كيف تحمي نفسك

- لا تستجب للتهديدات: لا تدفع أي فدية أو تستجب للمطالب.
- قم بتغيير كلمات المرور الخاصة بك: وقم بتفعيل المصادقة الثنائية لجميع حساباتك.
- تجنّب نشر بيانات ومعلومات مهمة أو شخصية على وسائل التواصل الاجتماعي.
- احذر من النقر على الروابط المشبوهة: أو تحميل الملفات من مصادر غير موثوقة.
- لاتحتفظ الاحتفاظ بأي مقاطع فيديو أو صور خاصة على الهاتف المحمول أو أجهزة الحاسوب.
- استخدم برامج مكافحة الفيروسات: وقم بتحديثها بانتظام.
- قم بتوثيق كل شيء: احفظ جميع الأدلة على الابتزاز، مثل الرسائل والتهديدات.
- قم بعمل نسخ احتياطي لبياناتك بانتظام:** لحماية نفسك من فقدان البيانات.
- أمتنع عن التواصل مع المُبتز نهائيًا واطلب من أصدقائك ومعارفك الشيء نفسه إذا حاول الوصول إليهم لترويعك.
- أغلق جميع الحسابات الخاصة بك على وسائل التواصل الاجتماعي بشكل مؤقت لسد طريق الوصول إليك أمام المُبتز.

توثيق وإثبات الجريمة

- جمع كل المستندات والأدلة التي قد تثبت صحة الدعوى والتي يمكن أن تكون تهديدات مكتوبة أو شفهية أو مرئية. التوجه إلى الإدارة المختصة في الدولة وتقديم الأدلة.
- جلب الشهود للإدلاء بشهاداتهم أو تسجيلات الكاميرا
- والصور والتسجيلات الصوتية ورسائل SMS والبريد الإلكتروني.

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

+218 21 361 4115
+218 21 361 4127
+218 21 361 4177
info@nissa.gov.ly
www.nissa.gov.ly
www.cert.gov.ly



الابتزاز الالكتروني

الابتزاز الإلكتروني

ماهو؟

هو جريمة إلكترونية يحاول عبرها المجرم الحصول على مكسب ما من الضحية (أفراداً أو مؤسسات) عبر الإكراه والتهديد. ويتم عادةً عن طريق:

- التهديد بنشر بيانات خاصة وحساسة قد تُلحق ضرراً بسمعة ومكانة الضحية.
- التهديد عبر سرقة الحسابات الالكترونية مثل البريد الإلكتروني أو مواقع التواصل الاجتماعي وصفحات الانترنت.
- التهديد عبر إلحاق الضرر وتشفير الملفات على الأجهزة الالكترونية سواءً كانت حواسيب أو أجهزة محمولة.



أنواعه

الابتزاز المادي

تهديد الضحية بنشر محتوى خاص وحساس مثل الصور والمرئيات والصوتيات أو نشر معلومات حساسة عنه والمطالبة بمبالغ مالية أو تحويلات مصرفية مقابل عدم نشرها والتزام الصمت.

الابتزاز الغير أخلاقي

تهديد الضحية بهدف الحصول على محتوى فاضح وفي أسوأ الحالات أن تقدم له خدمات غير أخلاقية على أرض الواقع بعد رضوخها ووقوعها في شباك المجرم.

الابتزاز النفعي

تهديد الضحية بعد الحصول على محتوى خاص وحساس لها مقابل الحصول على خدمات أو مصالح معينة، هذه الفئة من الابتزازات تختص دائمًا بالشخصيات العامة والأفراد الذين يشغلون مراكز سياسية أو مراكز حكومية وأيضًا الإعلاميين والمؤثرين أو الشخصيات البارزة.

ضحايا الابتزاز الإلكتروني

النساء والفتيات

وهم من أكثر ضحايا جرائم الابتزاز الإلكتروني معاناة، لأنهم الأكثر عاطفيةً ورضوخاً للتهديد والأكثر ملاءمةً لمطالب المجرمين الجنسية عبر الإنترنت، في كثير من الحالات يبتز المجرمون امرأة متزوجة بالصور ويهددونها بإرسالها إلى زوجها وعائلته إذا لم تستجب لمضايقاتهم الجنسية أو يبتزونها لتحويل مبالغ معينة من المال إليهم، أو أن تُقنع أحد أقاربها بفعل غير قانوني يلبي طلباتهم.



الأطفال والمراهقين



قد يتعرض الأطفال أيضًا للابتزاز الإلكتروني المادي إما من خلال مواقع التواصل الاجتماعي أو من خلال الألعاب التي يستخدمونها.

الرجال والأولاد

لا يقتصر ضحايا الابتزاز الإلكتروني على النساء والأطفال والمراهقين؛ إنما يقع الرجال أيضاً ضحايا للابتزاز وخصوصاً من يرجى من وراءه المصلحة.

الشركات والمؤسسات

على وجه الخصوص، الشركات الكبرى والمؤسسات الوطنية تعتبر من أكبر ضحايا الابتزاز الإلكتروني، ويركز غالب المجرمون هجماتهم عليها للحصول على بياناتها الخاصة وتشفيرها أو تهديدهم بتسريبها وفي أحيانٍ كثيرة يتم عرض البيانات المسربة في السوق السوداء للمزايدة عليها ولوضع كثير من الضغط على المؤسسة المتضررة ودفعها للتفاوض أو دفع قيمة الفدية.

