعل إذا تعرضت للابتزاز؟

1. لا تتجاوب مع المبتز ولا ترسل أموالاً.
2. احفظ الأدلة فوراً (صور شاشة، روابط، تواريخ، عناوين حسابات، سجلات محادثات). استخدم جهازاً آمناً للحفظ.

3. غيّر كلمات المرور وفعّل المصادقة الثنائية على جميع الحسابات.
4. احظر الحسابات المسيئة وبلّغ عنها داخل المنصة.
5. الإبلاغ للجهات الرسمية (وحدة الجرائم الإلكترونية/النيابة العامة) وفق الإجراءات المتاحة في بلدك.
6. حماية فورية للأجهزة: فحص برمجيات خبيثة، إلغاء جلسات تسجيل الدخول المفتوحة، مراجعة تطبيقات لديها صلاحيات زائدة، فصل النسخ الاحتياطية غير الآمنة.
7. اطلب دعماً متخصصاً:
    - دعم نفسي واجتماعي (خطوط ساخنة/منظمات محلية).
    - دعم قانوني (محامٍ، مؤسسات مسانِدة).
    - دعم تقني (خبير أمان رقمي/منصات مساعدة).

التأثيرات على الضحية:

الابتزاز يخلق حالة خوف دائم، توتر نفسي، شعور بالعجز، وقد يدفع الضحية للعزلة أو الانسحاب من المجتمع الرقمي، وأحياناً الواقعي.

كيف نمنع التعرض مستقبلاً؟

- كلمات مرور قوية وفريدة لكل خدمة، مع مدير كلمات مرور موثوق.
- المصادقة الثنائية (2FA) دائماً (تطبيق رموز أو مفاتيح أمان).
- ضبط إعدادات الخصوصية في المنصات وحصر الظهور للجمهور المناسب.
- عدم فتح الروابط المجهولة أو تنزيل مرفقات غير متوقعة.
- تحديثات دورية للنظام والتطبيقات والمضادّات.
- مراجعة صلاحيات التطبيقات على الهاتف (الكاميرا/المايك/الموقع).
- تقليل البصمة الرقمية: تجنّب مشاركة بيانات حساسة أو صور خاصة عبر أجهزة متصلة.

❖ كسر الصمت يضعف الابتزاز

الابتزاز يعتمد على الخوف والصمت، لكنه يفقد قوته حين يتم كسره بالوعي والدعم. لا تستجيبي لطلبات المبتز مهما بدأ التهديد مخيفاً، فالتوثيق، وحماية الحسابات، وطلب المساعدة المبكرة خطوات أساسية تحمي الضحية، تقلّل من الأذى، وتحدّ من توسّع الضرر.