

الأمن السيبراني

اعداد
أ.م.د. منى مجيد لفتة



ما لمقصود بالأمن السيبراني



ما هو الأمن السيبراني؟

الأمن السيبراني (CyberSecurity)

هو الجهد المستمر لحماية هذه الشبكات المتصلة بالشبكة وكافة البيانات من الاستخدام الغير مصرح (unauthorized) أو التلف (harm).



سايبير

معنى كلمة سايبير هي إلكتروني
إضافة كلمة سايبير إلى أي شيء آخر تعطيه معنى الإلكترونية مثل
cyber-security والتي تعني الأمن الإلكتروني
و *cyber-attack* والتي تعني الهجمات الإلكترونية
وهي تستخدم بمعنى "الفضاء الإلكتروني" أو فضاء الإنترنت.

الفرق بين أمن المعلومات والأمن السيبراني

على الرغم من التقاطع بين المجالين إلا أن هنالك نقاط اختلاف جوهرية بين المجالين.

• **الأمن السيبراني** يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا تهتم بذلك.

• **أمن المعلومات** يهتم بأمن المعلومات الفيزيائية "الورقية" بينما لا يهتم الأمن السيبراني بذلك.

الهدف من الأمن السيبراني





CIA

- السرية
- السلامة
- التوافر





ضمان توافر استمرارية عمل نظم المعلومات 

تعزيز حماية وسرية وخصوصية البيانات الشخصية 

اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة 

حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة 

تعزيز حماية أنظمة تقنية المعلومات 



تعزيز حماية الشبكات 

تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدم من خدمات،
وما تحويه من بيانات 

تحقيق الأمن السيبراني الشامل



٢٥ بليونون جهاز انترنت الأشياء متصل بالإنترنت في عام ٢٠٢٠ م 

١ يتم بحماية شبكات الاتصالات 

٢ شبكات المعلومات 

٣ أنظمة الحواسيب ذات الاستخدام العام 

٤ الانظمة المدمجة وما في حكمها 



تحقيق الامن السيبراني الشامل لحماية
ذوي الاحتياجات الخاصة 



المحتوى الغير أخلاقي

إدمان الإنترنت

الابتزاز

انتهاك الخصوصية

الأضرار الصحية

أبرز مخاطر
الفضاء
السيبراني

لتقنيات أكثر أمانا



المجرمون السيبرانيون (القراصنة)

- القراصنة المحترفون:
- هم مجموعة من المهاجمين المحترفين يتسللون إلى الجهاز أو الشبكة الضحية بهدف معين. يتم تقسيمهم حسب مقصدهم إلى ثلاثة أنواع



طرق إيقاف المجرمين والمهاجمين

السيبرانيون (حماية الأجهزة)

• ردع القرصنة: (الهجمات الإلكترونية)

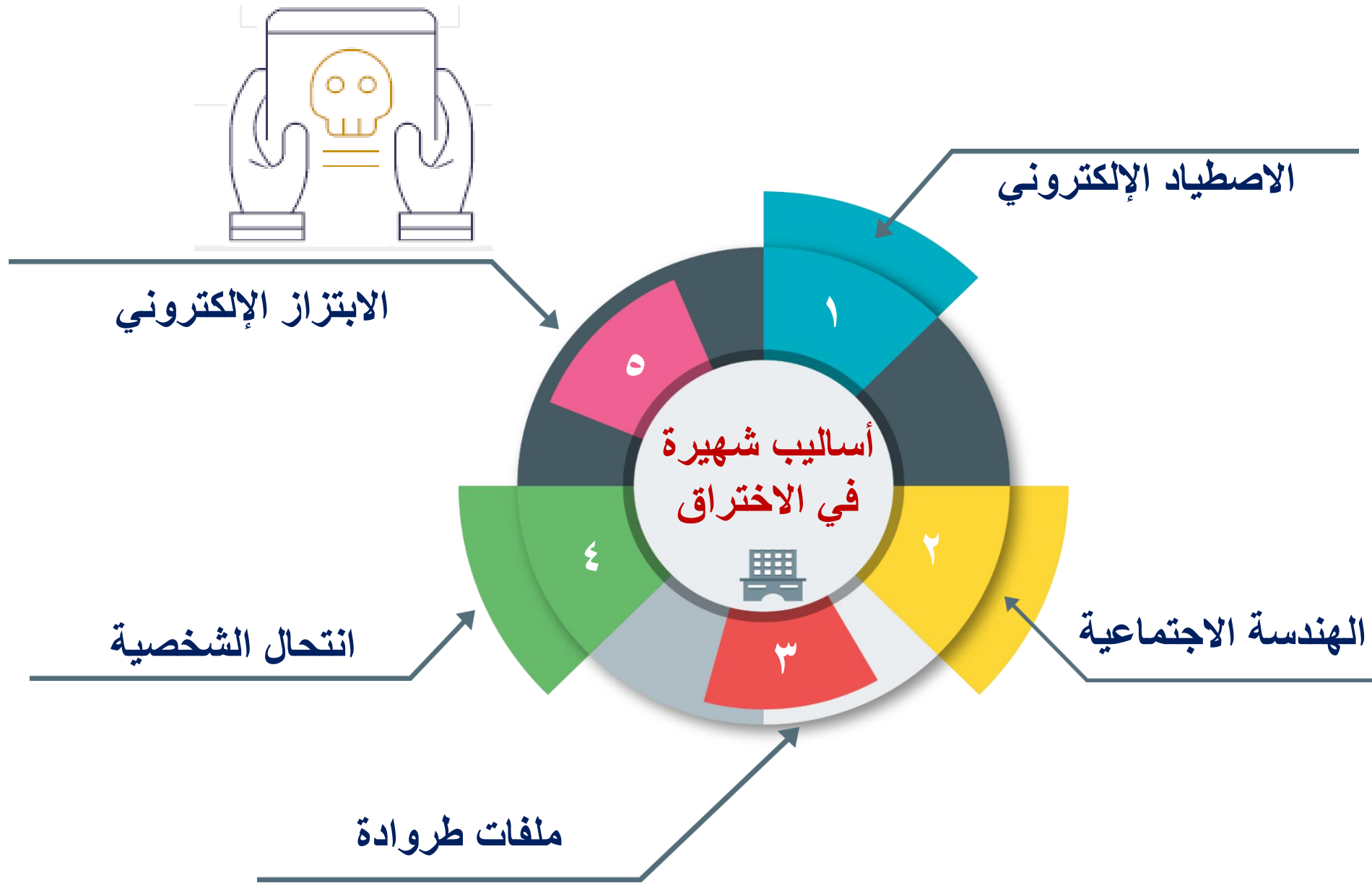
إيقاف المهاجمين والمجرمين السيبراني عمل شاق إذا لا توجد طريقة موحدة أو سلاح محدد لردعهم. وبرغم ذلك فالشركات والحكومات والمؤسسات الدولية.

بدأت في أخذ خطوات فعالة ومنظمة لتحجيم وإيقاف المجرمين

السيبرانيون. و فيما يلي نعرض تلك الجهود الدولية للحد من الإجرام السيبراني.

أساليب شهيرة في الاختراق وبعض نتائجها





١ سهولة الوقوع في فخ الاصطياد



٢ تتبع الروابط بدون تدقيق



يجب التأكد من مصدر الرابط

لا تقم بفتح روابط تصلك إلى بريدك لزيارة مواقع البنوك

قم بتهجئة العنوان قبل فتحه

عدم الوثوق بأي شخص مجهول في الفضاء الإلكتروني

احذر مواقع التصويتات التي تنتشر من فترة لأخرى

٤ تحميل البرامج غير الموثوقة



١ تأكد من تحميل البرامج من المتجر الرسمي سواء أندرويد أو أبل

٢ لا تثق بأي دعاية لأي برنامج إلا بعد قراءة التعليقات وتقييم المستخدمين له

٣ حمل ما تحتاج إليه فقط حدث البرامج والتطبيقات من حين لآخر

٤ كما أن هناك اصطياد في المواقع فهناك اصطياد في التطبيقات والفكرة واحدة (سرقة بياناتك)

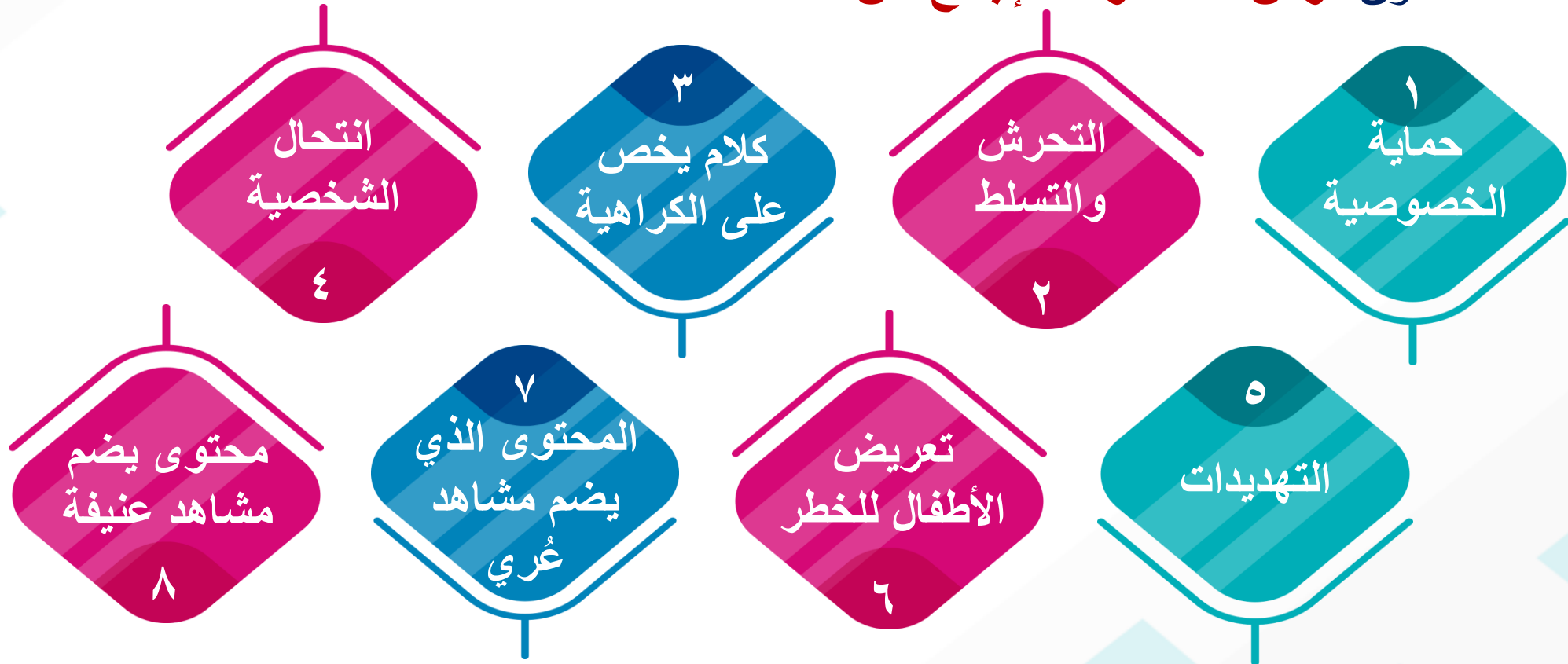
التعامل مع الإساءة في مواقع التواصل الاجتماعي



التعامل مع الإساءة في مواقع التواصل الاجتماعي



هل تعلم بأن موقع يوتيوب يوفر أدوات فعالة للإبلاغ عن الإساءات التي يتعرض لها المستخدمون، **ومن ذلك أدوات الإبلاغ عن**



سلوكي في الوسائط الإلكترونية يصنع تصورات الناس عني





أنواع الجرائم المعلوماتية



أنواع الجرائم المعلوماتية

جرائم الاعتداء على الحياة الخاصة



إفشاء الأسرار



السب والشتيم عبر الانترنت



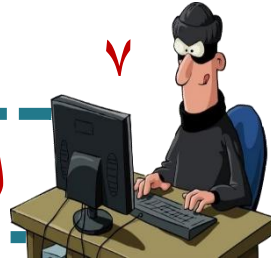
جريمة التنصت



الابتزاز والتهديد



التشهير بالأشخاص



جرائم إساءة استخدام الهواتف النقالة



الاستيلاء والاحتياال المعلوماتي



الانتحال والتغيرير



جريمة السطو على أموال البنوك



الجريمة المعلوماتية الأخلاقية
والاتجار بالبشر والاتجار بالمخدرات



التحريض على الجريمة المعلوماتية



الأمن السيبراني

