دورة تدريبية عن

المدرب د. محمد محمود أبوزيد

بنهاية هذه الدورة ستكون قادراً على أن:

- ✓ يحدد المقصود من الأمن السيبراني ومصطلحاته.
- ✓ يميز الفارق بين أمن المعلومات والأمن السيبراني.
- ✓ يذكر أهداف الأمن السيبراني.
- ✓ يذكر نشأة الأمن السيبراني في المملكة.
- ✓ يذكر الكيانات المعنية بالأمن السيبراني بالمملكة وأدوارها.
- ✓ يحدد معايير الأمن الشخصي في الفضاء السيبراني.
- ✓ يعدد تطبيقات تحقيق الأمن الشخصي السيبراني والاستفادة منها.
- ✓ يذكر الجرائم السيبرانية وطرق الحماية منها.

التعريف بالمصطلحات

السبرانية

مأخوذة من كلمة (سيبر) Cyber، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.

فالسيبرانية , تعني : (فضاء الانترنت)

الأمن السبراني

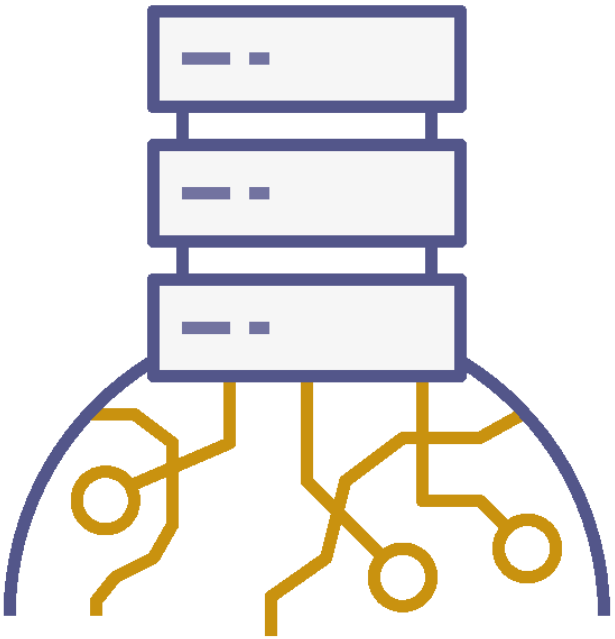
أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرّح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرّح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.

الأمن السيبراني :

- ✓ هو عبارة عن مجموع من الإجراءات التقنية والإدارية والتنظيمية التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات.
- ✓ كما يتضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين.
- ✓ كما يشمل ضمان استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف.

الفضاء السيبراني

«مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات، ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة»



وفي تعريف اخر

استخدام الفضاء السيبراني للدفاع أو الهجوم على المعلومات وشبكات الحاسب الآلي وحرمان العدو من تنفيذ نفس المقدرات

الفرق بين الأمن المعلوماتي والأمن السيبراني

الفرق بين الأمن المعلوماتي والأمن السيبراني

أمن المعلومات يهدف إلى

حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل.

يهـدف إلـى الحمايـة ضـد تعطيل خدمة المستخدمين الشرعيين

يُعنى أمن المعلومات بالوسـائل الضرورية لاكتشاف وتوثيق وصد كل هذه التهديدات.

أمن المعلومات يشمل كل ما من شـأنه حمايـة (المعلومة) التـي قـد تكـون فـي نظـام حاسوبي، أو قد لا تكون.

أمـن المعلومـات المظلـة الكبرى التـي تغطي كل الأفرع الأخـرى المرتبطـة بحمايـة البيانات والمعلومات وتأمينها.

أمـن المعلومـات يهتـم بمجـالات ضخمة، كالتشفير، والتخزين، والتأمين الفيزيائـي، والمعاييـر الأمنية، وإدارة أمن المعلومات والمخاطر..

الفرق بين الأمن المعلوماتي والأمن السيبراني

فأمن المعلومات والأمن السيبراني هما مصطلحان متشابهان، لكنهما ليسا متطابقَين

وأمـن المعلومـات بالتعريف هو أعم وأوسـع مـن الأمن السـيبراني. ولعل التخصيص هنا بالتركيز على مجال الأمن السيبراني، بوصفه مجالاً من مجالات العلم، هو أمر مفيد جدًّا؛ فعلم الحاسب وعلم التشفير - مثلاً - اشتُقّا أول ما اشـتُقّا من علم الرياضيات التطبيقية لأهميتهما، ثم ما لبثت هذه المجالات العلميـة أن حلقـت في فضـاء العلم الرحـب؛ لتتمدد، وتتوسـع، وتخرج خارج الأطـر العلميـة لمجالهـا الأب. وهـو الأمـر ذاتـه لمجـال الأمن السـيبراني.

الفرق بين الأمن المعلوماتي والأمن السيبراني

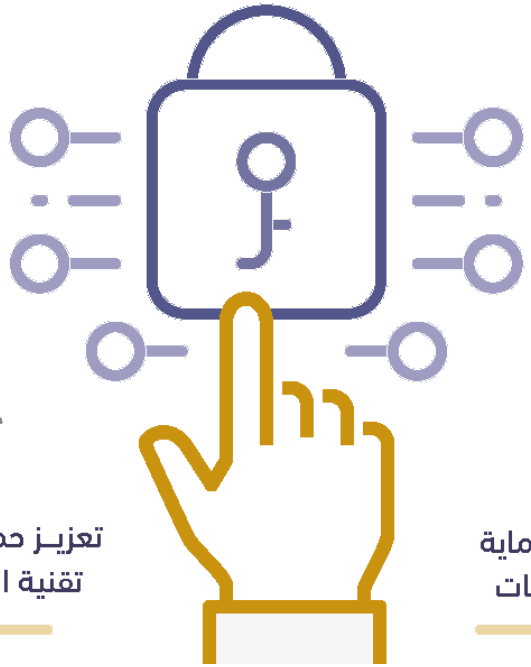
مفهوم الأمن السيبراني أوسع من أمن المعلومات، تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية، والتي يتم تخزينها في خوادم داخل أو خارج المنظمات من الاختراقات، وهذا هو أحد أهم الأسباب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني

الحرب الرقمية

الأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد، لا سيما أنّ الحرب السيبرانية أصبحت جزءًا لا يتجزأ من الأساليب الحديثة للحروب والهجمات بين الدول. نتذكر جميعًا الضجة الكبيرة التي أحدثها فيروس "شمعون" في المنطقة وخاصةً في المملكة العربية السعودية.

في عصر التكنولوجيا أصبح للأمن السيبراني الدور الأكبر في صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة

الهدف من الأمن السيبراني



- ضمان توافر استمرارية عمل نظم المعلومات
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة
- تعزيز حماية وسرية وخصوصية البيانات الشخصية
- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات
- حماية مصالح المملكة الحيوية وأمنها الوطني، والبنى التحتية الحساسة فيها
- التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال
- مراعاة الأهمية الحيوية المتزايدة لتخصصها
- تعزيز حماية الشبكات
- تعزيز حماية أنظمة تقنية المعلومات
- أن تكون المرجع الوطني للمملكة في شؤون تخصصها

تحقيق الأمن السيبراني الشامل

يتم بحماية شبكات
الاتصالات

شبكات
المعلومات

أنظمة الحواسيب
ذات الاستخدام العام

الانظمة المدمجة
ومافي حكمها

تحديـات وكابـوس مخيـف للمختصين فـي مجال الأمن السـيبراني يقابلـة ابتهاج
واحتفال بفرائس سمينة وسهلة في غابات وحقول الفضاء السيبراني

النشأة القانونية للأمن السيبراني

النشأة القانونية للأمن السيبراني

١١ صفر ١٤٣٩هـ الموافق ٣١ أكتوبر ٢٠١٧م

صدر أمر ملكي كريم برقم (٦٨٠١) وتاريخ ١٤٣٩/٢/١١هـ إنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) ترتبط بمقام خادم الحرمين الشريفين- أيده الله -، والموافقة على تنظيمها.

وهي الجهة المختصة في المملكة بالأمن السيبراني والمرجع الوطني في شؤونه بهدف

- تعزيز الأمن السيبراني للدولة
- حماية مصالحها الحيوية
- وأمنها الوطني
- والبنى التحتية الحساسة فيها

النشأة القانونية للأمن السيبراني

بأمر ملكي كريم رقم ٦٨٠١
تاريخ ١٤٣٩/٢/١١هـ
هيئة وطنية لحماية أمننا السيبراني

يرأسها الدكتور **مساعد بن محمد العيبان**
وزير الدولة وعضو مجلس الوزراء

أعضاء مجلس إدارة الهيئة الوطنية للأمن السيبراني

- رئيس أمن الدولة
- رئيس الاستخبارات العامة
- نائب وزير الداخلية
- مساعد وزير الدفاع

اختصاصات الهيئة

- حماية الشبكات
- تعزيز أنظمة تقنية المعلومات
- تعزيز أنظمة التقنيات التشغيلية ومكوناتها

يهدف عمل الهيئة إلى

- تعزيز الأمن السرياني للدولة
- حماية مصالح المملكة الحيوية
- حماية آمن المملكة الوطني
- حماية البنى التحتية الحساسة في المملكة

- استقطاب الكوادر الوطنية وتأهيلها
- بناء الشراكات مع الجهات العامة والخاصة
- تحفيز الإبتكار والاستثمار في مجال الأمن السيبراني
- الإسهام في تحقيق نهضة تقنية تخدم مستقبل الاقتصاد الوطني للمملكة

الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

النشأة القانونية للأمن السيبراني

اعتمـد رئيـس الهيئة العامـة للرياضـة تركي آل الشـيخ أول مجلـس إدارة للاتحاد السـعودي للأمن السـيبراني والبرمجة

سعود بن عبدالله القحطاني
رئيساً

أ.د. عبدالله بن شرف الغامدي
نائباً

وبعضوية كل من

أيمن السياري | د. عاصم الوقيت | خالد الثبيتي | د. غسان الشبل | فيصل الخميسي

عبدالرحمن الشتوي | د. معاذ الخلف | ديمة اليحيى | العنود الشهري | عبدالعزيز الدوسري

عن الاتحاد

منظمـة وطنيـة تحـت مظلـة
اللجنة الأولمبية السعودية

الاتحاد السعودي للأمن السيبراني والبرمجة
Saudi Federation for Cyber Security and Programming

يهـدف لإيصـال السـعودية إلى مصـاف الـدول المتقدمـة فـي صناعة المعرفة التقنية الحديثة

يسعى لبناء قدرات محلية واحترافية في مجال الأمن السيبراني والبرمجة بناءً على أفضـل الممارسـات والمعايـير العالميـة

الاتحاد السعودي
للأمن السيبراني
والبرمجة

Saudi Federation
for Cyber Security
and Programming

مجالات استخدام الإنترنت

- تعليم
- ابتكار
- هوايات
- ترفيه
- عمل
- تجارة

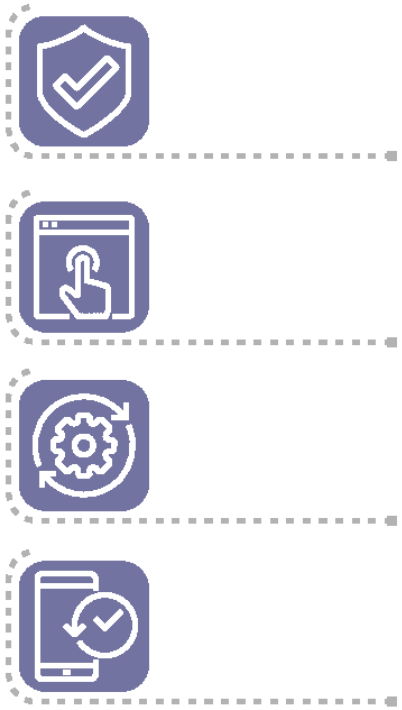
أبرز مخاطر استخدام الإنترنت

لإنترنت أكثر أماناً

إن معرفة سُبل حماية خصوصية معلوماتك وأجهزتك أثناء استخدامك للإنترنت يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع، والذي يلحق الضرر بك مادياً أو معنوياً

الجهاز الشخصي

محافظة منك على أمن جهازك وملفاتك الشخصية قم بالتالي

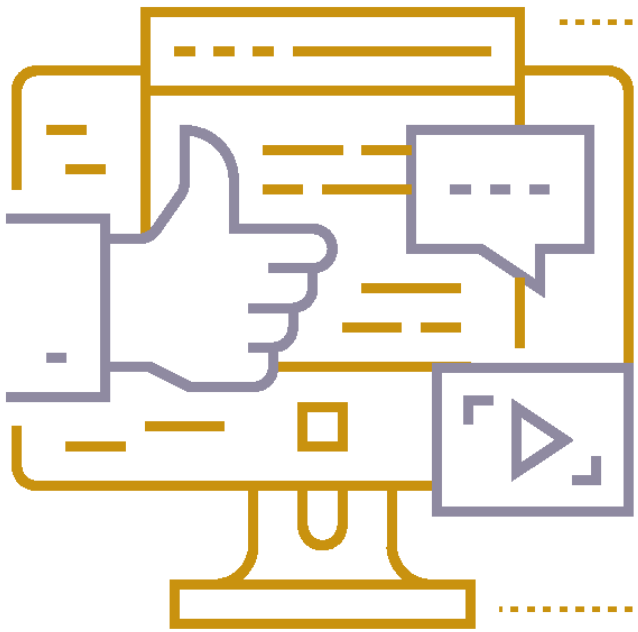


الجهاز الشخصي

محافظة منك على أمن جهازك وملفاتك الشخصية قم بالتالي

- تركيب برامج مكافحة الفيروسات والحرص على تحديثها وفحص الجهاز بشكل دوري
- الحذر عند الاتصال بالشبكات اللاسلكية العامة
- المداومة على تحديث نظام التشغيل والتطبيقات
- الاحتفاظ بنسخة احتياطية

استعادة السيطرة بعد اختراق - الجهاز الشخصي



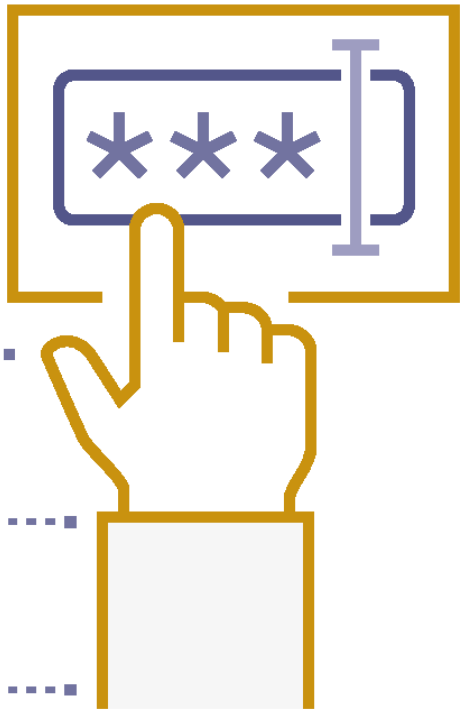
- فصل جهازك من الإنترنت حتى يُفصل الرابط بينك وبين المخترق
- إعادة تهيئة الجهاز
- تثبيت برامج حماية الفايروسات و إجراء فحص شامل للجهاز
- استعادة البيانات والمعلومات من النسخ الاحتياطية

كلمة المرور

كلمة المرور

طرق اختيار كلمة المرور

- اختيـار كلمـة مرور قويـة تحتوي علـى مجموعة من الاحرف والأرقام و الرموز
- استخدام كلمة مرور مستقلة لكل حساب
- عدم اختيار كلمة مرور مبنية على معلومات شخصية
- عدم مشاركتها
- تغييرها بشكل دوري



البريد الإلكتروني

حماية البريد الالكتروني

البريد الإلكتروني

حماية البريد الالكتروني

- وضع كلمات مرور قوية و تفعيل التحقق الثنائي
- عدم فتح المرفقات من مصدر مجهول
- تفادي الوقوع ضحية للرسائل الاحتيالية
- تخصيص بريد خاص للاستخدامات الرسمية والهامة

التحقق الثنائي لبرنامج WhatsApp

لتأمين برنامج WhatsApp من الاختراق

نفتح البرنامج

اضغط على الإعدادات
في الأسفل

اختر الحساب

ثم نختار التحقق بخطوتين

نفعل الخاصية عن طريق
الضغط على (تمكين)

يتم إدخال رقم
سري للبرنامج

أدخل البريد الإلكتروني
الخاص بك

تم تأمين الحساب بنجاح

سيطلب منك إدخال الرقم السري
لاحقا وفي أوقات مختلفة للتأكيد

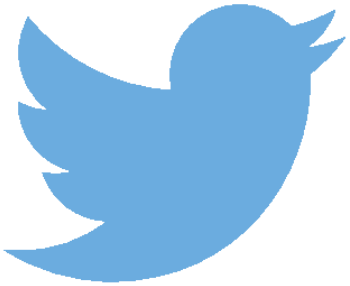
الإبلاغ عن الإساءة – تويتر

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية:

- انتحال الشخصية
- انتهاك حقوق النضر والملكية الفكرية.
- انتهاك الخصوصية.
- السلوك العنيف والتهديدات.
- الإساءة أو الرسائل المزعجة أو الترويج
- للبرمجيات الخبيثة.
- الإباحية.



٢ أدوات الإبلاغ

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

- انتحال الشخصية.
- انتهاك حقوق الملكية.
- بيع أو ترويج السلع المقلدة.
- انتهاك الخصوصية.
- الاستغلال الجنسي للأطفال.
- الإباحية.
- الإساءة أو التهديد.
- الرسائل المزعجة أو إساءة الاستخدام.
- مخالفة قوانين الاعلانات على الموقع.

هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://help.twitter.com/ar

الإبلاغ عن الإساءة – سناب تشات

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : الموقع يشترط أن تبلغ من العمر ١٣ عاماً لتكون مؤهلاً لاستخدامه؟

المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية

- انتهاك الخصوصية.
- انتهاك الحقوق التجارية، الملكية أو النشر
- الإساءة، المضايقة، التهديد أو التشهير.
- الإباحية.
- العنف أو الكراهية
- الرسائل المزجة، الفيروسات، البرمجيات
- الخبيثة أو تعريض الخدمة للاختراق.

٢ أدوات الإبلاغ

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

- الإساءة أو المسائل المتعلقة بالأمان أو بالمحتوى غير الملائم.
- الرسائل المزعجة.
- إنتحال الشخصية.

هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://support.snapchat.com

الإبلاغ عن الإساءة – انستغرام

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : الموقع يشترط أن تبلغ من العمر ١٣ عاماً لتكون مؤهلاً لاستخدامه؟
المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية

- انتحال الشخصية
- العنصرية، الكراهية أو السلوك العنيف.
- انتهاك حقوق الملكية.
- انتهاك الخصوصية.
- الإساءة المضايقة أو التهديد.
- القري أو الإباحية.

٢ أدوات الإبلاغ

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

- الحسابات المخترقة.
- إنتحال الشخصية.
- الأطفال دون السن القانونية.
- العنصرية، الكراهية أو السلوك العنيف.
- إنتهاك حقوق الملكية.
- إنتهاك الخصوصية.
- إيذاء الذات.
- الإساءة، المضايقة أو التهديد.
- الفري أو الإباحية.

هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://help.instagram.com

الإبلاغ عن الإساءة – يوتيوب

١ سياسة المحتوى وشروط الاستخدام

هل اطلت بعناية على سياسة الخصوصية وشروط الاستخدام للموقع حتى تتمكن من استخدام الموقع بشكل ممتع وآمن؟

هل تعلم بأن : المحتويات التالية تعد مخالفة لسياسة المحتوى لدى الموقع. وربما يقع صاحبها تحت طائلة المسائلة القانونية:

- انتحال الشخصية
- انتهاك الخصوصية.
- التهديدات.
- تعريض الأطفال للخطر.
- المحتوى الذي يضم مشاهد عُري ومشاهد جنسية.
- محتوى يضم مشاهد عنيفة أو قاسية.

٢ أدوات الإبلاغ

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

- حماية الخصوصية.
- التحرش والتسلط بر الإنترت
- كلام يخص على الكراهية.
- إنتحال الشخصية التهديدات.
- تعريض الأطفال للخطر.
- المحتوى الذي يضم مشاهد عُري ومشاهد جنسية.
- محتوى يضم مشاهد عنيفة أو قاسية.

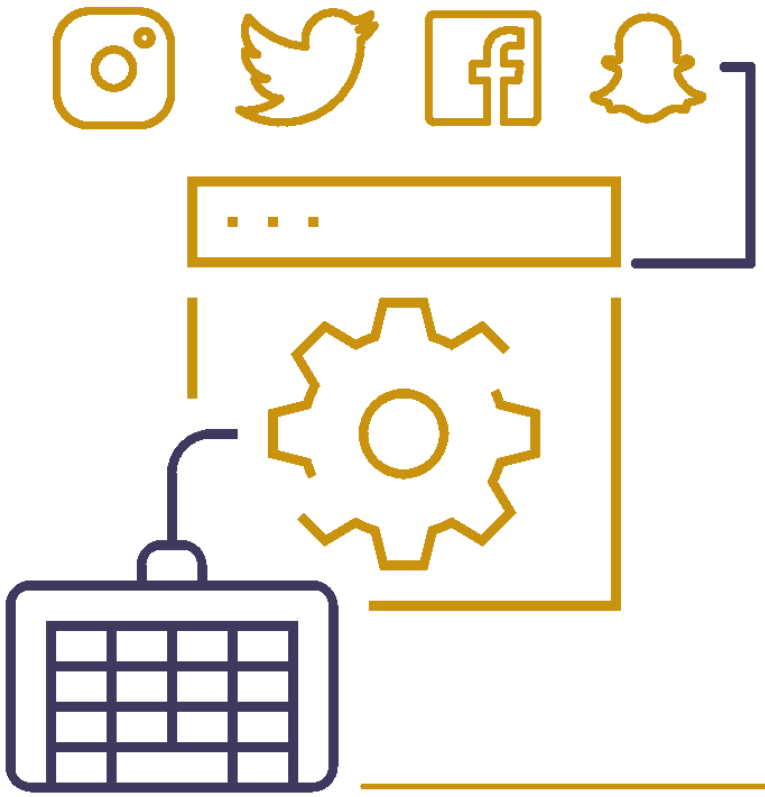
هل سبق وتواصلت مع الموقع للإبلاغ عن إساءة تعرضت لها ؟

تواصلت مع الموقع بشكل مباشر يساعدك على التخلص سريعاً من مصدر الإساءة بشكل صحيح، وربما لمنع المسيئ من الإساءة إلى آخرين أيضاً

- من المهم تحري الدقة عند تعبئة المعلومات المطلوبة في نموذج الإبلاغ.
- تحرص الكثير من المواقع على معالجة شكاوى مستخدميها بفعالية واهتمام.
- يعتبر الكثير من المواقع عدم إبلاغ المستخدمين عن شكاويهم بمثابة دليل على رضاهم وعلى خلو تلك المواقع من المخالفات.

زيارة الرابط التالي: https://www.youtube.com/reportabuse

استعادة السيطرة بعد الاختراق - حسابات مواقع التواصل الاجتماعي



استعمال جهاز اخر للدخول إلى حساباتك الشخصية وتغيير كلمات المرور.

في حال عدم تمكنك من الدخول للبريد الالكتروني الخاص بجهازك الذكي أو البريد الالكتروني الخاص بحسابات التواصل الاجتماعي؛ يمكن استعادته باستخدام خاصية نسيان كلمة المرور، ويمكنك في هذه الحالة الاستفادة من عنوان البريد الثانوي (الاحتياطي).

في حال عدم تمكنك من استعادة حساب التواصل الاجتماعي أو البريد الالكتروني يجب التواصل مع الدعم الفني الخاص بالجهة الموفرة للحساب.

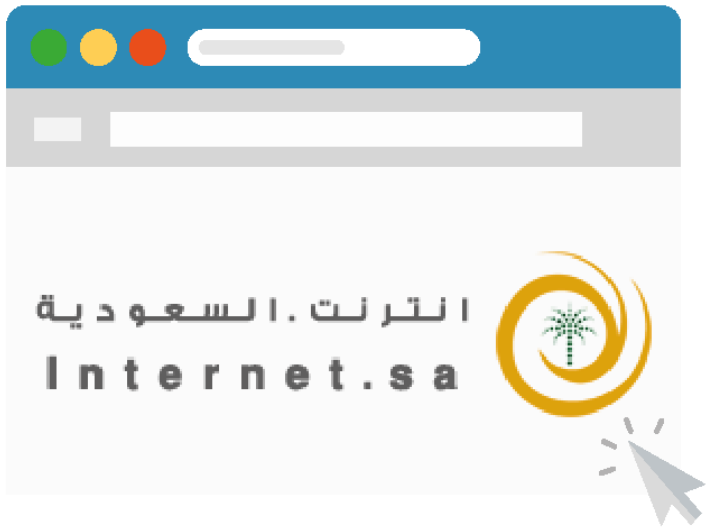
الإبلاغ عن الإساءة

الدليل الإرشادي

كيفيـة التعامل مع إسـاءة الاسـتخدام
فـي بعض مواقع الشـبكات الإجتماعية

من خلال موقع انترنت السعودية

www.internet.sa



الإبلاغ عن الإساءة – خدمة الترشيح

للإبـلاغ عـن المواقـع والمـواد التـي تتنافـى مـع الديـن الحنيف
والأنظمـة الوطنية يمكن طلب حجبها، مـن خلال القنوات التالية:

موقع ترشيح السعودية	تطبيق ترشيح السعودية	البريد الإلكتروني	الهاتف
www.filter.sa	البحث في متاجر الايفون والأندرويد	block@internet.gove.sa	011 - 4619485

الإبلاغ عن الإساءة – تطبيق خدمة الترشيح

خطوات طلب حجب أو رفع حجب المواقع الإلكترونية من خلال تطبيق (ترشيح.السعودية)

لتحميل تطبيق (ترشيح.السعودية)
من المتجر الخاص بجهازك

Google play

App Store

١ استخدام خاصية المشاركة المتوفرة في الأجهزة الذكية

٢ اختر خدمة الترشيح المطلوبة (طلب حجب، طلب رفع حجب)

٣ تعبئة النموذج الخاص بخدمة الترشيح المطلوبة

٤ معالجة الطلب من قبل الفريق المختص

لا تشترط خدمة الترشيح الوطنية أي معلومات خاصة من مقدمي طلبات الحجب

ماهو مقياس؟

عبارة عن منظومة أدوات لقياس واختبار جودة الإنترنت بغرض تزويد مستخدمي الإنترنت في المملكة

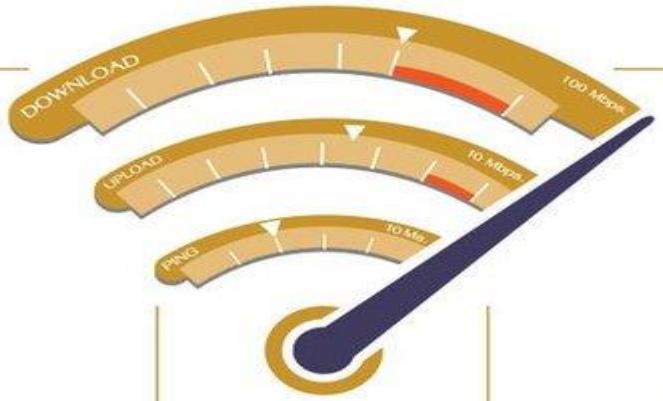
وهذه المنظومة مبنية على معايير موثقة ومطبقة في عدد من دول العالم مثل أمريكا وبريطانيا وسنغافورة والبرازيل.

وتتكون من الأدوات التالية

- موقع إلكتروني، لقياس سرعة الإنترنت من أجهزة الحاسب
- تطبيق للأجهزة الذكية، لقياس خدمة الإنترنت المتنقل
- أجهزة لقياس خدمة الإنترنت الثابت

ماذا يقيس مقياس؟

ماذا يقدم مقياس لمستخدمي الإنترنت؟



توفير معلومات دقيقة حول جودة تجربة الإنترنت لدى المستخدم

نشر تقارير دورية حول تجربة الإنترنت في المملكة

توفير معدل قياسات جودة تجربة الإنترنت للمستخدم على فترات زمنية مختلفة (يوم، أسبوع، شهر، سنة)

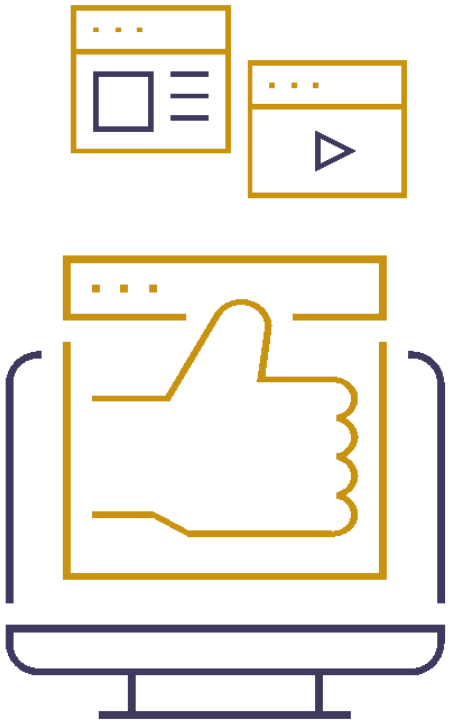
زيادة الشفافية والمنافسة بين مقدمي الخدمة

قياس التجربة لبعض خدمات ومحتوى الإنترنت الشائع في المملكة

سلوكي في الفضاء الإلكتروني يصنع تصورات الناس عني

- المعرفات الشخصية على وسائل التواصل
- المواقع والقنوات التي أشترك فيها
- الأشخاص الذين يتابعونني
- الأشخاص الذين أتابعهم
- الأجهزة الشخصية التي أستخدمها

كيف أكون انطباع إيجابي عن نفسي في الفضاء الإلكتروني



المعرفات الشخصية على وسائل التواصل

- المعرف يفضل أن يكون حقيقيا لحماية نفسك.
- عـدم التهـاون أبدا في إعطاء المعرف لأحـد مهما كان (عند الشباب).
- حماية المعرف بكلمة مرور قوية.
- التأكـد من وجود طرق آمنة لاسـتعادة المعرف حال سـرقته مثـلا التصديـق الثنائي، أو ربطه برقم جوال لاسـتعادة كلمة المرور.

المواقع والقنوات التي أشترك فيها

- مـن خـلال القنـوات المشـترك فيها يتحـدد الانطبـاع العام حولـك، فكـن على حذر مـن القنوات المشـبوهة أو الكيانات الوهمية والغير موثوقة، مثل:
- القنوات الإباحية
- قنوات التفحيط
- قنوات أجنبية عدائية
- قنوات مجهولة الهوية ولو كانت دينية أو هادفة في البداية

كيف أكون انطباع إيجابي عن نفسي في الفضاء الإلكتروني

الأجهزة الشخصية

الجهاز الشخصي يحتوي على معرفاتك عادة على وسائل التواصل، التفريط في الجهاز أو لو طلبك أحد الجهاز الخاص بك لإجراء مكالمة أو إرسال رسالة يجب أن تعتذر بدون تردد، لأنه قد ينتحل شخصيتك ويسيء لأحد باستخدام جوالك.

الأشخاص الذين يتابعوني

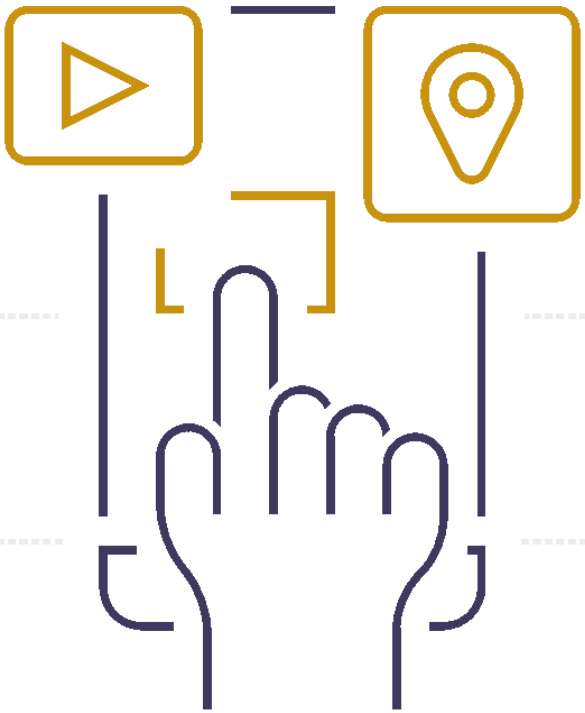
تستطيع التحكم في متابعيك أيضا، فلو تابعك حساب مشبوه أو حساب إباحي أو مجهول الهوية بإمكانك حظره مباشرة. (أحيانا يتم اللجوء لحماية الحساب)

الأشخاص الذين أتابعهم

قل لي من تتابع أقل لك من أنت – بالإمكان تحديد بعض معالم شخصيتك من خلال الأشخاص الذين تتابعهم، لذلك يجب أن تختار من تتابع بعناية، وتجنب متابعة المجاهيل، مثال:

حساب ينشر نصائح ووصل عدد متابعية عشرات الآلاف وبعد فترة غير الشعار والحساب، وأصبح يعمل لصالح مجموعات إرهابية

من أخطاء المستخدمين



سهولة الوقوع في فخ التصيد الإلكتروني أو انتحال الشخصية

تحميل برامج غير موثوقة

تتبع الروابط بدون تدقيق

أخطاء في إدارة كلمات المرور

الاسترسال في تتبع الروابط والوصلات الدعائية

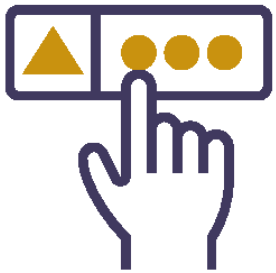
أخطاء في استخدام وسائل التواصل الاجتماعي

من أخطاء المستخدمين

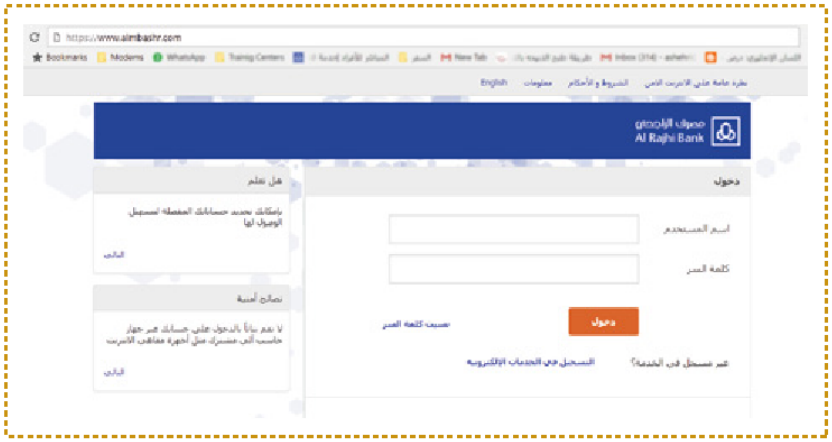
سهولة الوقوع
في فخ الاصطياد

ماهو الاصطياد الإلكتروني؟

استغلال وسائل تقنية المعلومات لمحاولة خداع الضحية للكشف عن معلوماته السرية مثل كلمات السر الخاصة به أو معلومات حسابه المصرفي.



(كيف أعرف)



المواقع الموثوقه & المواقع المشبوهه

عنوان الموقع Domain Name

المواقع المشبوهه & المواقع الموثوقه

هيئة الموقع وتصميمه

- ✓التصاميم والشعارات والصور.
- ✓الصياغة اللغوية والترجمات.
- ✓صفحة بيانات التواصل.

المواقع المشبوهه & المواقع الموثوقه

استخدام مواقع مراجعة وفحص المواقع الأخرى

- URLVoid.com
- VirusTotal.com
- ScamAdviser.com
- MyWOT (Web of Trust)
- NetCraft.com

من أخطاء المستخدمين

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.

الاسترسال في تتبع الروابط والوصلات الدعائية

- يجب أن يكون هناك ثقافة تجاهل الإعلانات.
- كثير من البرمجيات الخبيثة تتسلل عن طريق الإعلانات.

من أخطاء المستخدمين

تحميل البرامج غير الموثوقة

- تأكد من تحميل البرامج من المتجر الرسمي سواء أندرويد أو أبل.
- لاتثـق بـأي دعايـة لأي برنامـج إلا بعـد قـراءة التعليقـات وتقييم المستخدمين له.
- حمل ما تحتاج إليه فقط.
- حدث البرامج والتطبيقات من حين لآخر
- كمـا أن هنـاك اصطيـاد في المواقـع فهنـاك اصطياد في التطبيقات والفكرة واحدة (سرقة بياناتك)

أخطاء في إدارة كلمات المرور

- كلمة المرور (سرية لك وحدك)
- يجب أن تكون كلمة المرور معقدة بشـكل كاف يمنع برامج التخمين من اكتشافها.
- نوع كلمات المرور ولا تجعلها متطابقة.
- لا تكتب كلمة المرور مطلقا قريبا من جهازك أو في جيبك .
- تجنب كلمات المرور المرتبطة بمناسبة معروفة لديك، مثل تاريخ الميلاد أو الزواج أو رقم الجوال ...الخ
- قم بتغيير كلمة المرور من حين لآخر.

أساليب شهيرة في الاختراق وبعض نتائجها (هجومية من المخترقين)

الهندسة الاجتماعية

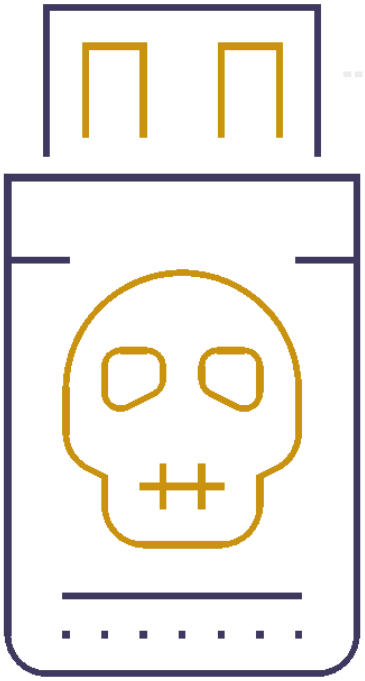
ملفات طروادة

الاصطياد الإلكتروني

الابتزاز الإلكتروني

انتحال الشخصية

أساليب شهيرة في الاختراق



الاصطياد الإلكتروني	سبق الكلام عليه
الهندسة الاجتماعية	التحايل على المستخدم بغرض الحصول على معلومات المفترض ألا يفشيها
ملفات طروادة	ملف يصلك ويبدو طبيعيا بينما هو عبارة عن برنامج خبيث
انتحال الشخصية	تقمص شخصية أحد المشاهير أو الأقارب للحصول على معلومات من المفترض ألا تقوم بإفشائها
الابتزاز الإلكتروني	الحصول على معلومة أو مادة أو صورة إما طوعاً أو عن طريق الهجوم على جهاز الضحية ثم استخدامها ضده مقابل الحصول على مال

الخصوصية في الفضاء الإليكتروني

تصنيف المعلومات الشخصية في الشبكات

معلومات عامة

معلومات خاصة

معلومات عائلية

معلومات محظورة

تصنيف المعلومات الشخصية في الفضاء الإلكتروني

معلومات عامة

الجميع يعرفها (بداية عطلة – أعياد - ..الخ)

معلومات خاصة

(السفر – النشاط اليومي - أماكن التواجد لحظياً ... ؟)

معلومات عائلية

(الهدايا العائلية – الوجبات – حفلات داخل البيوت ... ؟)

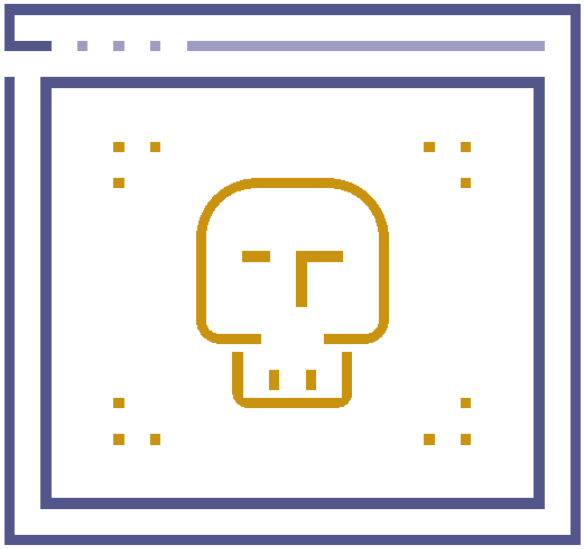
معلومات محظورة

بيانات الهوية الشخصية : (رقم السجل المدني – رقم الإقامة – الحسابات بطاقات البنوك) – جهات الاتصال (NumberBook) – الخطابات السرية

الجرائم السيبرانية

هـي السـلوك غيـر المشـروع أو المنافـي للأخـلاق أو غير المسـموح بـه المرتبـط بالشـبكات المعلوماتيـة العالميـة

فهي جرائم العصر الرقمي التي تطال



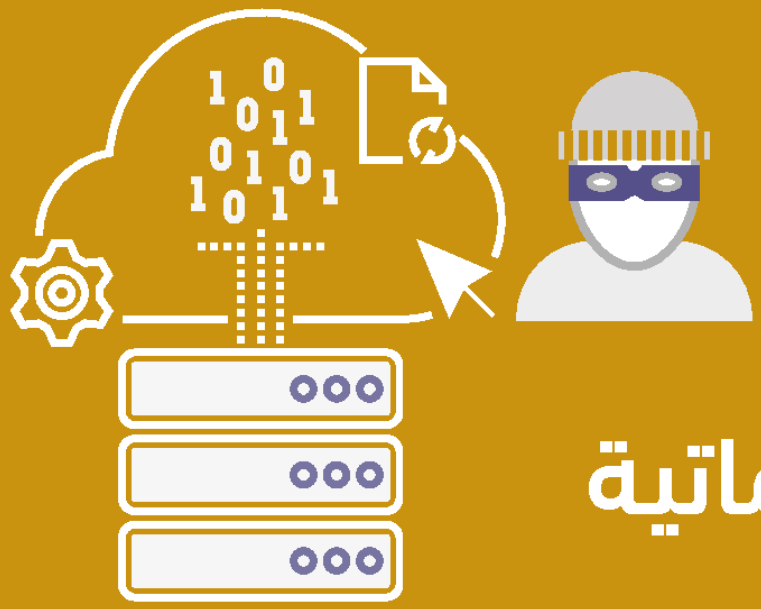
الثقة

المعرفة

المال

السمعه

وهي كلها تنفذ عن طريق التقنية



أنواع الجرائم المعلوماتية

أنواع الجرائم المعلوماتية

1 جرائم الاعتداء على الحياة الخاصة

الحق في الخصوصية هو أحد الحقوق اللصيقة الثابتة للإنسان

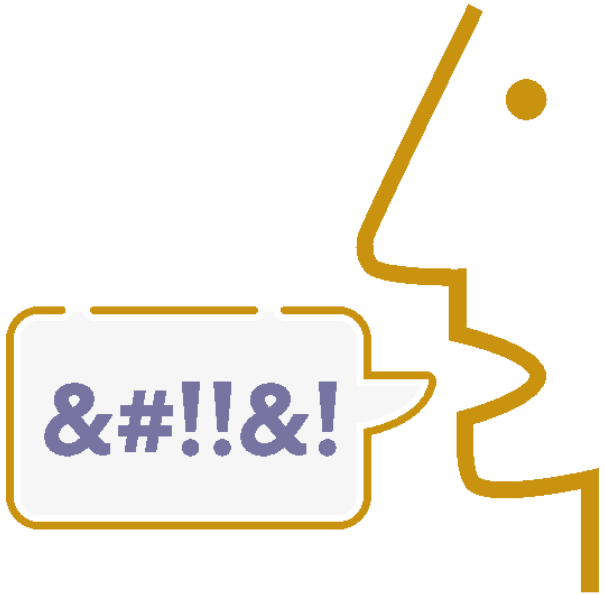
والمقصود من الحياة الخاصة

ما يقوم به الشخص ولا يرتضي أن يطلع عليه الغير, واعتاد الناس على أن هذا الحق من الخصوصية للشخص.

أنواع الجرائم المعلوماتية

2 السب والشتم عبر الانترنت

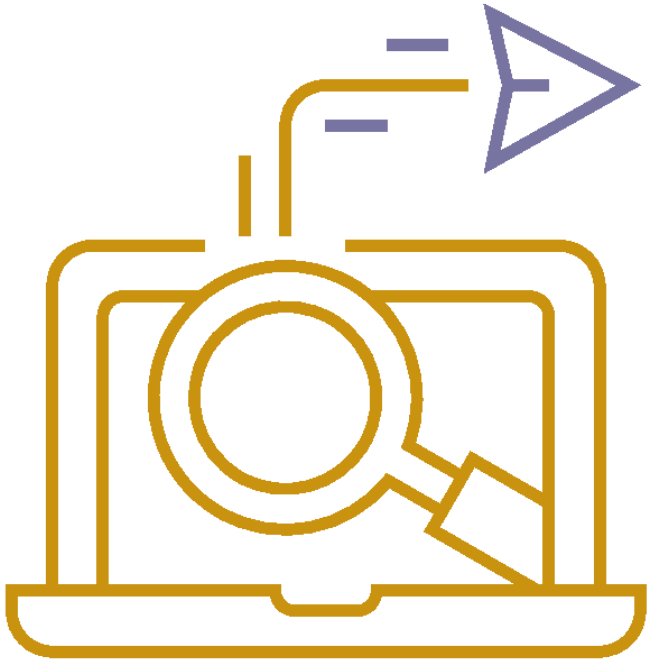
الشتم وهو كل قبيح اعتاد الناس قبحه وسوؤه فتجد بعض المتعاملين بشبكات المعلومات العالمية , يستسهل السب للآخرين وذلك راجع للأسباب التالية :



١ أن غالب من يرتكب ذلك يختفي وراء أسباب وهمية فيأمن العقوبة في زعمه .

٢ أن المتعاملين بالإنترنت لا تحدهم حدود جغرافية فنجد الساب من بلد والمسبوب من بلد آخر الأمر الذي يأمن معه من الملاحقة القضائية وقد يتم السب عبر البريد الالكتروني للمسبوب فيتم إرسال هذه الرسالة إلى الشخص وحده وقد ترسل إلى عدة أشخاص.

أنواع الجرائم المعلوماتية



3 إفشاء الأسرار

عـن طريـق الحاسـب يمكـن الاعتداء علـى خصوصيـات الأفراد وإفشـاء أسرارهم وذلك باستعمال بيانات شخصية حقيقية بدون ترخيص أو إفشاء أسـرار بصورة غير قانونية وإسـاءة اسـتعمالها أو عدم الالتـزام بالقواعد الشـكلية الخاصة بتنظيم عملية جمع ومعالجة ونشـر البيانات الشخصية

نصت المادة السادسة الفقرة الأولى من النظام :

يعاقب بالسجن مدة لا تزيد على خمس سنوات

وبغرامة لا تزيد على ثلاثة ملايين

أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

إنتـاج مـا من شـأنه المسـاس بالنظام العـام , أو القيم الدينيـة أو الآداب العامـة أوحرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي

أنواع الجرائم المعلوماتية

4 الابتزاز والتهديد

تهديد الجاني المجني عليه إما بنشر أخباره أو صورة أو معلومات صحيحة ولكن لايرغب المجني عليه لسبب ما ظهورها للآخرين وإما يهدده بنشر صور أو أخبار أو معلومات غير صحيحة ويقوم بطلب مقابل حتى لا ينشرها سواء كان هذا المقابل مادي أو علاقة غير مشروعة

وقد جرم النظام هذا التهديد والابتزاز المعلوماتي حيث نصت المادة الثالثة الفقرة الثانية

يعاقب بالسجن مدة لاتزيد على سنة

وبغرامة لاتزيد على خمسمائة الف ريال

أو بإحدى هاتين العقوبتين , كل شخص يرتكب أيّاًمن الجرائم المعلوماتية الآتية : الدخول غير المشروع لتهديد شخص أو ابتزازه , لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً)).

فيتضح من النص مجرد فعل التهديد أو الابتزاز كاف لإقامة هذه الجريمة

أنواع الجرائم المعلوماتية

5 جريمة التنصت

يعاقب على هذه الجريمة بنص المادة الثالثة الفقرة الأولى من النظام

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة

وبغرامة لا تزيد على خمسمائة ألف ريال

أو بإحدى هاتين العقوبتين من يرتكب جريمة التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو التقاطه أو اعتراضه))

أشكال التنصت المعلوماتي

1

استخدام برنامج في جهاز الشخص المعتدى عليه يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم إدخال هذا الملف إلى جهاز المعتدى عليه عن طريق البريد الالكتروني أو عن طريق مواقع مغرية يزورها المعتدى عليه فيقوم بتنزيل بعض البرامج ومنها برنامج التنصت.

2

استخدام برنامج المحادثة, فيقوم المجرم بإغراء الضحية بأن هذا البرنامج يحتوي على ألعاب مثيرة أو غير ذلك فيقوم الضحية باستقبال الملف

أنواع الجرائم المعلوماتية

ركائز جريمة التنصت

الالتقاط أو **الاعتراض**

الالتقاط هو مشاهدة البيانات عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب .

الاعتراض : اعتراض ماهو مرسل عبر الشبكة المعلوماتية أو أحـد أجهـزة الحاسـب الالـي بحيـث يتـم عمـل إجرام كتحويل أموال .

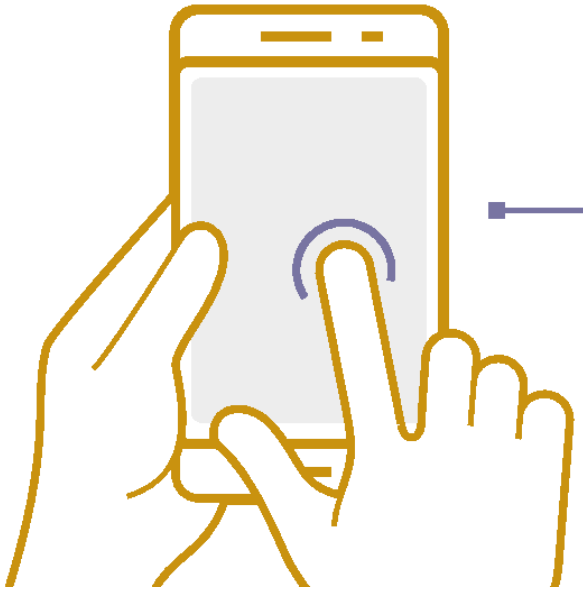
التمييز بين التنصت الذي يعتمد على السماع والالتقاط الذي يعتمد على المشاهدة دون تحديد كيفية الحصول عليها.

أنواع الجرائم المعلوماتية

6 جرائم إساءة استخدام الهواتف النقالة

وهذا النوع من الجرائم له العديد من الآثار الاجتماعية والنفسية على مستوى الأفراد, نظراً لما تدخله في نفوس الأفراد من الخوف في الوقوع كضحايا لهذا النوع من الجرائم ولقد ظهرت العديد من المشاكل في المجتمع السعودي نتيجة للاستخدام السيء للجوال .

نصت الفقرة الرابعة من المادة الثالثة على أنه :



يعاقب بالسجن مدة لاتزيد على سنة

وبغرامة لاتزيد على خمسمائة الف ريال

او بإحدى العقوبتين

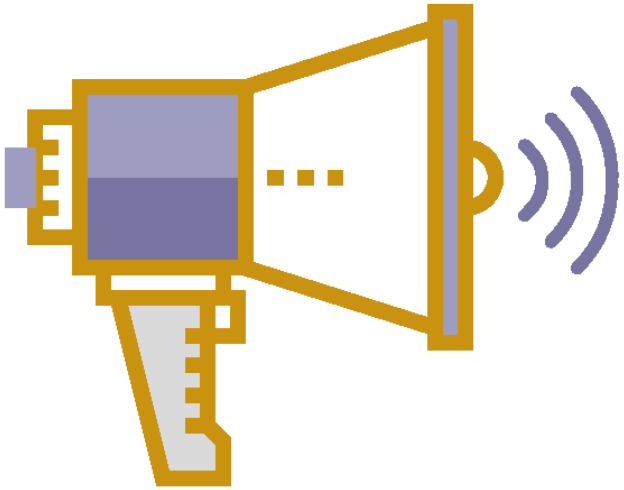
أيا من يرتكب الجرائم المعلوماتية التالية :

المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها .

أنواع الجرائم المعلوماتية

7 التشهير بالأشخاص

أصبحت هذه الجريمة من أبرز الجرائم الواقعة في الانترنت بل هناك مواقع صممت لأجل التشهير بالأشخاص والتسميع بهم .



التشهير له طرق أبرزها :

- البريد الالكتروني
- شبكة الويب العالمية
- مجموعة الأخبار
- غرف المحادثة

نصت المادة الثالثة الفقـرة الخامسـة من النظام

يعاقب بالسجن مدة لاتزيد على سنة

وبغرامة لاتزيد على خمسمائة الف ريال

أو بإحدى هاتين العقوبتين

كل شخص يقوم بالتشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة

أنواع الجرائم المعلوماتية

8 الاستيلاء والاحتيال المعلوماتي

الاستيلاء له :

إساءة استخدام الحاسبات الآلية والتلاعب في نظام المعالجة الالكترونية للبيانات والمعلومات

للحصول بغير حق على الأموال أو الخدمات والاستيلاء عليها للمجرم فعليا على مال منقول أو سند أو توقيع هذا السند.

الاستيلاء لغيره :

ويكون الاستيلاء لغيره بأن يسهل للغير الحصول على تلك الأموال بتزويده ببرامج مثلا تسهل تلك الجريمة

الاستيلاء

أنواع الجرائم المعلوماتية

الاحتيال المعلوماتي

له طرق متعددة كأن يوهم المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح ، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وقد يتخذ اسم أو صفة كاذبة تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الالكتروني للأموال وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو بتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في إيهام الحاسب والاحتيال عليه فيسلمه النظام المال .

نصـت المـادة الرابعـة الفقـرة الأولى من النظام على أنه

يعاقب بالسجن مدة لاتزيد على ثلاث سنوات

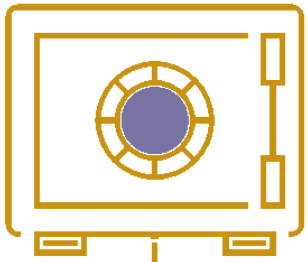
وبغرامة لاتزيد على مليوني ريال

او بإحدى هاتين العقوبتين كل شخص يرتكب
أياً من الجرائم المعلوماتية الاتية:

الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة.

أنواع الجرائم المعلوماتية

10 جريمة السطو على أموال البنوك



ويتم ذلك : عن طريق استخدام الجاني الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية .وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى وذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها وإتلافها وتقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جداً من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال .

وقد جرمت هذه الافعال كما في المادة الرابعة الفقرة الثانية

(الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق ماليه للحصول على بيانات أو معلومات أو أموال أو ماتتيحه من خدمات)

يعاقب بالسجن مدة لاتزيد على ثلاث سنوات

وبغرامة لاتزيد على مليوني ريال

او بإحدى هاتين العقوبتين

أنواع الجرائم المعلوماتية

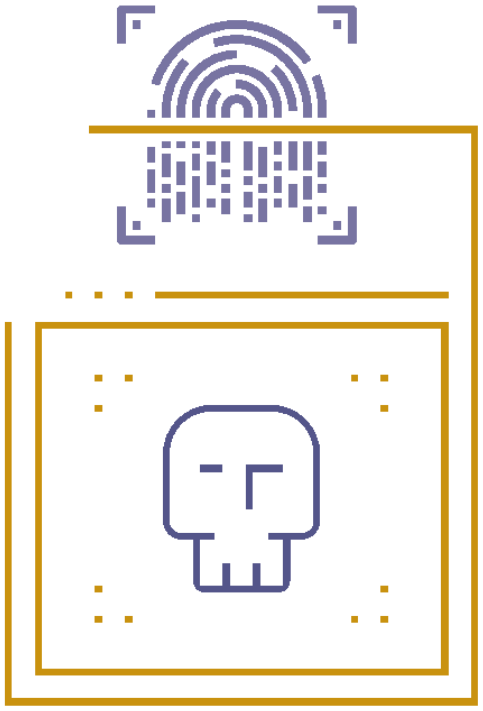
11 الانتحال والتغرير

والانتحال على صورتين

١ - انتحال شخصية فردية

بسـبب التنامي المتزايد لشبكة الإنترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشـخصية المطلوبة والاستفادة منها في ارتـكاب جرائمهـم فتنتشـر في شـبكة الإنترنـت الكثير مـن الإعلانات المشـبوهة والتي تحاكي الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية, فهناك إعلان عن جائزة فخمة يكسـبها مـن يسـاهم بمبلـغ رمـزي لجهـة خيريـة, وهـذا يتطلب الإفصـاح عن معلومات سـرية الأمر الذي يؤدي الى اسـتيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو الاساءة إلى سمعة الضحية

أنواع الجرائم المعلوماتية



٢ - انتحال شخصية المواقع

و يكـون باختـراق حاجز أمني وتتـم عملية الانتحال بهجوم يشـنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشـهورين ثم يقوم بتركيب البرنامـج الخـاص به هنـاك مما يؤدي إلـى توجه أي شـخص إلى موقعه بمجرد كتابة اسم الموقع المشهور

نصت المادة الرابعة الفقرة الأولى

يعاقب بالسجن مدة لاتزيد على ثلاث سنوات

وبغرامة لاتزيد على مليوني ريال

ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم التالية

الاستيلاء لنفسه ...أو انتحال صفة غير صحيحة

أنواع الجرائم المعلوماتية

التغرير بالقصر ومن في حكمهم واستغلالهم

وفيما يخص التغرير

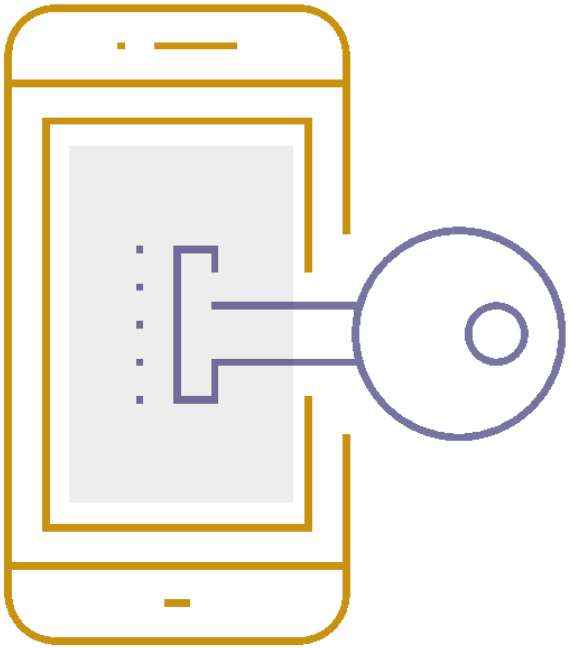
فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة حيث يوهم المجرمون ضحايا هذا النوع برغبتهم في تكوين صداقة على الانترنت وقد تتطور إلى التقاء مادي بين الطرفين .

نصت المادة الثامنة

لاتقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات التالية

أنواع الجرائم المعلوماتية

12 التحريض على الجريمة المعلوماتية



نصت المادة التاسعة من النظام على أنه:

(يعاقب كل من حرض غيره أو ساعده أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام إذا وقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق

بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ويعاقب بما لايتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية)

وقد جعل المنظم العقوبة على التحريض في الجرائم المعلوماتية مماثلة لعقوبة الفاعل الأصلي للجريمة بل في حال عدم فعل الجاني المعلوماتي وثبت التحريض عليها فيعاقب المحرض بنصف العقوبة المقررة لتلك الجريمة في النظام .

أنواع الجرائم المعلوماتية

13 الجريمة المعلوماتية الأخلاقية والاتجار بالبشر والاتجار بالمخدرات :

نصت المادة السابعة من النظام

يعاقب بالسجن مدة لاتزيد على خمس سنوات

وبغرامة لاتزيد على ثلاثة ملايين ريال

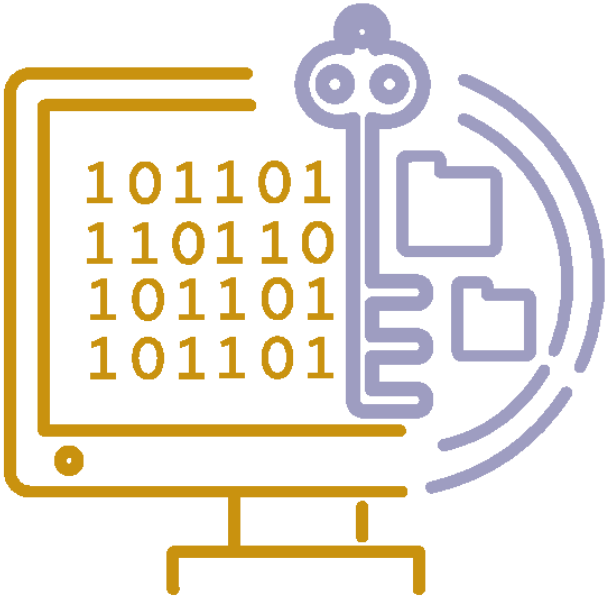
أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الاتية :

1. إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار في الجنس البشري أو تسهيل التعامل به.
2. إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.
3. إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرائق تعاطيها أو تسهيل التعامل بها.

أنواع الجرائم المعلوماتية

14 الجريمة المعلوماتية الأمنية

نصت المادة السابعة من النظام



يعاقب بالسجن مدة لاتزيد على عشر سنوات

وبغرامة لاتزيد على خمسة ملايين ريال

أو بإحدى هاتين العقوبتين , كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

1. إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية, أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات , أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية .

2. الدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.

أدوات الإبلاغ عن الجريمة المعلوماتية

الشرطة حسب
الاختصاص المكاني

تطبيق كلنا أمن على
الأجهزة الذكية

هيئة الامر بالمعروف والنهي عن
المنكر عن طريق الهاتف المجاني
1909 أو الموقع الإلكتروني
www.pv.gov.sa

الاتصال على
الرقم **989**

البوابة الإلكترونية
لوزارة الداخلية (أبشر)

البريد الإلكتروني
info.cybercrime@moisp.gov.sa

المحاكمة في الجريمة المعلوماتية

مرحلة المحاكمة الجزائية

تحال الدعوى بعد استكمال مرحلة التحقيق بدعوى عامة تقوم النيابة العامة بالترافع فيها امام المحكمة الجزائية مطالبة بتطبيق المواد الواردة في نظام مكافحة الجرائم المعلوماتية.

الاحالة الى النيابة العامة

وفي النيابة العامة دوائر متخصصة في التحقيق في الجرائم المعلوماتية تسمى بدوائر المال تقوم هذه الدوائر باستجواب المتهم والتحقيق معه في الجريمة المنسوبة اليه

المراجع والمصادر

- رؤية المملكة 2030 https://vision2030.gov.sa/
- الهيئة الوطنية للأمن السيبراني https://nca.gov.sa/index.html
- هيئة الاتصالات وتقنية المعلومات تقرير الأمن الرقمي وحماية المستخدم من مخاطر الانترنت إعداد صالح عبد الله الربيعة.

شكراً