الابتزاز الإلكتروني : انواعه وعقوبته في العراق

ا.د بلقيس عيدان لويس

كلية التربية للبنات

قسم التاريخ

المقدمة :

يمتاز عصرنا بسرعة التطور التكنولوجي ، وقد رافق هذا التطور مع الاسف نمو الأشكال المختلفة للجريمة الالكترونية عبر شبكة الإنترنت نذكرها على وجه الاختصار كالتالي :

1-هجمات الحرمان من الخدمات: ويُرمز لها بالرمز(DDoS) ، وتُنفّذ هذه الهجمات باستخدام مجموعات كبيرة من أجهزة الكمبيوتر يُتحكَّم بها عن بُعد بواسطة أشخاص يستخدمون نطاق ترددي مشترك، وتهدف هذه الهجمات لإغراق الموقع المستهدف بكميّات هائلة من البيانات في آن واحد، ممّا يُسبّب بطئاً وإعاقةً في وصول المستخدمين للموقع.

2-التصيد الاحتيالي: يُعتبر هذا النوع من الجرائم الإلكترونية الأكثر انتشاراً، وهو إرسال جماعي لرسائل تصل عبر البريد الإلكتروني تحتوي على روابط لمواقع أو مرفقات ضارّة، وبمجرّد نقر المستخدم عليها فإنّه قد يبدأ بتحميل برامج ضارة بجهاز الكمبيوتر أو الهاتف الخاص به.

3- مجموعات الاستغلال: يعرّف هذا النوع على أنّه استخدام برامج مصمّمة لاستغلال أيّ أخطاء أو ثغرات أمنية في أجهزة الكمبيوتر، كما يُمكن للقراصنة اختراق مواقع ويب شرعية واستخدامها للإيقاع بضحاياهم.

4-برامج الفدية: تمنع هذه البرامج صاحب الجهاز من الوصول إلى ملفّاته المخزّنة على محرّك الأقراص الصلبة، ويشترط المجرم على الضحيّة دفع مبلغ ماليّ كفدية لإتاحة استعادة ملفاته التي يحتاجها.

5-القرصنة: تُعرّف القرنصة على أنّها وصول غير شرعي إلى بيانات ومعلومات موجودة على أجهزة الكمبيوتر أو شبكات الإنترنت او الهواتف من خلال استغلال نقاط ضعف وثغرات في هذه الأنظمة.

6-سرقة الهويّة: يحدث هذا النوع من الجرائم عندما يحصل شخص ما على المعلومات الشخصية لشخص آخر بشكل غير قانونيّ ويستخدمها لأغراض غير شرعية مثل الاحتيال والسرقة.

7- الهندسة الاجتماعية: يعتمد هذا النوع من الجرائم على العنصر البشري في التلاعب النفسي بالضحية لإرغامها على القيام بأعمال غير قانونية أو إفشاء معلومات سريّة، وهي من الأساليب التي يستخدمها مجرمو الإنترنت للقيام بأعمال الاحتيال أو الابتزاز .

8- قرصنة البرمجيات: تُعرّف قرصنة البرمجيات على أنّها إعادة توزيع واستخدام لبرمجيات دون تصريح من الشركة المالكة للبرمجية.

9-البرمجيات الخبيثة: تُعرف البرمجيات الخبيثة بأنّها البرمجيات التي تؤثّر على الأداء الطبيعيّ لأجهزة الكمبيوتر تتضمّن برمجيات الإعلانات، وبرمجيات التجسس، وبرمجيات خبيثة هجينة .

الابتزاز الإلكتروني:

يقصد به عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية.

وعادة ما يتم تصيد الضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الاجتماعي المختلفة كـ الفيس بوك، تويتر، وإنستغرام وغيرها من وسائل التواصل الإجتماعي نظرًا لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع أو عن طريق استعادة محتويات الهاتف المحمول بعد بيعه أو سرقته.

ويمكن أن يحدث أيضًا عندما يرسل الضحايا أنفسهم (بالتراضي أو بالإكراه) صورهم ومقاطع الفيديو الخاصة بهم إلى الآخرين (بما في ذلك الأصدقاء أو شركاء العمل)، والذين بدورهم يستخدمون المحتوى لغرض تهديد الضحية والحصول على شيء ما بالقوة في المقابل.

عادة ما يستهدف المجرمين الضحايا من الشباب أو الأطفال أو كبار السن. وغالبًا ما يتم استهداف النساء والفتيات بغرض نشر صور أو محادثات ذات محتوى فاضح أو خاص.و يمكن أن يقع الرجال والشباب أيضًا ضحايا لهذا النوع من الابتزاز، وإن كان بدرجة أقل من الإناث.

عملية الابتزاز

تبدأ العملية عادة عن طريق إقامة علاقة صداقة مع الشخص المستهدف، ثم يتم الانتقال إلى مرحلة التواصل عن طريق برامج المحادثات المرئية ، ليقوم بعد ذلك المبتز بإستدراج الضحية وتسجيل المحادثة التي تحتوي على محتوى مسيء وفاضح للضحية. ثم يقوم أخيرا بتهديده وابتزازه بطلب تحويل مبالغ مالية أو تسريب معلومات سرية، وقد تصل درجة الابتزاز في بعض الحالات إلى إسناد أوامر مخلة بالشرف والأعراف والتقاليد مستغلًا بذلك استسلام الضحية وجهلة بالأساليب المتبعة للتعامل مع مثل هذه الحالات.

اسباب ارتكاب المجرمين لجريمة الإبتزاز الإلكتروني؟

يمكن أن يكون الدافع وراء مرتكبي الابتزاز والتهديد الالكتروني مجموعة متنوعة من العوامل منها بشكل عام : الدوافع مادية أو مالية أو نفسية أو عاطفية.

الاضرار المترتبة عن عملية الابتزاز

قد يكون ضرر الابتزاز الالكتروني مباشرًا أو غير مباشر، جسديًا، نفسيًا، أو ماليًا، ويمكن للضحية أن تعاني من آثار طويلة الأمد للجريمة. ويمكن أن يؤدي هذا النوع من الجرائم إلى ضرر كبير بما في ذلك الأذى النفسي اذا اقدم المبتز على الانتقام من الضحية أن رفضت للمجرم مطلباً أو قطعت علاقتها معه ؛ فضلا عن كون الابتزاز قد يدفع البعض إلى الانتحار أو اقدام الاهل على جرائم الشرف، فضلاً عن الضرر الذي قد يلحق بتعليم الضحية وآفاقها المهنية والاستقرار المالي.

إرتفاع جرائم الإبتزاز الإلكتروني في العراق

شهدت السنوات الأخيرة زيادة كبيرة في عدد الجرائم الإلكترونية المرتكبة في العراق. ووثقت وزارة الداخلية العديد من الجرائم التي تستهدف الضحايا خاصة الفتيات والنساء.

على سبيل المثال، اعتقلت الشرطة العراقية حوالي 60 شخصًا شكلوا عصابات لاستهداف الفتيات المراهقات، والاستيلاء على صورهن، وابتزازهن مقابل دفع المال أو ممارسة الجنس.

وبشكل متكرر، تكشف وزارة الداخلية العراقية عن وقوع حوادث مماثلة، يطالب فيها المبتزون بمبالغ مالية يدفعها الضحايا تجنبا للفضيحة، أو يطالبونهم بالقيام بممارسات شائنة ، عادة ما تنطوي على ممارسة أفعال جنسية.

كما قالت الداخلية العراقية إنها تمكنت من اعتقال "متهم ببغداد لقيامه بابتزاز فتاة إلكترونيا، وتهديدها بنشر صورها، ومقاطع الفيديو على مواقع التواصل الاجتماعي، إذا لم تدفع له مبلغا من المال."

ويقول المتحدث باسم وزارة الداخلية خالد المحنا إن "الجرائم الإلكترونية ازدادت بشكل كبير في العراق نتيجة استخدام الأجهزة الذكية وتعدد مواقع التواصل الاجتماعي واعتماد المواطنين عليها حاليا بشكل كبير حتى في تعاملاتهم التجارية."

ويضيف المحنا في حديث لموقع "الحرة" انه في الآونة الأخيرة بدأت تتصاعد حالات الابتزاز الإلكتروني، ما دفع وزارة الداخلية إلى التحرك بعد أن اكتشفت أن الموضوع يؤثر كثيرا على الأمن المجتمعي".

وللاسف لا تتوفر إحصاءات دقيقة عن عدد حالات الابتزاز الإلكتروني في العراق، سواء لدى السلطات أو منظمات المجتمع المدني لأن كثيرا من العائلات أو الفتيات اللواتي يتعرضن للابتزاز يحجمن عن الإبلاغ.

ويشير خبراء علم النفس في العراق، إن معظم الضحايا لا يتوجهون للمؤسسات المعنية لأنهم يخافون "الفضيحة" وبالتالي نادرا ما يمكن الوصول لأرقام دقيقة لعدد ضحايا الابتزاز الإلكتروني في البلد.

عقوبة الإبتزاز الإلكتروني

وفقًا للقانون العراقي، تنقسم الجرائم الإلكترونية إلى عدة أجزاء، بما في ذلك جرائم التهديد والابتزاز، في المواد ما بين 430 - 432 من قانون العقوبات. والعقوبة على هذه الجرائم، حسب شدة الجريمة، هي السجن من سنة إلى سبع سنوات.

وتشير وزارة الداخلية إلى أن "أغلب الأشخاص الذين تم ضبطهم متلبسين أحيلوا للمحاكم وحكم عليهم بأحكام طويلة بعضها وصلت لـ 14 سنة و7 سنوات."

ويبدو ان هذه العقوبات والملاحقة المستمرة"، تمكنت من المحافظة أو تخفيض نسبة الجرائم الالكترونية بشكل ملحوظ.

ماذا تفعل إذا كنت ضحية لجرائم الإنترنت؟

أولًا: لا تحاول الرد على المبتز أو إقناعه بعدم نشر صورك. قد يقودهم ذلك إلى الاعتقاد بأنك ضعيف أو عدواني أو مستجيب لمطالبهم، مما قد يدفعهم إلى زيادة مطالبهم أو التحقق من صحتها.

ثانياً: لا تزودهم بتفاصيل عن قيمة الأموال التي لديك ولا تدفع لهم. قد يشجعهم ردك في المرة الأولى على طلب المزيد من المال أو المزيد من الصور ومقاطع الفيديو. إذا هددوك بالعنف، فاتصل بالشرطة.

ثالثاً: 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، إذ أن حذف الأدلة التي يمكن استخدامها لإدانة المجرمين وبحذف الإدلة تسمح لهم بأن يكونوا المالك الوحيد للمحتوى.

رابعًا: بينما لا يجب التخلص من أدلة الإدانة، يجب عليك منع المبتز من متابعة حساباتك على مواقع التواصل الاجتماعي وتغيير جميع كلمات المرور الخاصة بحساباتك وبريدك الإلكتروني على الفور.

خامساً: إذا كنت تشعر بالأمان لأحد قريب منك، أخبر شخصًا موثوقًا بما حدث لك، لتزويدك بالدعم النفسي حتى يتمكن من تقديم أدلة لصالحك إذا لزم الأمر في المحكمة. إذا كنت قادرًا على ذلك، اطلب دعمًا نفسيًا من متخصصين مدربين، حيث يمكن أن يكون للابتزاز الإلكتروني آثار كبيرة على الصحة العقلية والنفسية.

سادسًا: إذا كنت في العراق، فاتصل بالشرطة أو جهاز الأمن الوطني وقسم الجرائم الإلكترونية في مديرية تحقيقات الأدلة الجنائية. سيمكن هذا من توجيه اتهام رسمي ضد المبتز. ، وبكون ذلك بالاتصال على الخط الساخن الحكومي بالارقام 131 أو 533.

ويمكن لضحايا الابتزاز أو التهديد الألكتروني تقديم شكوى في أقرب مركز شرطة. وبعد تسجيل الشكوى يحيل القاضي الامر إلى ضابط التحقيق في مركز الشرطة المعني لإجراء تحقيق قانوني.

نصائح مهمة لتجنب الوقوع ضحية لجرائم الإبتزاز الإلكتروني:

فيما يأتي بعض النصائح للأشخاص لزيادة سلامتهم عبر الإنترنت وتقليل فرص الوقوع ضحية للجرائم الإلكترونية:

1-تأمين الجهاز الإلكتروني، سواء كان جهاز كمبيوتر أو هاتفًا ذكيًا، وعدم استخدام التطبيقات والروابط غير الموثوق بها.

2-تجنّبوا نشر بيانات ومعلومات مهمة أو شخصية عنكم على وسائل التواصل الاجتماعي.

3-تجنبوا مشاركة أي صور أو مقاطع فيديو فاضحة على وسائل التواصل الاجتماعي حتى لا يسهل الاستيلاء عليها واستخدامها كذريعة للابتزاز.

4-لا تحتفظوا بأي مقاطع فيديو أو صور خاصة على الهاتف المحمول، بسبب خطر التعرض للسرقة. في حالة سرقة الهاتف نفسه وحفظها على قرص صلب خارجي يتم حفظه في مكان آمن.

5-قوموا بتغيير كلمات المرور بانتظام ولا تستخدموا نفس كلمة المرور لحسابات أنظمة أساسية مختلفة.

6-إختاروا كلمات مرور قوية لحساباتكم على مواقع التواصل الاجتماعي، وهي كلمات يصعب على المخترق تخمينها، بحيث تكون بعيدة عن اسمائكم وتاريخ ميلادكم، وكذلك الأرقام 123 على التوالي، وهي كلمات المرور التي يفضلها المستخدمون غالبًا.

7-اكتبوا كلمات مروركم على قطعة من الورق واحتفظوا بها في مكان آمن لا يعرفه أحد، ولا تشاركوا كلمات مروركم أبدًا مع أي شخص بغض النظر عن مدى ثقتكم بهم.

8-تحققوا من إعدادات الأمان والخصوصية على جميع حسابات وسائل التواصل الاجتماعي

9-إذا قررتم بيع هاتفكم، فلا تكتفوا بمسح الصور وأرقام الهواتف، يجب بعدها أن تخرجوا من جميع حساباتكم على هاتفكم المحمول قبل بيعه أو التخلص منه. ثم يجب عليكم تشغيل الجهاز، ثم تشغيل كاميرا الفيديو وترك الهاتف في غرفة مظلمة، على سبيل المثال، حتى تمتلئ ذاكرة الهاتف الداخلية بالكامل، وفي ذلك الوقت سيقوم الهاتف بإيقاف تشغيل الكاميرا تلقائيًا، ثم إحذفوا الفيديو، هكذا تتأكدون من أن أي شخص يحاول استعادة محتويات الكاميرا سيجد هذا الفيديو المظلم فقط