**جريمة الأبتزاز الالكتروني وكيفية التعامل معها والتصدي لها**

منذ أن دخلت وسائل التواصل الاجتماعي إلى البلاد واصبح التواصل متاح على نطاق واسع بين الافراد مما آدى الى انتشار جرائم الابتزاز الإلكتروني بشكل واسع وتطوّرت مع مرور الوقت وخرجت منها عصابات منظمة، حيث يمكن لهذه العصابات ان تنتشر بصورة متزايدة وتتمادى في عملها في حالة ضعف تطبيق القانون الرادع لهم والتعامل غير الحازم مع هذه القضايا وعدم إيجاد تشريعات قانونية مجدية وحديثة مع التطور التكنولوجي الحاصل، وإضافة إلى ضعف القانون، يرى مختصون أن انتشار البطالة والفقر وعدم الاستقرار قد ساعد على ارتكاب مثل هذه الجرائم، إذ أن ما يحدث من جرائم في كل المجالات، هو تعبير جلي عن الواقع السياسي بالبلاد الذي يشهد تراجعًا في القضاء على البطالة وتقديم الخدمات والتنمية وفرص العمل، ودائمًا ما يعتبر الابتزاز الإلكتروني هو مصدر لجني الأموال من الضحية أو محاولة لملئ الفراغ الذي يمر به الشباب.

لذا فأن أستمرار التكنولوجيا في التقدم بسرعة، وغياب تكبيق بعض القوانين الرادعه ادى الى انتشار الأشكال المختلفة للجريمة عبر الإنترنت من بينها جريمة الابتزاز الإلكتروني، والتي الغاية من ارتكابها هي المطالبة بالمال أو المعلومات أو المكاسب الأخرى من الأشخاص اوالشركات من خلال [التهديد](https://www.simaetbhatha.com/hc/ar/articles/5350806551319-%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF-%D8%A8%D8%AD%D8%B3%D8%A8-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82%D9%8A-) بنشر أمور خاصة أو مخزية وبيانات سرية على وسائل التواصل الاجتماعي وبالتالي تتعرض حياة الفرد للخطر..

فالابتزاز الإلكتروني: عملية تهديد وترهيب للضحية بنشر صور أو مقاطع فيديو أو تسريب معلومات سرية خاصة بالنسبة للضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل او اجبار الضحية على عمل فعل غير مشروع أو غيرها من الأعمال غير القانونية..

وعادة ما يتم تصيد الضحايا عن طريق برامج التواصل الاجتماعي او البريد الإلكتروني نظرًا لانتشارهم الواسع واستخدامهم الكبير من قبل جميع فئات المجتمع..

ولا ننسى بأن جريمة الأبتزاز الالكتروني يمكن أن يحدث أيضًا عندما يرسل الضحايا أنفسهم (بالتراضي) بحسن النية صورهم ومقاطع الفيديو الخاصة بهم إلى الآخرين بسبب منح الثقة الزائدة في المقابل (بما في ذلك الأصدقاء أو الشركاء الحميمون)، والذين بدورهم يضمرون سوء النية ويستخدمون المحتوى لغرض [تهديد](https://www.simaetbhatha.com/hc/ar/articles/5350806551319-%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF-%D8%A8%D8%AD%D8%B3%D8%A8-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82%D9%8A-) الضحية والحصول على شيء ما بالقوة في المقابل..

فالطريقة التي تبدأ بها عملية الأبتزازغالبًا تبدأ العملية عن طريق إقامة علاقة صداقة مع الشخص المستهدف، او اي نوع اخر من العلاقات ثم يتم الانتقال إلى مرحلة التواصل عن طريق برامج المحادثات المرئية (مكالمات الفيديو)،او المحادثات الكتابية ليقوم بعد ذلك المبتز باستدراج الضحية وتسجيل المحادثة او اخذ لقطات شاشة لها والتي تحتوي على محتوى مسيء وفاضح للضحية،او امور اخرى ثم يقوم أخيراً بتهديده وابتزازه بطلب تحويل مبالغ مالية أو تسريب معلومات سرية، وقد تصل درجة الابتزاز في بعض الحالات إلى إسناد أوامر مخلة بالشرف والأعراف والتقاليد مستغلاً بذلك استسلام الضحية وجهلة بالأساليب المتبعة للتعامل مع مثل هذه الحالات.

لذا في حالة التعرض للأبتزاز الالكتروني يجب عدم التواصل مع الشخص المبتز، حتى عند التعرض للضغوطات الشديدة من قبله وعدم تحويل أي مبالغ مالية، أو الإفصاح عن رقم البطاقة البنكية الخاصة وكذلك عدم التجاوب معه والافصاح عن معلومات سرية خاصة وتجنب المشادات مع المبتز وعدم تهديده بالشرطة، وقم بالإبلاغ بصورة سرؤة عن المبتز عند وقوع الحادثة مباشرة لدى الجهات المختصة..

قم بتخزين المحتوى الذي تم إبتزازك به، أو أي محتوى شخصي وحساس آخر، في مكان آمن ومضمون لا يمكن الوصول إليه أو اختراقه. لا تحذف المحتوى ولا رسائل [التهديد](https://www.simaetbhatha.com/hc/ar/articles/5350806551319-%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF-%D8%A8%D8%AD%D8%B3%D8%A8-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82%D9%8A-)، إذ أن حذف الأدلة التي يمكن استخدامها لإدانة المجرمين وبحذف الإدلة تسمح لهم بأن يكونوا المالك الوحيد للمحتوى.

هناك تساؤلات عديدة حول لماذا يرتكب المجرمين جريمة الإبتزاز الإلكتروني؟

فالجواب يمكن أن يكون الدافع وراء مرتكبي الابتزاز والتهديد الالكتروني مجموعة متنوعة من العوامل بشكل عام ، قد تكون الدوافع مادية أو مالية أو نفسية أو عاطفية. قد لا يعرف المجرم بالضرورة الضحية التي يستهدفها وقد لا يكون على دراية بتأثير الجريمة على حياتهم غالبًا ما يكون الهدف في هذه الحالات مرتبطًا بالحصول على منفعة مالية من الضحية، ولكن يمكن أن يتضمن أيضًا دافعًا لإلحاق ضرر نفسي في الحالات التي يعرف فيها المجرم الضحية شخصيًا، يمكن أيضًا أن يكون الدافع هو المكاسب المالية وكذلك الرغبة في التسبب في ضرر نفسي للضحية، غالبًا للانتقام إذا رفضت الضحية أن تقدم للمجرم مطلباً أو قطعت علاقتها مع المجرم.

كل حالة فريدة من نوعها ويجب أن تعامل على هذا النحو من قبل تنفيذ القانون. الموضوع المشترك بين جميع حالات الابتزاز الإلكتروني هو الآثار السلبية للجريمة على الضحايا، والتي يمكن أن تكون طويلة الأمد. يمكن أن يؤدي هذا النوع من الجرائم إلى ضرر كبير بما في ذلك الأذى النفسي طويل الأمد والانتحار وبالضافة الى ان هذا الضرر الواقع على الضحية قد يمتد و يلحق باماكن تعليمه وآفاقه المهنية والاستقرار المالي..

لذا نظراً لما سبق فيمكن لاي فرد ان يحمي نفسة من الابتزاز ويتجنبه وذلك باتباع هذه النصائح المهمة :

١-تجنب قبول طلب الصداقة من قبل أشخاص غير معروفين.

٢\_ عدم الرد والتجاوب على أي محادثة ترد من مصدر غير معروف.

٣\_ تجنب مشاركة معلوماتك الشخصية حتى مع أصدقائك في فضاء الإنترنت .

٤\_ ارفض طلبات إقامة محادثات الفيديو مع أي شخص، ما لم تكن تربطك به صلة وثيقة.

٥\_ تجنب ان يتم جذب انتباهك للصور الجميلة والمغرية، وتأكد من شخصية المرسل.

٦\_ تجنب الرد على شخص غير معروف حتى لو تعرضت للتعديد لا تحاول إقناعه بعدم نشر صورك. قد يقوده ذلك إلى الاعتقاد بأنك ضعيف أو مستجيب لمطالبهم، مما قد يدفعهم إلى زيادة مطالبهم أو التحقق من اهميتها لديك

٧\_ تأمين الجهاز الإلكتروني الخاص بك سواء كان جهاز كمبيوتر أو هاتفًا ذكيًا، وعدم استخدام التطبيقات والروابط غير الموثوق بها او المرسلة لك خلال المحادثات الكتابية عن طريق التواصل الاجتماعي

٨\_الامتناع او تجنب نشر بيانات ومعلومات مهمة أو شخصية عنك على وسائل التواصل الاجتماعي

٩\_ عدم الاحتفاظ بأي مقاطع فيديو أو صور خاصة على الهاتف المحمول، بسبب خطر التعرض للسرقة وحفظها على قرص صلب خارجي يتم حفظه في مكان آمن.

١٠\_ اختيار كلمات مرور قوية لحساباتكم على مواقع التواصل الاجتماعي، وهي كلمات يصعب على المخترق تخمينها، بحيث تكون بعيدة عن اسمائكم وتاريخ ميلادكم.

١١\_ في حالة بيع هاتفكم الخاص، فلا تكتفوا بمسح الصور وأرقام الهواتف، وأنما يجب تسجيل الخروج من جميع حساباتكم على هاتفكم المحمول المراد بيعة وعمل فورمات ومن ثم بعدها يتم تشغيل الجهاز، ومن ثم تشغيل كاميرا الفيديو وترك الهاتف في غرفة مظلمة، ويبقى التسجيل مفتوح حتى تمتلئ ذاكرة الهاتف الداخلية بالكامل، وفي ذلك الوقت سيقوم الهاتف بإيقاف تشغيل الكاميرا تلقائيًا، ثم يتم حذف الفيديو الاخير ، ففي هذه الحالة يتم التأكد من أن أي شخص لا يستطيع استعادة محتويات الكاميرا سيجد هذا الفيديو المظلم فقط .

ففي هذا المقال، تم تزودكم ببعض النصائح و المعلومات الأساسية حول هذه الجريمة وهي جريمة الابتزاز الالكتروني وكيفية التعامل معها للتصدي .