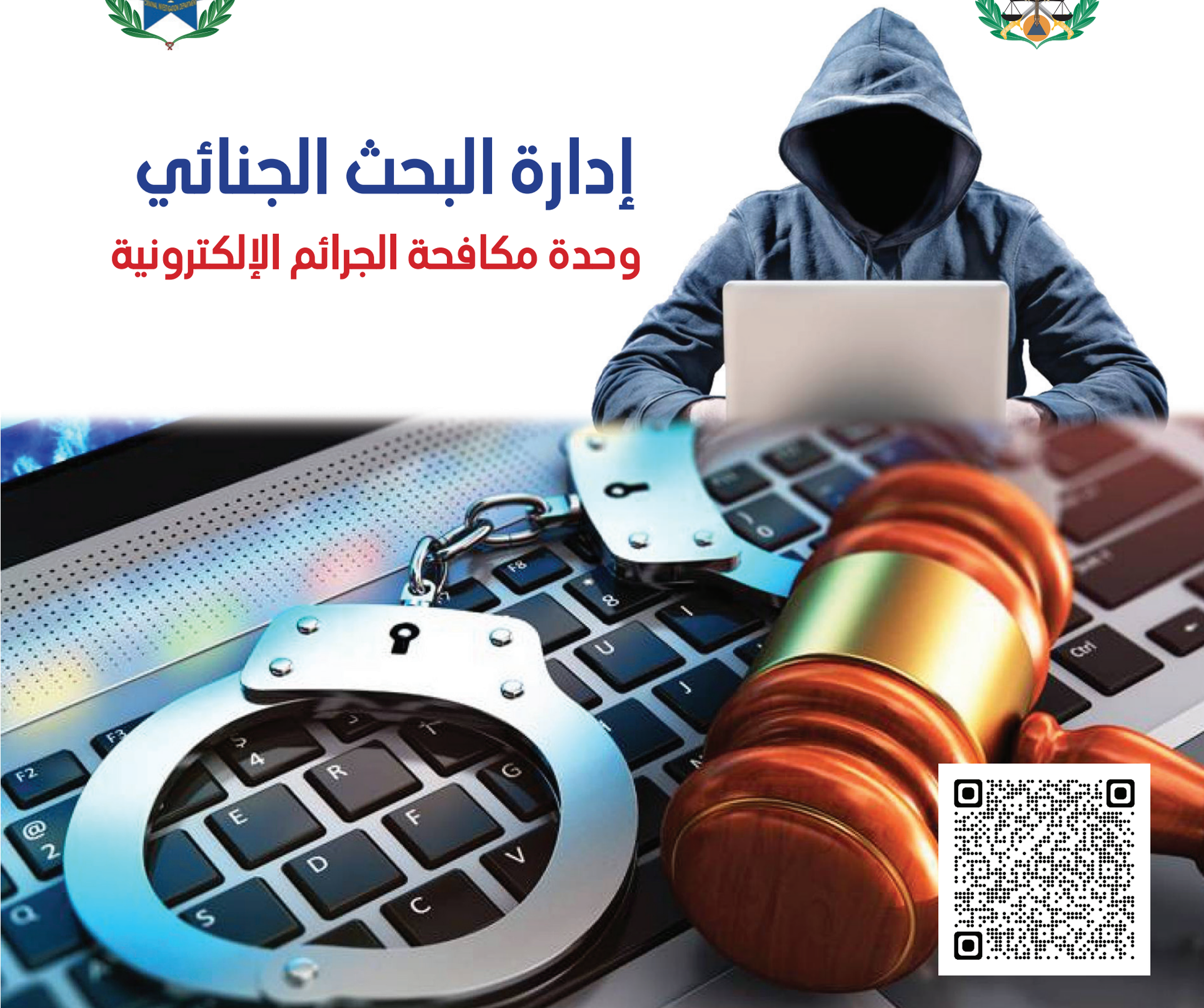
إدارة البحث الجنائي

وحدة مكافحة الجرائم الإلكترونية

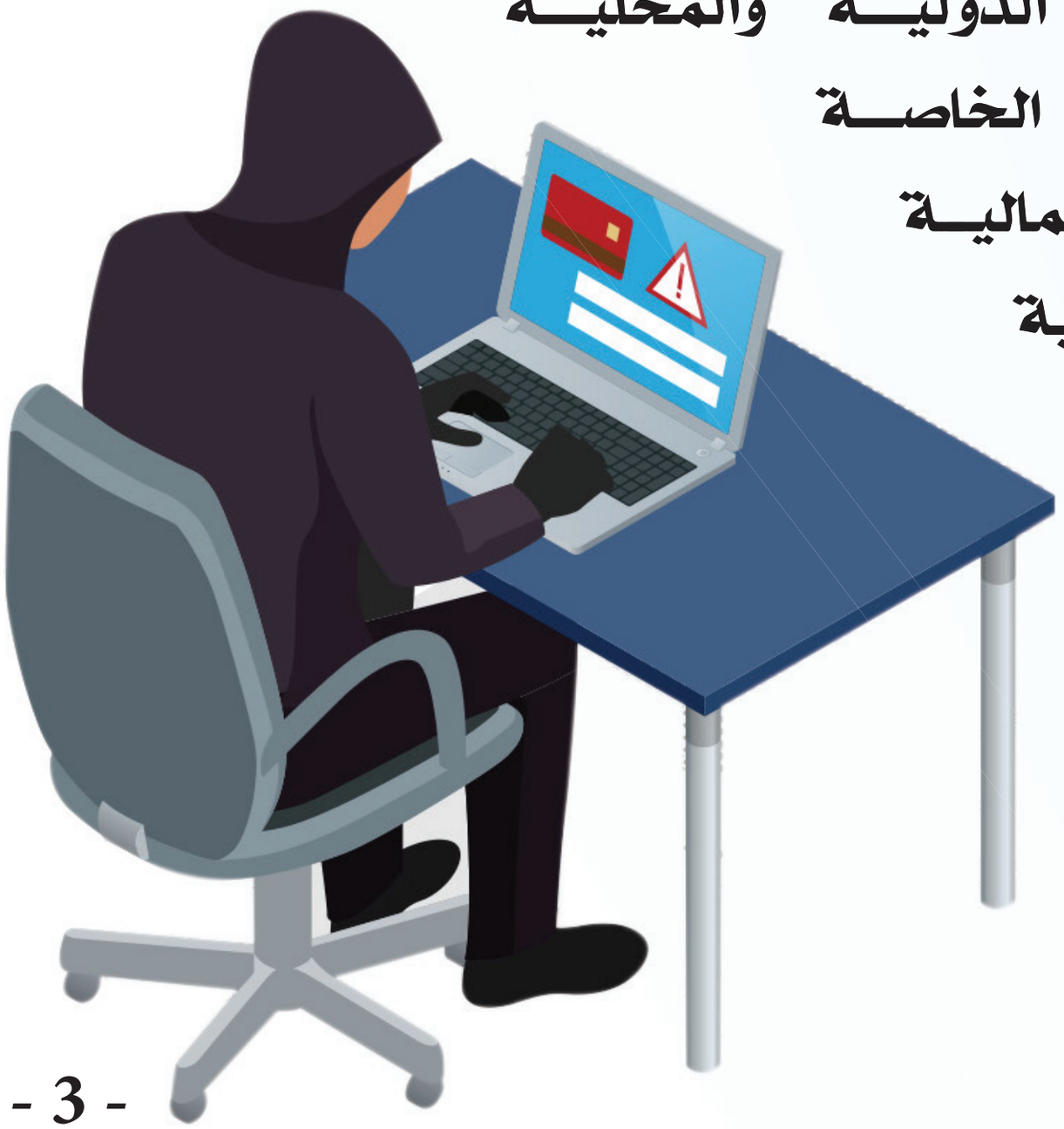


مديرية الأمن العام

وحدة الجرائم الإلكترونية

ترجمةً للرؤيا الملكية السامية، وتنفيذاً لتلك التوجيهات في حماية المواطن ، ومواكبة التطور الأمني أنشأت مديرية الأمن العام في إدارة البحث الجنائي قسم الجرائم الإلكترونية عام 2008م، وطورته عام 2015م باسم وحدة مكافحة الجرائم الإلكترونية ، وفي العام نفسه صدر قانون الجرائم الإلكترونية رقم (27) لمعالجة القضايا الإلكترونية ضمن مواده التي تبين الجرم وعقوبته.

وسعياً من مديرية الأمن العام لمكافحة الجريمة الإلكترونية، وتوعية المجتمع ضد مخاطرها تعمل الوحدة وفق نهج تشاركي مع المؤسسات والشركات الدولية والمحلية والمؤسسات الخاصة والمؤسسات المالية والمصرفية وشركات الاتصالات ومؤسسات المجتمع المدني.

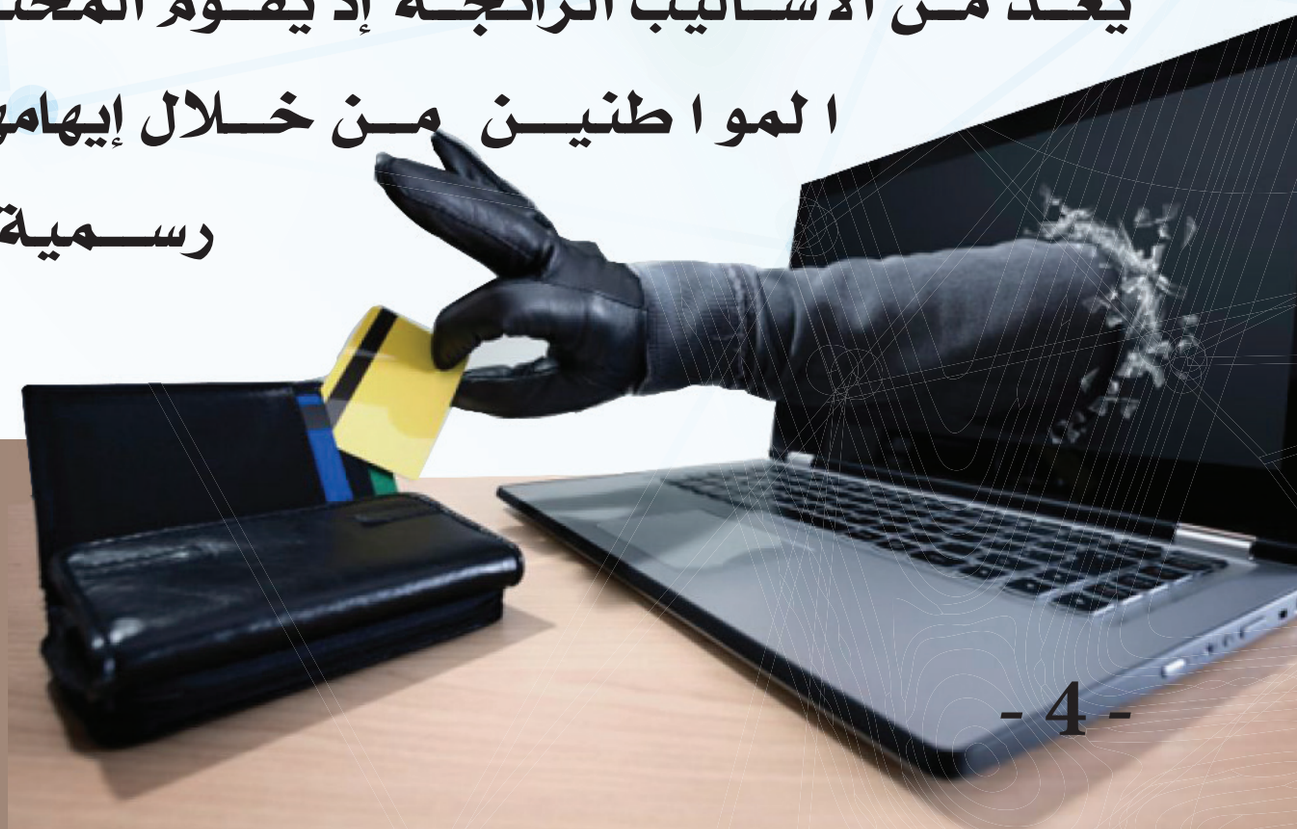


أولاً: الاحتيال المالي الإلكتروني

الاحتيال المالي : يُعد من القضايا الواقعة على الأموال سواء (منقولة أو غير منقولة) بهدف الوصول إلى كسب مادي أو معنوي غير مشروع ،باستخدام أسلوب احتيالي معين (الإيهام) والخديعة .

- **أساليب الاحتيال الإلكتروني :**
- **تقديم المساعدات المالية :**

يُعد من الأساليب الرائجة إذ يقوم المحتال بالتواصل مع المواطنين من خلال إيهامهم بأنهم جهة رسمية تقوم بتقديم مساعدات مالية



من خلال مكتب أحد الأمراء أو الشيوخ بالدول المجاورة المعروفة بالثراء ويوهم الضحية بمبالغ مالية كبيرة مقابل تحويله مبالغ مالية قليلة لحسابات بنكية ومحافظ إلكترونية على أنها مساعدات لعائلات فقيرة وفي الحقيقة هي حسابات مشبوهة يستخدمها المحتالون.

ربح جائزة :

يقوم المحتال في هذا الأسلوب بالاحتيال على المواطنين من خلال إيهامهم بأنهم جهة تقوم بعمل مسابقات لربح مركبة أو مبلغ مالي ، ويطلب من الضحية تحويل مبالغ نقدية على أنها رسوم جمركية أو ضرائب لنقل واستلام الجائزة ، وتحويل تلك المبالغ لحسابات بنكية أو محافظ إلكترونية تعود للمحتالين .

• مواقع الزواج :

أسلوب يقوم فيه المحتال باستغلال الفتيات من خلال علاقات غرامية على أساس الوعد بالزواج ويقوم بالاستيلاء

على أموالهن بالخداع والتهديد والابتزاز من خلال حسابات وهمية على مواقع التواصل الاجتماعي .

- **البورصات العالمية :**

أسلوب يقوم فيه المحتال باستغلال رغبة الضحية بالربح السريع من خلال إيهامه باستثمار أمواله في شركات تداول مالي وهمية .

- **الشعوذة والسحر:**

أسلوب يتم من خلاله الحصول على مال الغير بطرق الغش والخداع، وإيهام المجني عليه بالقدرة على تلبية الحاجات في العلاج من الأمراض المختلفة أو العلم بالغيب وكشف المستور، وذلك باستخدام طرق وأساليب احتيالية مضللة.

يستغل المحتال في هذا الأسلوب ذكاءه في مخاطبة الناس بفطرتهم، وبطرق مقنعة مرتبطة بالموروث الديني مستغلا حاجاتهم، وبعض المفاهيم المجتمعية المغلوطة في علم الغيب .

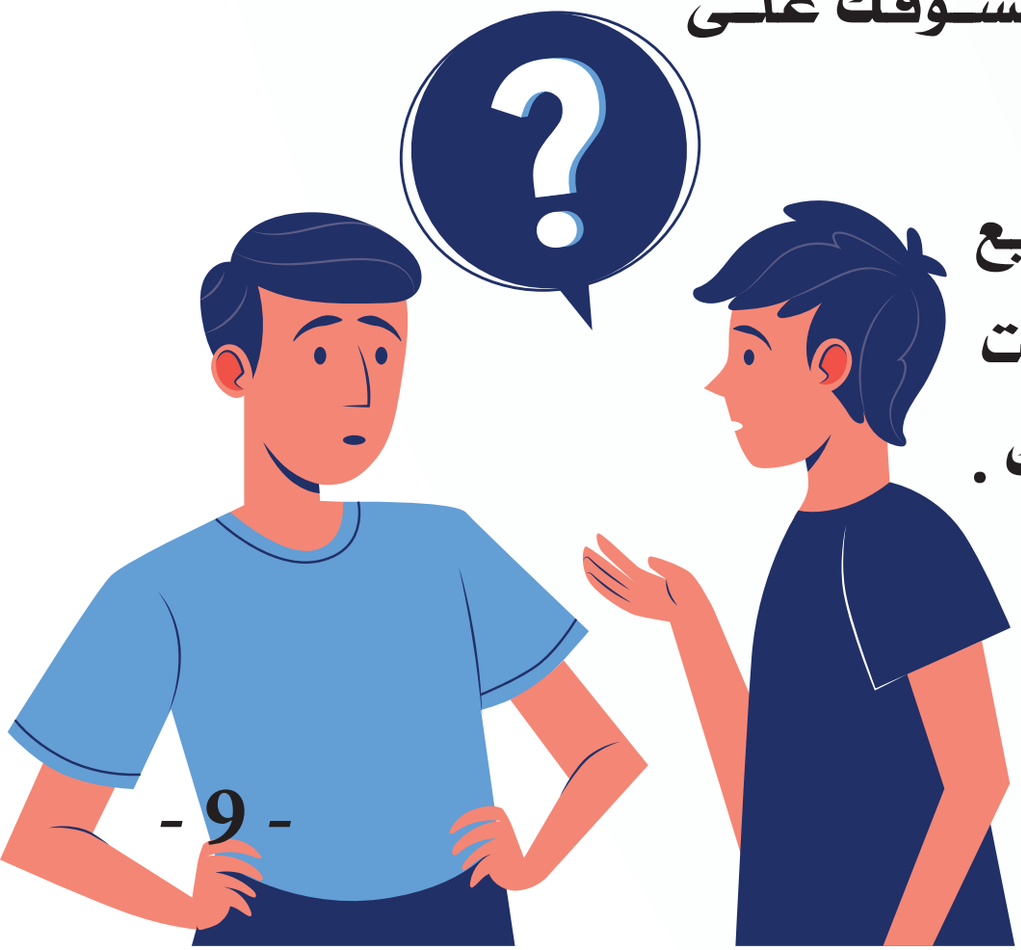
ننصحك باتباع الإرشادات التالية
حتى لا تقع ضحية للاحتيال الإلكتروني:

- لا تشارك بياناتك الائتمانية مع أي شخص حتى لو طلب منك التاجر أو المندوب ذلك.
- لا ترسل صوراً لوثائقك الشخصية ولا تشاركها مع أحد.
- التأكد باستمرار من معلومات الحوالة بالتفصيل من خلال الاتصال هاتفياً مع الجهة المستفيدة قبل إرسالها .
- لا تقم بعمليات الشراء الإلكتروني إلا من المواقع الموثوقة بها عالمياً .
- تأكد دائماً من صحة الإعلان والجهة المعلنة قبل تنفيذ أية عملية دفع إلكتروني .
- تابع تقييمات العملاء حول المتجر الإلكتروني وحول معاملات الشراء نفسها.
- قم بقراءة مواصفات المنتج جيدًا ،وتأكد بأنها تطابق الصورة المعروضة .

- قم بقراءة شروط الخصوصية التابعة للموقع، وتأكد من خلوها من أي بند فيه أي انتهاك للبيانات والخصوصية.
- لا تتردد بطرح الأسئلة على فريق الدعم التابع لموقع الشراء الإلكتروني للتأكد من جودة البضاعة .
- احذر من المواقع ذات التصميم الرديء، والمحتوى الضعيف، والصور منخفضة الجودة، فهي في الغالب مواقع مزيفة أُنشئت لهدف مؤقت وهو استغلال الضحايا.
- ابتعد عن البائع الذي يصر على ضرورة الدفع الإلكتروني الفوري من دون توفير ضمانات الاسترجاع أو المعاينة .
- لن يقوم البنك أو أية شركة مصرفية بطلب معلوماتك الشخصية وحساباتك المصرفية عن طريق اتصال هاتفي بما في ذلك كلمات المرور .
- خذ وقتك بالبحث والتحري عن أية معاملات مالية أو

تجارية تعقدها عبر الإنترنت ،وافترض الأسوأ دائماً .

- تجاهل أية رسائل إلكترونية مشبوهة أو غير مألوفة بما فيها الرسائل الدعائية، ولا تتواصل إلا مع الجهات الموثوقة بها لديك .
- معلوماتك الشخصية سرية ومشاركتها عبر مواقع التواصل الاجتماعي تعرضك للاحتيال .
- احتفظ بنسخة احتياطية لبياناتك بشكل دوري .
- قم بدور المحقق عند تسوّقك على الإنترنت .
- احذر صفقات الربح السريع المغرية على الإنترنت وكن واقعياً في تفكيرك .



ثانياً : الابتزاز الإلكتروني

منفعة مادية أو جنسية أو سياسية أو اجتماعية .

الأساليب المستخدمة بالابتزاز:

- **كسب الثقة:** ويكون ذلك من خلال الاتصال مع الضحية عن طريق وسائل التواصل الاجتماعي، للحصول على المعلومات أو الصور ومقاطع الفيديو.
- **الاختراق أو ملفات خبيثة:** ويكون من خلال برامج أو ملفات يرسلها المبتز إلى جهاز الضحية للحصول على بياناته وملفاته، أو حتى إتلافها أو تشفيرها.

- **الإيهام بتقديم مساعدة أو الوعد بالزواج:** ويكون ذلك باستخدام

الوسائل السابقة بهدف الحصول على بيانات ومعلومات الضحية.

نصائح لتجنب الوقوع ضحية الابتزاز الإلكتروني:

- عدم قبول طلبات الصداقة المجهولة أو التواصل مع جهات غير معروفة لديك.
- لا تشارك معلومات حساسة أو صوراً أو فيديوهات مع أي شخص على شبكة الإنترنت، حتى ولو كانوا معروفين بالنسبة لك.
- الابتعاد عن المواقع والصفحات غير المعروفة لديك أو غير الآمنة، وإهمال التطبيقات أو المواقع غير المستخدمة.
- تحميل أو تنزيل التطبيقات والبرامج من المواقع الرسمية.
- تأمين حساباتك الشخصية على مواقع التواصل الاجتماعي.
- عدم الوثوق بالعلاقات الغرامية على مواقع التواصل الاجتماعي .

الإجراءات الواجب اتباعها حال تعرضك للابتزاز:

. لا تتواصل مع المبتز تحت أية ضغوط.

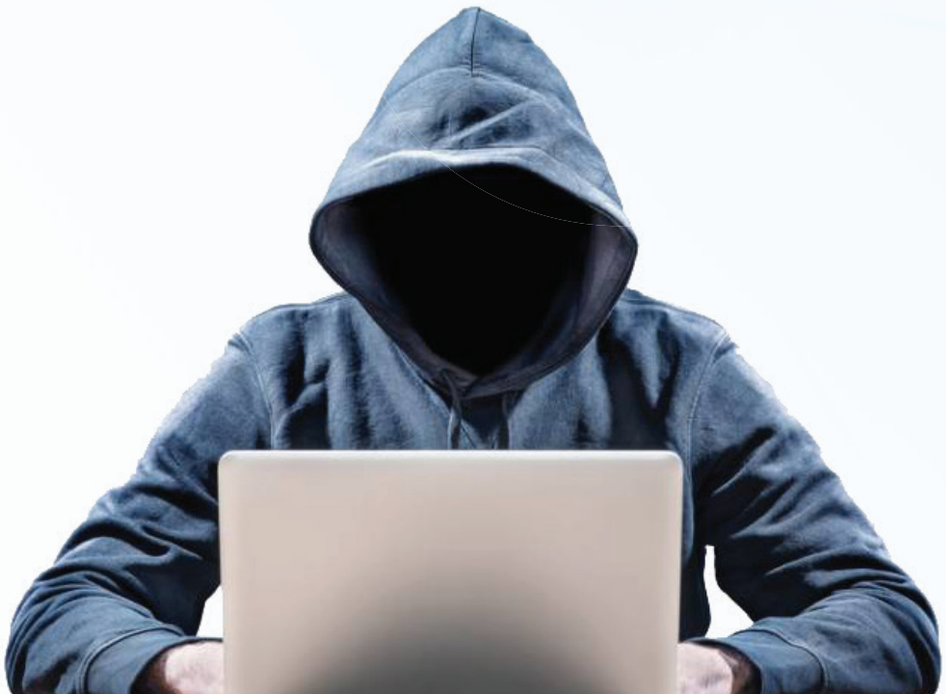
. لا تتجاوب مع طلبات المبتز ،وتأكد أنها لن تتوقف إذا قمت بالخضوع لها.

. حاول إخبار أحد أفراد عائلتك.

. قم بالتواصل مع الجهات الأمنية المعنية بأسرع وقت ممكن.

أشكال الابتزاز:

- تحرش جنسي.
- ابتزاز مالي.
- ابتزاز جنسي وعاطفي.
- استغلال العوز والحاجة .



ثالثاً: الاختراق وحماية الخصوصيـــة

أهم أساليب الحماية وتأمين الخصوصية :

- احـذر الروابـط الإلكترونيـة الوهميـة علـى مواقـع التواصـل الاجتماعـي والبريـد الإلكترونـي .
- حافـظ دائمـاً علـى تحميـل الإصـدار الأخيـر مـن البرمجيـات التـي تتعامـل معهـا .
- تأكـد دائمـاً مـن تفعيـل المصادقـة الثنائيـة، واسـتخدام كلمـات المـرور القويـة .

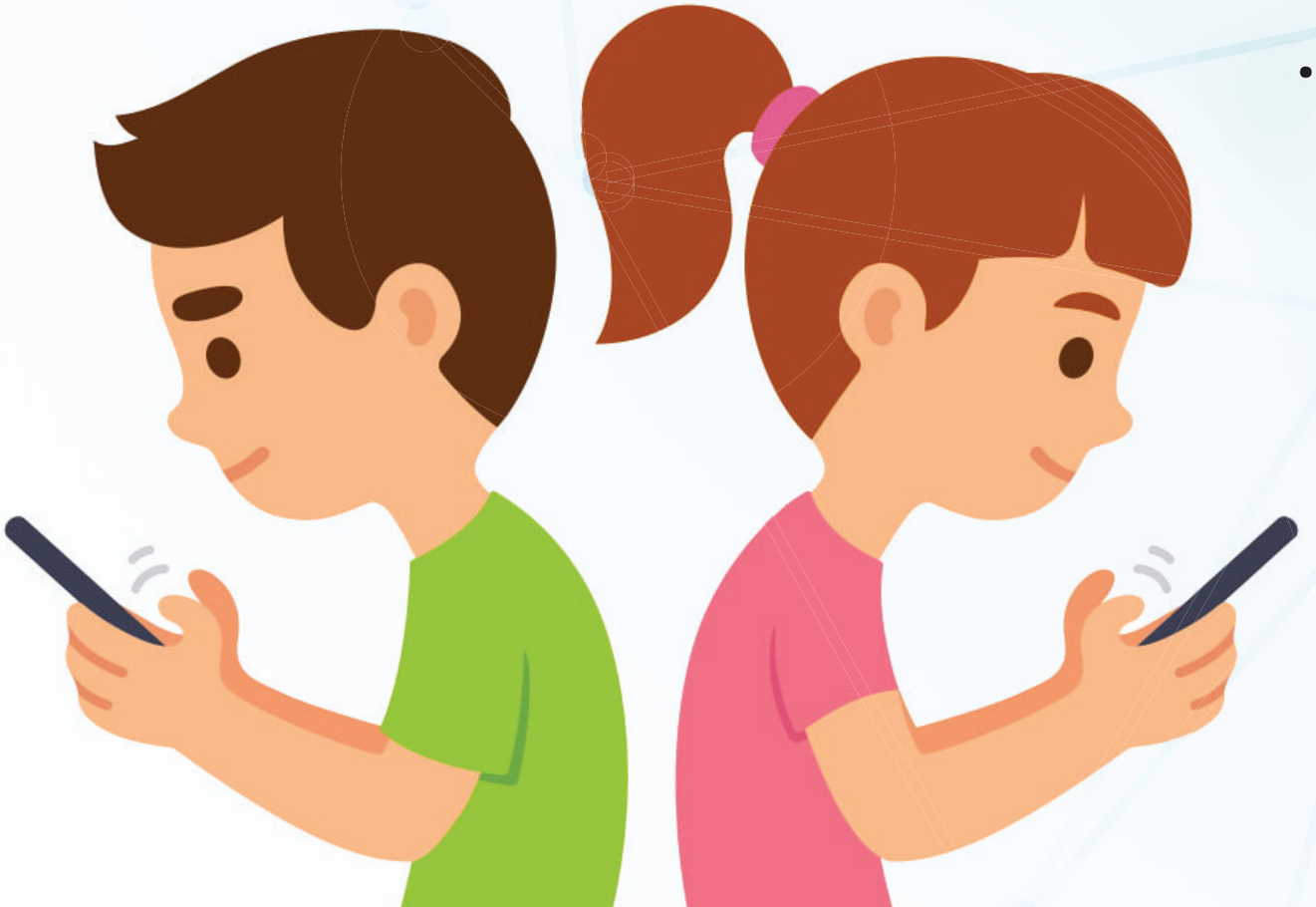
- عدم مشاركة المعلومات الشخصية التي تعرضنا لخطر الاختراق .
- الابتعاد عن شبكات (الواي فاي) المتاحة والمفتوحة .
- تجاهل الاتصالات الدولية من أرقام غريبة فقد تكون احتيالية .
- حافظ على استخدام برامج وتطبيقات الحماية المحدثة وتجنب تحميل التطبيقات من المصادر غير الموثوقة بها

رابعاً : مخاطر الألعاب الإلكترونية

الألعاب الإلكترونية لها العديد من المخاطر من أهمها :

- الألعاب الإلكترونية بيئة خصبة للعلاقات المشبوهة فلا تجعل أطفالك عرضة للاستغلال .
- لا تترك بطاقتك الائتمانية في يد أطفالك، وقم بنفسك بتنفيذ عمليات الشراء الإلكتروني على مواقع الألعاب الإلكترونية .

- لا تترك أبناءك وحدهم على منصات الألعاب الإلكترونية وشاركهم اهتماماتهم .
- إدارة الوقت لأبنائك على منصات الألعاب الإلكترونية يحمي صحتهم ويحميهم من ضعف التحصيل الدراسي .
- ابتعد بأبنائك عن الألعاب الإلكترونية العدوانية ،فهي تؤثر على سلوكهم وشخصياتهم .
- احمِ أبناءك من التنمر الإلكتروني على مواقع الألعاب الإلكترونية .



خامساً: حماية الأطفال عند استخدام الإنترنت

الشعارات :

- الإنترنت عالم مرعب لا تترك طفلك وحيداً معه
- ابنِ الثقة مع طفلك ،واجعله صديقاً لك .
- إدمان الألعاب الإلكترونية طريق للمجهول .
- كن أنت خط الدفاع الأول لطفلك .
- معاً نحو حماية أطفالنا من مخاطر الإنترنت .
- حماية أطفالنا مسؤوليتنا جميعاً .
- مراقبة طفلك هي الطريق لحمايته .

النصائح :

- كن واعياً، الإنترنت عالم غامض يحتوي بعض المواقع المناسبة لأطفالك ،والعديد من المواقع الخطرة عليهم .
- استمع لطفلك دائماً وكن قريباً منه؛ لأن حديثه سيكون متعلقاً بما يشاهده بشكل يومي على الإنترنت .
- احذر من الألعاب الإلكترونية التي يستخدمها طفلك ،والتي تمكنه من التواصل مع أشخاص غرباء من دون قيود ومحددات .
- تابع محتوى (اليوتيوب) الذي يشاهده طفلك، وكن مستمعاً جيداً لحديثه لتكون صديقه الأقرب الذي يلجأ إليه .

• استمر بسؤال طفلك عما يشاهد عبر الإنترنت وما هي اهتماماته لتتمكن من حمايته في حال مشاهدته لمواقع غير مناسبة لعمره .

• حدد وقتاً لمدة استخدام طفلك للإنترنت والألعاب الإلكترونية، لأن الوقت الطويل على الإنترنت يزيد من فرصة رؤية المحتويات غير المناسبة لطفلك .

• راقب طفلك أثناء استخدامه لمواقع التواصل الاجتماعي، حتى لا يقع ضحية لجريمة تهديد أو ابتزاز أو احتيال أو استغلال .

• وجه طفلك إلى المنصات الإلكترونية الآمنة المتوفرة على الإنترنت .

سادساً : التنمر الإلكتروني

آثار التنمر الإلكتروني على الضحية :

- ضعف الثقة بالنفس وعدم تقدير الذات.
- الانطواء وعدم الرغبة بالمشاركة في الحياة الاجتماعية.
- الاضطرابات النفسية والجسدية المتمثلة في الاكتئاب، والخوف والقلق والترقب، وفقدان الشهية وسوء التغذية التي تتطور لاحقاً إلى أمراض نفسية وجسدية.

• التشتت وفقدان التركيز مع تدني التحصيل العلمي وقد يصل أحياناً إلى ترك المدرسة.

• اللجوء إلى أشخاص أو أماكن لا يتعرض فيها إلى التنمر وقد تشكل خطراً عليه.

النصائح :

• ابنِ الثقة مع أبنائك واستمع إليهم ولا تكن أنت المتنمر عليهم.

• لا تقم بالرد على المتنمر، ولا تشعر بالخجل والإحراج من طلب المساعدة للتخلص من المشكلة .

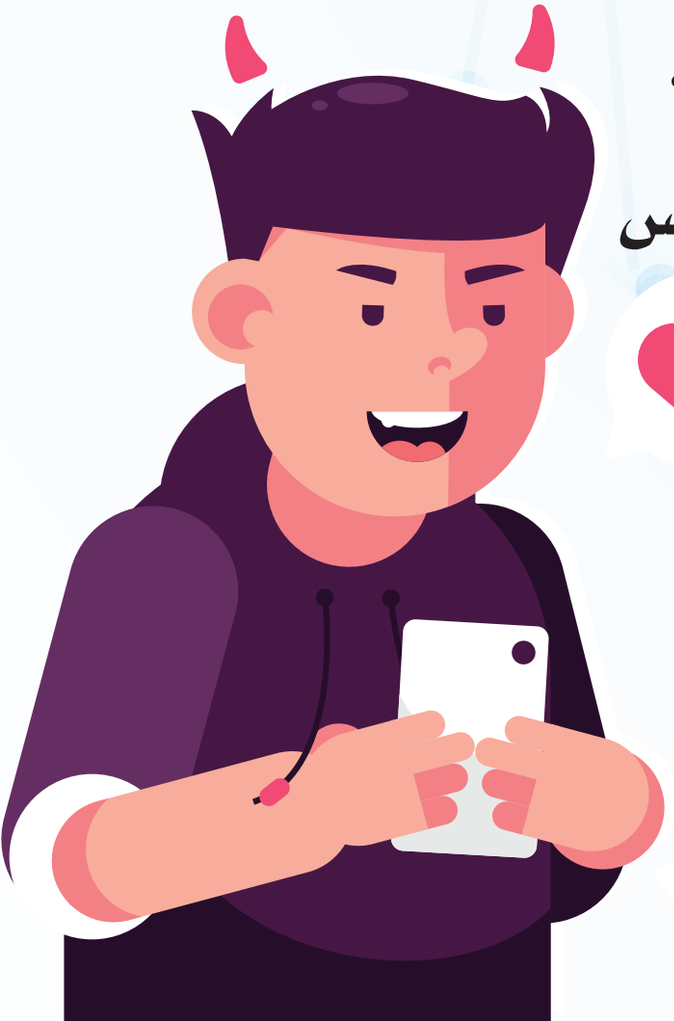
• لا تقم بالتعليق والتفاعل مع المحتوى المسيء وغير الأخلاقي عبر الإنترنت، حتى لا تعرض نفسك لخطر التنمر.

• احتفظ بلقطات شاشة لعملية التنمر لتقديمها كدليل للجهات الأمنية لحمايتك من المتنمر .

• لا تجعل معلومات ومحتويات حساباتك على مواقع التواصل الاجتماعي عامة ومتاحة للجميع .

• راقب تفاعل أطفالك مع مواقع التواصل الاجتماعي لتتمكن من حمايتهم من التنمر .

• كن حذراً في تعاملك مع الناس فالمشاكل النفسية والكراهية والحقد لدى البعض تؤدي بهم للتنمر على الناس .



عند التعرض لأي نوع من الجرائم الاتصال على الارقام التالية:

إدارة البحث الجنائي

الهاتف الخلوي: 0798518985

الرقم الأرضي: 064602430

البريد الإلكتروني: jenaee.dept@psd.gov.jo

نظام السيطرة (عميش) : 911

وحدة مكافحة الجرائم الإلكترونية:

الموقع : إدارة البحث الجنائي – عمان – العبدلي

رقم الهاتف: الرقم المجاني (196)

الفرعي رقم (812232-812594)

البريد الإلكتروني: cyber.crimes@psd.gov.jo

الصفحة الرسمية على موقع الفيس بوك

تم بحمد الله