جامعة الانبار

كلية التربية العلوم الصرفة

شعبة ضمان الجودة

الابتزاز الالكتروني

اعداد

الاستاذ المساعد سميرة عدنان

مسؤولة وحدة الارشاد التربوي والتوجيه النفسي

الابتزاز لعبة من تعفنت روحه

ما هو الابتزاز الالكتروني

هي جريمة إلكترونية يقوم فيها شخص بالاحتفاظ بملفات إلكترونية خاصة بك كرهينة بنيّة الحصول على مقابل مالي أو تنفيذ طلب معين سوآءا أكان هذا الطلب أخلاقي أو غير أخلاقي، والابتزاز الإلكتروني يتضمن الشخص الذي يبتز ويسمى بذلك "مبتز"، والذي وقعت عليه عملية الابتزاز ويدعى الضحية، والمقابل المادي أو المعنوي وأخيرًا طريقة الابتزاز.

أهم أسباب الابتزاز الالكتروني

يمكن أن يحدث الابتزاز الالكتروني نتيجة قلة الوعي بالأمن الالكتروني، حيث تجد أن أكثر الضحايا ممن لا يعرفون الكثير عن التقنية وعن تفادي هذه الظاهرة، وكيف يتصرفون في حال وقعوا فيها، إذن فالسبب الرئيسي لوقوع الضحايا في هذه المصيدة هي قلة الوعي الأمني .

أيضا هناك أسباب أخرى وهي:

١. تكوين علاقات مجهولة بالنسبة للبنت، لأن بعض البنات قد تدخل في علاقة مع شخص ما، فيشرع بالتقاط صور لها على حين غفلة منها، بعد ذلك يبدأ مسلسل الابتزاز وذلك بطلب أشياء أخرى مقابل أن لا يخبر أهلها بأنها قابلته.

٢- اختراق حسابات التواصل الاجتماعي بأنواعها وبالتالي امتلاك المبتز لعدد من المحادثات الخاصة.
٣- إرسال الصور إلى شخص غير موثوق، وهذا يحدث غالبًا بهدف التعارف الالكتروني، على مواقع التواصل الاجتماعي.
٤- عدم التأكد من محو المعلومات والملفات قبل الشروع في بيع الجهاز سوآءا أكان هاتف أو حاسوب.
٥- تبادل الصور المفرط في وسائل التواصل بين الشابات مما يجعل الصور الخاصة في أكثر من جهاز وبالتالي احتمالية أكثر لوقوعها في أي أحد المبتزين فاقدي الوازع الديني.
٦- البطالة وأوقات الفراغ بالنسبة للشباب.
٧- قلة الوعي القانوني بعقوبة التهديد والابتزاز بشكل عام بالنسبة للمبتز.
٨- ضعف الرقابة على الشباب والشابات من قبل العائلة

أشكال الابتزاز الإلكتروني

يمكن تقسيم أنواع الابتزاز الالكتروني على حسب الغرض الذي يريده المبتز من الضحية، سوآءا أكان ماديًا أو جنسيًا أو منفعيًا:

١- فقد يكون هدف مادي بطلب المال من الضحية أو الأسرة أو الشركة

٢- أيضا الابتزاز الالكتروني الجنسي حيث يكون الابتزاز الالكتروني في هذا النوع لإشباع الغريزة لدى المبتز، فهو عادة ما يستهدف الشابات، أو حتى الأطفال.
٣- أخيرا قد يكون للمبتز أهداف أخرى كالأهداف السياسية أو المنفعية يستهدف بها مثلًا من يعمل في مجال الإعلام أو مجال التحقيق وذلك بهدف الكف عن تغطية الإعلام لقضية معينة أو عرقلة جهود التحقيقات

لو كانت المشاكل تحل بالهروب ، لكانت الكرة الأرضية كوكب مهجور

ماذا أفعل إذا وقعت في الابتزاز الالكتروني؟

- لا تتفاوض أو تدفع أي مال للمبتز لأن ذلك لن يجعله يتوقف عن ابتزازك.
- حاول بقدر الإمكان التعرف على أي تفاصيل عن المبتز مثل الهوية، والحساب ونوع هاتفه، وأي دليل يدعم جريمة الابتزاز.
- أيضا من الممكن أن تطلب المساعدة من محقق أو مستشار لجمع وتوثيق الأدلة.
- في حال كان الابتزاز الالكتروني نتيجة عملية اختراق، فاستعن بأحد المختصين لتوثيق عملية الاختراق، ثم اقطع الاتصال بالإنترنت على الجهاز.
- لكن إذا لم تكن بسبب الاختراق، فحينها يفضل فحص الجهاز من الفيروسات.

- سواءا أكنت قاصرًا صغيرًا أو حتى كبيرًا راشدًا فمن الأفضل استشارة من هو قريب إليك وخاصًا أحد والديك حتى يحاولان إيجاد حل للمشكلة قبل أن تتفاقم ويصبح حلها معقّدًا.
- أخيرا قم بإبلاغ أقرب أحد جهات مكافحة الابتزاز الالكتروني في بلدك

مكافحة الابتزاز الالكتروني على النطاق الشخصي

- التأكد من محو جميع الصور والملفات الحساسة قبل بيع الهاتف المحمول إما باستخدام أحد تطبيقات محو الملفات في الجهاز نهائيًا مثل تطبيق Super Easer للأندرويد، أو عن طريق إعادة تهيئة الجهاز ثم تخزين ملفات غير مهمة فيه مرة أخرى، ثم إعادة التهيئة مرة أخرى ويفضل التكرار لعدد من المرات.
- عدم إرسال الصور الشخصية إلى أفراد غير معروفين على وسائل التواصل الاجتماعي حتى لغرض التعارف.

- تجنب إرسال الصور الخاصة على حسابات التواصل، لأن اختراقها قد يتسبب في حدوث الابتزاز الالكتروني.
- تفعيل دور الرقابة في الأسرة.
- اتباع الطرق الآمنة في استخدام الانترنت وذلك بعدم فتح الروابط مجهولة المصدر قبل فحصها من التهديدات، وكذلك عدم فتح البرامج من أي مصدر غير معروف ما عدا تنزيلها من المتاجر المعروفة.
- الاهتمام بتحديث النظام والبرامج المشهورة على الجهاز وذلك لتجنب أمتلاك تطبيق يحتوي على ثغرات يمكن استغلالها.

مع اطيب التحيات