

أكد في لقاء مع «الأنباء» أن الحملة التوعوية «وقاية.. وأمان» تهدف إلى تعزيز الوعي والوقاية

المقدم سعود الوزان: 3 آلاف شكوى وقضية تستقبلها «مكافحة الجرائم الإلكترونية» سنوياً



المقدم سعود أنور الوزان

منصور السلطان

الجرائم الإلكترونية تتنوع بين التهديد والابتزاز والنصب والاحتيال وإساءة استعمال الهاتف والتشهير والمساس بالأداب العامة والتحرش على الفسق والفجور، مؤكداً أن التعامل مع هذه القضايا يتطلب سرعة في الاستجابة ودقة في جمع الأدلة الرقمية وتنبع الآثار الإلكترونية المرتبطة بالواقعة. وأضاف أن التطور المتسارع في التقنيات الحديثة وفي مقدمتها الذكاء الاصطناعي أوجد أنماطاً جديدة من التحديات بعدما أصبح بالإمكان استخدام تقنيات التزييف والتلاعب بالصور ومقاطع الفيديو وتقليد الأصوات في عمليات الاحتيال أو انتحال الشخصية، مشدداً على أهمية عدم التعامل مع أي صورة أو تسجيل أو رسالة على أنها حقيقية لمجرد ظهورها بصورة مقنعة. وشدد المقدم الوزان على أن العالم الافتراضي ليس خارج نطاق القانون، وأن استخدام وسائل التواصل الاجتماعي لا يعني مستخدمها من المسؤولية القانونية، مبيناً أن حرية التعبير مكفولة في حدود القانون، إلا أن هذه الحرية لا تمتد إلى ارتكاب أفعال مجرمة، كالتهديد أو الابتزاز أو التشهير أو الاحتيال أو انتهاك خصوصية الآخرين. كل هذه الأمور وغيرها تطرق إليها المقدم سعود الوزان خلال اللقاء، تفصيلها في السطور التالية.

أكد المقدم سعود أنور الوزان من إدارة مكافحة الجرائم الإلكترونية بالإدارة العامة للمباحث الجنائية، أن «الجرائم الإلكترونية» تستقبل نحو 3000 شكوى وقضية سنوياً. وفتح المقدم الوزان في لقاء مع «الأنباء» ملف الجرائم الإلكترونية متحدثاً عن واقعتها في الكويت وأبرز القضايا التي تتعامل معها الإدارة والتحديسات التي تواجه رجال الأمن في ملاحقة مرتكبيها وتأثير الذكاء الاصطناعي في تطوير أساليب الجريمة إلى جانب المخاطر التي تهدد الأطفال والشباب ودور الأسرة في الوقاية وأهمية الوعي وسرعة الإبلاغ والمحافظة على الأدلة الرقمية، وذلك ضمن الحملة التوعوية «وقاية... وأمان» التي تنظمها إدارة الإعلام الأمني بوزارة الداخلية منذ انطلاق العام الدراسي 2026-2027. وأوضح أن الجرائم الإلكترونية في البلاد تشهد تطوراً ملحوظاً في نوعيتها وأساليب ارتكابها في ظل التوسع الكبير في استخدام الوسائل والمنصات الإلكترونية، مشيراً إلى أن أساليب الاحتيال وانتحال الشخصية والتصيد الإلكتروني وسرقة البيانات والمسابقات الشخصية إلى جانب استهداف المسابقات البثكية باتت من أبرز صور الجرائم التي تتعامل معها الجهات المختصة. وكشف أن القضايا التي تستقبلها إدارة مكافحة

- الجرائم الإلكترونية تتطور مع تسارع التكنولوجيا.. والذكاء الاصطناعي يفرض تحديات جديدة
- يتم رصد حسابات ومواقع تنشر محتويات تتعلق باستخدام الأسلحة وصناعة المتفجرات
- التزييف بالذكاء الاصطناعي.. صور وأصوات ومقاطع قد تستخدم في الاحتيال
- التهديد والتشهير والابتزاز والدخول غير المشروع أبرز الأفعال المستوجبة للمساءلة

به الشخص إلكترونياً قد يعرضه للمساءلة القانونية. والجهات المعنية تتابع ما يحدث في الفضاء الإلكتروني، وسيتم اتخاذ الإجراءات القانونية بحق كل من يتجاوز القانون.

كم يبلغ عدد الشكاوى والقضايا التي تستقبلها إدارة مكافحة الجرائم الإلكترونية سنوياً؟ وما أبرز أنواعها؟

● تستقبل إدارة مكافحة الجرائم الإلكترونية سنوياً ما يقارب 3000 شكوى وقضية، وتتعدد أنواعها، ومن أبرزها التهديد والابتزاز والنصب والاحتيال وإساءة استعمال الهاتف والتشهير والمساس بالأداب العامة والتحرش على الفسق والفجور.

ما النصيحة الأهم التي تقدمونها لمستخدمي الهواتف ووسائل التواصل؟

● الوقاية تبدأ من الوعي والانتباه في التعامل مع الوسائل الإلكترونية. يجب عدم مشاركة البيانات الشخصية أو البثكية، وتجنب الضغط على الروابط المجهولة، واستخدام كلمات مرور قوية ومختلفة مع تفعيل خاصية التحقق بخطوتين، والتأكد دائماً من هوية الطرف الذي يتم التعامل معه، كما أن توعية الأبناء ومتابعة استخدامهم للإنترنت وتضلّلان جانباً مهماً من حماية الأسرة. لأن كثيراً من الجرائم تنتخذ الإجراءات القانونية الباذلة، أو إجراء بسبب يتم من دون التأكد من عواقبها.

كيف يتم التعامل مع المواقع التي تنشر محتويات تشجع استخدام الأسلحة أو صناعة المتفجرات؟

● قد توجد مواقع أو حسابات تنشر محتويات تتعلق باستخدام الأسلحة أو صناعة المتفجرات، ويتم رصدها والتعامل معها وفقاً لسياسة المحتوى والغرض من نشرها، فإذا تبين وجود تحريض أو تعليم بقصد ارتكاب أعمال إجرامية أو تهديد الأمن تتخذ الإجراءات القانونية اللازمة بالتنسيق مع الجهات المختصة. وقد سبق التعامل مع قضايا ومحتويات مشابهة، وفقاً لما تسفر عنه التحريات والأدلة الفنية والإجراءات القانونية المتبعة.

كيف يتم التعامل مع المحتويات المحظورة التي يتم تداولها عبر مواقع التواصل الاجتماعي؟

● يتم رصد المحتوى والتحقق منه فنياً، والعمل على تحديد القائم على الحساب وجمع الأدلة الرقمية المرتبطة بالواقعة، ثم اتخاذ الإجراءات القانونية وإحالتها إلى جهة الاختصاص. ومن المهم أن يدرك مستخدمو مواقع التواصل أن النشر الإلكتروني لا يعني الاعتقاد عن المساءلة، فالمحتوى الرقمي يمكن تتبعه وتوقيفه والاستدلال من خلاله على مرتكب الواقعة.

العنف بين الشباب

ما دوركم في الحد من العنف بين الأحداث والشباب عبر مواقع التواصل؟

● يتمثل دورنا في الرصد المبكر للمحتويات التي تتضمن تهديداً أو تحريضاً أو تشميراً أو دعوات إلى العنف، واتخاذ الإجراءات القانونية اللازمة، إلى جانب الجانب الوقائي والتوعوي. وفي هذا الجانب، تبقى الأسرة والمدرسة شريكتين أساسيتين في حماية الأبناء، من خلال المتابعة والتوعية والتدخل المبكر، كما يساعد على معالجة السلوكيات الخطرة قبل أن تتطور إلى مشكلات أو جرائم فعلية.

الحساسية مع الآخرين..

استدراج الأطفال إلكترونياً

هل ترصد الإهارة محاولات لاستدراج الأطفال عبر الألعاب الإلكترونية أو منصات التواصل؟

● نعم، قد تحدث محاولات لاستدراج الأطفال من خلال المحادثات داخل الألعاب الإلكترونية أو عبر منصات التواصل الاجتماعي، وقد تبدأ هذه المحاولات بصورة طبيعية من خلال التعارف أو اللعب أو الحوار، ثم تتطور تدريجياً إلى طلب معلومات شخصية أو صور خاصة أو محاولة الانتقال إلى وسيلة تواصل أخرى أكثر خصوصية.

وهنا تكمن أهمية توعية الأطفال بعدم التعامل مع الأشخاص مجهولين كأنهم أشخاص موثوقون لمجرد استمرار التواصل معهم لفترة، وضرورة إبلاغ الأسرة فوراً عند وجود أي طلب غير طبيعي أو موقف يثير الشك أو الخوف.

ما العلامات التي يمكن أن تلاحظها الأسرة وتدل على تعرض أحد الأبناء لمشكلة إلكترونية؟

● هناك مجموعة من المؤشرات التي قد تلفت انتباه الأسرة، منها التغير المفاجئ في سلوك الابن، أو ظهور الخوف والقلق أثناء استخدام الهاتف، أو إخفاء المحادثات والحسابات، متكررة من حسابات مجهولة. ومن العلامات التي تستوجب الانتباه أيضاً طلب المال بصورة غير معتادة أو ظهور حالة من التوتر عند وصول إشعارات أو اتصالات معينة. ولا يعني ظهور إحدى هذه العلامات بالضرورة أن الطفل يتعرض لجريمة إلكترونية، لكنها مؤشرات تستدعي الحوار الهادئ معه ومعرفة ما يواجهه، دون تخويف أو توبيخ، حتى يتمكن من الإفصاح عن المشكلة وطلب المساعدة.

هل ترون أن التشريعات الحالية تواكب التطور السريع في الجرائم الإلكترونية؟

● نعم، التشريعات الحالية تواكب بدرجة كبيرة التطور في مجال الجرائم الإلكترونية، إلا أن التطور المتسارع في التقنيات ووسائل ارتكاب الجرائم الإلكترونية يفرض الحاجة إلى مراجعة وتحديث بعض التشريعات بصورة مستمرة، بما يضمن مواكبة المستجدات التقنية والتعامل مع الأساليب الجديدة التي قد يستخدمها مرتكبو الجرائم الإلكترونية. ما أبرز العقوبات التي يجب أن يعرفها مستخدمو وسائل التواصل الاجتماعي حتى لا يقعوا تحت طائلة القانون؟

● يجب على مستخدمي وسائل التواصل الاجتماعي أن يدركوا أن استخدام هذه الوسائل لا يعفي



المقدم سعود أنور الوزان مع الزميل منصور السلطان (رئيس كورام)

الحملة التوعوية «وقاية... وأمان» التي أطلقتها إدارة الإعلام الأمني والتي تستهدف تعزيز الثقافة الأمنية لدى مختلف شرائح المجتمع من المنصات الإلكترونية، ومعرفة التطبيقات التي يستخدمونها وطبيعة تفاعلهم معها، ووضع قواعد واضحة ومناسبة للاستخدام. وفي الوقت نفسه، يجب ألا تتحول المتابعة إلى مصدر للخوف أو انعدام الثقة، بل ينبغي أن تقوم على الحوار والتوجيه والتوعية، حتى يشعر الابن بأنه يستطيع اللجوء إلى والديه في حال تعرضه لأي موقف غير آمن. ما محاولة استدراج أو ابتزاز. كما ننصح الأسرة بتوعية الأبناء بأهمية المحافظة على كلمات المرور والبيانات الشخصية وعدم مشاركة الصور الخاصة أو المعلومات

الرسالة التي توجهونها للأباء والأمهات بشأن متابعة استخدام

جهود كبيرة للعقيد السمحان والقائمين على حملة «وقاية.. وأمان»



العقيد مشاري أحمد السمحان

دور مهم تقوم به الحملة التوعوية «وقاية... وأمان»، التي أطلقتها إدارة الإعلام الأمني بوزارة الداخلية في تعزيز الثقافة الأمنية في شرائح المجتمع، ونشر الرسائل التوعوية بأسلوب مبسّط يواكب التحديات والمخاطر المستجدة، وهو ما تستحق عليه الإشادة والثناء. ويأتي هذا النجاح ثمرة للجهود المخلصة التي يبذلها القائمون على الحملة، بقيادة مدير إدارة الإعلام الأمني في الإدارة العامة للعلاقات والإعلام الأمني بوزارة الداخلية العقيد مشاري أحمد السمحان، وما يقدمه فريق العمل من جهود متواصلة في إعداد وتنفيذ البرامج والرسائل التوعوية بما يعزز الشراكة بين المؤسسة الأمنية والمجتمع. وقد أكدت الحملة أن التوعية تمثل خط الدفاع الأول في مواجهة العديد من المخاطر وأن الوصول إلى مختلف فئات المجتمع برسائل أمنية واضحة وهادئة يسهم في رفع مستوى الوعي والوقاية ويعزز المسؤولية المجتمعية في الحفاظ على الأمن والسلامة.

بعض الجرائم الإلكترونية، يمكن أيضاً توظيف تقنياته في دعم العمل الأمني.

ويمكن الاستفادة من التقنيات الحديثة في مجالات متعددة، ومنها تحليل كميات كبيرة من البيانات والأدلة الرقمية، ورصد الأنماط المشبوهة، ودعم عمليات البحث والتحليل، بما يسهم في تعزيز قدرات الجهات المختصة في مواجهة الجرائم الإلكترونية ومواكبة التطور التقني المتسارع.

تطبيق القوانين النافذة

هل هناك تشريعات خاصة بقضايا الذكاء الاصطناعي؟ وفي حال وجود قانون، هل هناك نية لتعديله؟

● يتم التعامل مع الأفعال الإجرامية التي تستخدم فيها تقنيات الذكاء الاصطناعي وفق التشريعات والقوانين النافذة، متى انطبقت عليها الأوصاف القانونية المجرمة، سواء تعلقت بالأحداث أو الانتحال الشخصية أو التحدي على الخصوصية أو غيرها من الأفعال التي تجرمها القوانين المعمول بها.

أما ما يتعلق باستخدامات تشريعات خاصة بالذكاء الاصطناعي أو إجراء تعديلات على التشريعات القائمة، فهو من اختصاص الجهات المعنية بالتشريع، بينما تقوم الإدارة بتطبيق القوانين والأنظمة النافذة، ومواكبة أي تحديثات أو تشريعات جديدة تصدر في هذا المجال.

كيف تفرق الإدارة بين حرية التعبير والمحتوى الذي يشكل جريمة إلكترونية؟

● يتم التفرقة في خلال مضمون المحتوى وطبيعته ومدى مخالفته للقوانين النافذة، فحرية التعبير مكفولة في حدود القانون، إلا أن هذه الحرية لا تمتد إلى ارتكاب

أفعال مجرمة قانوناً أو الاعتداء على حقوق الآخرين، وبالتالي يتم التعامل مع كل بلاغ وفق ظروفاً وملاساته والمحتوى محل الشكوى، ويتم فحص الأدلة الرقمية والتحقق من الواقعة قبل اتخاذ الإجراءات القانونية المناسبة، بما يضمن تطبيق القانون وفقاً لطبيعة كل حالة.

نشر الوعي

ما دوركم في تثقيف ونشر الوعي لدى المجتمع عن مخاطر الاستخدام السيئ للفضاء الإلكتروني؟

● إن نشر الوعي والتثقيف الأمني يمثلان جانباً أساسياً في مواجهة أن حماية المجتمع لا تقتصر على ضبط مرتكبي الجرائم بعد وقوعها وإنما تبدأ بالوقاية ورفع مستوى الوعي لدى المواطنين والمقيمين وتعريفهم بأساليب الاحتيال والاستدراج والابتزاز التي تستخدمها العصابات الإلكترونية. ووزارة الداخلية

تولي الجانب التوعوي اهتماماً كبيراً من خلال الحملات الأمنية والأعلامية المستمرة وفي مقدمتها

إلى أي مدى يمكن استخدام الذكاء الاصطناعي في انتحال شخصية شخص آخر أو تقليد صوته؟

● أصبحت تقنيات الذكاء الاصطناعي قادرة على إنتاج محتوى يحاكي صور وأصوات الأشخاص بدرجة متقدمة، وقد يستغلها البعض بصورة إجرامية في انتحال شخصية شخص آخر أو إيهام شخصية بأن الاتصال أو الرسالة صادرة من شخص تعرفه أو من جهة موثوقة. وقد يتم توظيف هذه التقنيات في محاولات الاحتيال الإلكتروني أو الحصول على البيانات الشخصية والمصرفية أو دفع الضحية إلى تنفيذ تحويلات مالية أو إجراءات معينة، ولهذا يجب عدم الاعتماد على الصورة أو الصوت وحدهما للتحقق من هوية الشخص، خصوصاً عندما يتعلق الأمر بالبيانات البثكية أو التحويلات المالية أو رموز التحقق.

التزييف بالذكاء الاصطناعي

هل أصبحت تقنيات التزييف عبر الذكاء الاصطناعي تحدياً جديداً أمام أجهزة مكافحة الجرائم الإلكترونية؟

● بالتأكيد، تمثل تقنيات التزييف باستخدام الذكاء الاصطناعي أحد التحديات الحديثة في مجال الجرائم الإلكترونية، إلا أنها تأتي في إطار التطور المستمر والمتسارع لأساليب ارتكاب الجريمة الإلكترونية. وتتعاظم الإدارة مع هذه المستجدات من خلال مواكبة التقنيات الحديثة، ورفض فكرة الكوادر المختصة، وتطوير وسائل الفحص والتحليل للأدلة الرقمية، بما يساعد على التعامل مع الأنماط الجديدة من الجرائم وتحديد طبيعة المحتوى الرقمي المستخدم في الواقعة.

ملاحقة المتورطين

ما أبرز التحديات التي تواجه إدارة الجرائم الإلكترونية في ملاحقة المتورطين؟

● من أبرز التحديات أمام الإدارة في ظل هذا التطور التكنولوجي المتلاحق سرعة تطور أساليب وتقنيات الجرائم الإلكترونية، واستخدام الجناة وسائل متعددة لإخفاء هوياتهم ومواقعهم، إضافة إلى ارتكاب بعض الجرائم من خارج الدولة وتعدد الاختصاصات القضائية، كما تمثل سرعة حذف الأدلة الرقمية أو تشفيرها، إلى جانب تنوع المنصات الإلكترونية، تحدياً يتطلب سرعة الاستجابة والتعامل مع البلاغات، فضلاً عن أهمية التعاون المستمر مع الجهات المختصة ومزودي الخدمات التقنية.

كيف تواكب الإدارة التطور المتسارع في وسائل وتقنيات ارتكاب الجرائم الإلكترونية؟

● تواكب الإدارة هذا التطور من خلال التدريب والتأهيل المستمر للكوادر المتخصصة، وتحديث الكوادر والأنظمة التقنية المستخدمة في رصد وتحليل الجرائم الإلكترونية، إلى جانب تعزيز التعاون وتبادل المعلومات مع الجهات المختصة محلياً ودولياً. ويأتي ذلك بهدف مواكبة أحدث الأساليب والتقنيات المستخدمة في مجال مكافحة الجرائم الإلكترونية، ورفع مستوى القدرة على التعامل مع الأنماط المستجدة من الجرائم والاحتيال الإلكتروني.

مع الانتشار الكبير للذكاء الاصطناعي، هل ظهرت جرائم جديدة تعتمد على تقنيات التزييف والتلاعب بالصور والفيديو وتقليد الأصوات، بهدف الاحتيال أو انتحال شخصية أشخاص آخرين.

وتكمن الخطورة في قدرة هذه التقنيات على إنتاج محتوى يبدو في بعض الحالات مقنعاً للمستخدم العادي، وهو ما قد يستغله بعض المجرمين في عمليات الاحتيال أو انتحال الشخصية أو استدراج الضحايا، الأمر الذي يتطلب رفع مستوى الوعي والتعامل بحذر مع المحتوى الرقمي وعدم التعامل معه على أنه حقيقي لمجرد ظهوره بصورة أو صوت مقنع.

الأطفال والشباب أمام مخاطر الاستدراج

والابتزاز عبر الألعاب والمنصات

لدى سؤاله عن أبرز المخاطر التي يواجهها الأطفال والشباب، وهم من أكثر الفئات استخداماً للفضاء الإلكتروني، قال المقدم سعود الوزان إن هناك عدداً من المخاطر التي قد يتعرض لها الأطفال والشباب أثناء استخدامهم للفضاء الإلكتروني، أبرزها الابتزاز الإلكتروني والتشهير والاحتيال وسرقة الحسابات والبيانات الشخصية، إضافة إلى التواصل مع أشخاص مجهولين قد يحاولون استدراجهم أو استغلالهم. وتابع: قد تبدأ بعض عمليات الاستدراج بصورة تبدو عادية من خلال محاولة أو صداقة عبر إحدى المنصات، ثم تتطور تدريجياً إلى طلب معلومات شخصية أو صور خاصة أو الانتقال إلى محادثات أكثر خصوصية، الأمر الذي قد يعرض الطفل أو الشاب للاستغلال والابتزاز، لذلك فإن الوعي والرقابة الأسرية والحوار المستمر مع الأبناء تمثل عناصر مهمة في الوقاية من هذه المخاطر.

الأسرة شريك أساسي في حماية الأبناء من مخاطر

الفضاء الإلكتروني عبر المتابعة المستمرة

في إجابته على سؤال عن كيفية حماية الأسرة لأبنائها من الابتزاز والاستدراج الإلكتروني، قال المقدم سعود الوزان إن الحماية تبدأ بالتوعية والمتابعة وبناء علاقة قائمة على الثقة والحوار بين الأبناء وأولياء الأمور، مع تعليم الأبناء عدم مشاركة الصور أو المعلومات الخاصة مع الأشخاص الذين لا يعرفونهم. وعدم استجابة للمطالبات المشبوهة أو الانتقال إلى محادثات سرية مع