الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

دليل السلامة الرقمية

دليل السلامة الرقمية

حقوق الملكيَّة الفِكْرِيَّة

للتواصل مع إدارة التميز السيبراني الوطني

https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa
00974 404 663 79
00974 404 663 62

فهرس المحتويات

تمهيد

الوكالة الوطنية للأمن السيبراني، وفي سياق سعيها لبناء مجتمع آمِن سيبرانياً، وتعزيزاً لمؤشرات الأمن السيبراني والسلامة الرقمية على مستوى الدولة والمؤسسات والمجتمع؛ أطلقت المبادرة الوطنية للسلامة الرقمية، والتي تستهدف مختلف شرائح المجتمع؛ من خلال تقديم محتوى توعوي سيبراني يُسهم في تعزيز الثقافة السيبرانية في المجتمع، ويُسهم في تحويلها لثقافة عامة وأسلوب حياة، بما يعزّز من مؤشرات السلامة الرقمية في المجتمع.

إن التطور التكنولوجي المتسارع، والانتشار الأفقي والعمودي للإنترنت، وتطورات الفضاء السيبراني، وظهور تهديدات سيبرانية متقدّمة، لا سيما بعد ثورة الذكاء الاصطناعي والذكاء الاصطناعي التوليدي؛ كل هذا وغيره أسهم بشكلٍ مباشرٍ في تصاعد المخاطر السيبرانية التي تُواجه شرائح المجتمع دون استثناء، هذا الواقع يحتّم الاهتمام المتزايد بنشر الوعي والثقافة السيبرانية، وتزويد الأفراد بمحتوى توعوي سيبراني يُمكّنهم من القدرة على التعامل الآمِن والفعّال مع الإنترنت والتكنولوجيا الحديثة.

من جهةٍ أخرى، فإنّ نشر الوعي والثقافة السيبرانية يعتمد على أدوات توعوية مختلفة، والأدلّة تُعدّ من هذه الأدوات الفعّالة؛ وانطلاقاً من هذا الطرح كانت فكرة هذا الدليل، والذي يُقدّم بين دفَّتيه عرضاً عامّاً لمختلف المخاطر السيبرانية التي يمكن أن يواجهها الأفراد في تعاملهم اليومي مع الإنترنت بمختلف تطبيقاته، كما يتضمّن الدليل نصائح وتوجيهات عامة لكيفية التعامل مع المخاطر السيبرانية، لا سيما تلك التي تُهدّد البيانات الشخصية، إضافةً إلى مخاطر الهندسة الاجتماعية والتصيد الاحتيالي، وكيفية تأمين الحسابات الإلكترونية والبريد الإلكتروني، وغيرها من المفاهيم ذات الصلة.

فكرة الدليل

تستمدّ فكرة الدليل أهميتها من أهمية المبادرة الوطنية للسلامة الرقمية، والتي تسعى لتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية في المجتمع، كما تشمل الفكرة تزويد مختلف شرائح المجتمع بمحتوى توعوي، بهدف تمكينهم من التعرُّف الدقيق على المخاطر السيبرانية التي يمكن أن تواجههم في تعاملهم اليومي مع الإنترنت والأدوات التكنولوجية.

تتَّسع فكرة الدليل لتشمل تزويد مختلف شرائح المجتمع بدليلٍ ومرجعٍ لكيفية التعامل مع المخاطر والتهديدات السيبرانية، فالدليل وفقاً لهذا الطرح لا يَستهدف شريحةً بعينها، فهو مُوجَّه للمجتمع بمختلف شرائحه، ولذلك فهو يتضمَّن محتوًى توعوياً شاملاً وغير مخصَّص، يتناسب مع الاحتياجات التوعوية للمجتمع ككل، ما يُعزّز من القيمة المعرفية المضافة المتوقَّعة من الدليل.

كما تشمل فكرة الدليل تحفيز التفكير النقدي والتحليلي لدى الأفراد؛ من خلال التوجُّه لهم بأسئلة تحليلية عَقِب كل فصل من فصول الدليل، وبذلك يخرج الدليل من نطاق التلقين ليتحوَّل بشكلٍ نسبيّ إلى كُتَيِّب تفاعُلي، ما يُعزّز الأثر المتوقَّع منه، ويُسهم في ترسيخ المحتوى في أذهان الشرائح المستهدَفة.

أهداف الدليل

يسعى الدليل لتحقيق جملة أهداف، تتمحور حول تعزيز الوعي والثقافة السيبرانية لدى مختلف شرائح المجتمع، وفيما يلي تبيان لأبرز أهداف الدليل:

1. توضيح مفاهيم الأمن السيبراني والسلامة الرقمية، وتوضيح نقاط الاتفاق والاختلاف بينهما.
2. تزويد شرائح المجتمع بمحتوى توعويّ سيبرانيّ يتعلّق بأهمّ وأشهر التهديدات والمخاطر السيبرانية وأكثرها شيوعاً.
3. تعزيز ثقافة السلامة الرقمية في المجتمع، وتحويلها لثقافة عامّة وأسلوب حياة.
4. تمكين الأفراد من التعرُّف الدقيق على المخاطر السيبرانية، وتوعيتهم بمخاطرها، وكيفية التعامل معها.
5. توفير مرجع خاصّ بالسلامة الرقمية، يكون متاحاً للجميع، بما يمكّن من الرجوع الدائم إليه للتعرُّف على المخاطر السيبرانية.
6. توضيح الأخطاء الشائعة التي يقع فيها المستخدمون عند تعاملهم مع الإنترنت، وتوعيتهم بمخاطر هذه الممارسات.
7. الإسهام في تحقيق أهداف المبادرة الوطنية للسلامة الرقمية؛ من خلال الإسهام في تعزيز مؤشرات الأمن السيبراني والسلامة الرقمية في الدولة.

الفصل الأول
مفهوم الأمن السيبراني والسلامة الرقمية

- مقدمة
- مفهوم الأمن السيبراني
- أهداف الأمن السيبراني
- محاور عمل الأمن السيبراني
- مجالات الأمن السيبراني
- مفهوم السلامة الرقمية وأبعادها
- أهداف السلامة الرقمية
- التقاطع والاختلاف بين الأمن السيبراني والسلامة الرقمية
- أنشطة

مقدمة

مع الانتشار الواسع للتكنولوجيا والإنترنت، أصبحت مفاهيم الأمن السيبراني والسلامة الرقمية شائعة نسبياً، ويتم تداولها على مستوى واسع، بما يشمل المتخصصين وغير المتخصصين، ولكن فيما يتعلق بشرائح المجتمع من غير المتخصصين بالأمن السيبراني وتكنولوجيا المعلومات، تبدو هذه المفاهيم متشابهة، وهذا غير دقيق، فعلى الرغم من وجود تقاطعات واسعة بين المفهومين، إلا أن كلاً منهما يهتم بجانب محدَّد، كما يختلفان في النطاق والأهداف والمحاور.

وإن الوعي والإدراك التام لمفاهيم الأمن السيبراني والسلامة الرقمية، يُعدّ مدخلاً رئيساً لتعزيز الوعي السيبراني وثقافة السلامة الرقمية في المجتمع، فمن الناحية التطبيقية من غير الممكن تعزيز مؤشرات السلامة الرقمية في المجتمع دون إدراك كل الأفراد لهذا المفهوم بدقة، ومعرفة محاوره وأهدافه ونطاق عمله وتأثيره، وانطلاقاً من هذا الطرح سيتم في سياق هذا الفصل التعريف بكلٍّ من الأمن السيبراني والسلامة الرقمية، وغيرهما من المفاهيم ذات الصلة.

مفهوم الأمن السيبراني

يعرّف الأمن السيبراني بأنه:

> حماية النُّظم والشبكات والبنية التحتية الحيوية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدّمه من خدمات، وما تحتوي عليه من بيانات، من أيّ اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع.

كما يُعرّف على أنه:

> مجموعة من الوسائل التقنية والإدارية والتنظيمية التي يتم الاعتماد عليها واستخدامها لمنع سرقة المعلومات الإلكترونية للأفراد والمؤسسات، كما يساعد على استعادة كافة المعلومات التي تمت سرقتها[1].

1. يوسف، أمير. (2015م). جرائم تقنية المعلومات بدول الخليج العربي، والجهود الدولية والمحلية لمكافحتها: جرائم الإنترنت والحاسوب الإلكترونية في دول الخليج العربي. مصر: دار الكتب العربية. ص 68 - 74.

ومـن هـذه التعريفـات يبـدو واضحـاً أن الأمـن السيبرانـي يتعلّـق بـالإجراءات والتدابيـر التـي تتَّخذهـا الحكومـات والمؤسسـات والهيئـات المتخصصـة بالأمـن السيبرانـي لحمايـة البنيـة التحتيـة الحيويـة، وحمايـة النُّظـم والشـبكات مـن الهجمـات السيبرانيـة. وبذلـك هـو إجراءات وتدابيـر تُتَّخـذ علـى أرض الواقـع، وذلـك مِـن قِبَـل المتخصصيـن فـي الأمـن السيبرانـي وتكنولوجيـا المعلومـات.

مصطلـح الأمـن السيبرانـي يتألـف مـن كلمتيـن؛ الأولـى أمـن، وهـي نقيـض الخـوف، ويُقصَـد بهـا الاطمئنـان والسـكينة، وشـعور الفـرد بالاطمئنـان عنـد تعاملـه مـع شـيءٍ مـا. والكلمـة الأخـرى هـي السيبرانـي، ويُقصَـد بهـا الفضـاء الإلكترونـي والإنترنـت، وكلّ مـا يتصـل بهمـا مـن مسـتلزمات ماديـة وغيـر ماديـة، كالأجهـزة والشـبكات والبرامـج وغيرهـا، وكلمـة سيبرانـي مشـتقة مـن كلمـة Cybernetics التـي تتَّصـل اصطلاحـاً بعلـم التحكُّـم الآلـي والقـدرة علـى التحكـم بالآلـة[1].

وكلمـة سيبرانـي، ذات جـذور يونانيـة، وتعنـي فـي اللغـة اليونانيـة القديمـة «الحاكـم». واسـتُخدِمت لأول مـرة فـي أربعينيـات الـقرن الماضـي (1940م) للدلالـة علـى عِلْـم التحكُّـم والاتصـال بيـن الكائنـات الحيـة والآلات، **ومـن هـذا السـياق يمكننـا تعريـف «السيبرانـي» بأنـه:**

> عمليات التحكُّم بكلّ ما هو رقمي ومتَّصل بالإنترنت.

1 . كمال، محمد. الإرهاب السـيبراني عندما يسـتخدم الإرهابي الكيبورد بدلاً من القنبلة، دار كليم للطباعة والنشر والتوزيع (القاهرة – مصر)، ط1، 2022م، ص11.

أهداف الأمن السيبراني

يسعى الأمن السيبراني لتحقيق جملةٍ من الأهداف المتكاملة، والتي تتمحور حول ضمان استقرار الفضاء السيبراني بما فيه من مكونات مادية وغير مادية، وفيما يلي تبيان تفصيلي لأهمّ هذه الأهداف:

1

حماية المعلومات والبيانات الحسّاسة

الهدف الرئيسي هو حماية البيانات الحسّاسة مثل المعلومات المالية، الصحية، والأسرار التجارية من السرقة أو التلاعب.

2

مواجهة الهجمات السيبرانية

من خلال اتخاذ تدابير وإجراءات تُتيح توقُّع الهجمات والتعامل معها قبل استهدافها للمؤسسات والبنى التحتية الحيوية.

3

دعم إجراءات التعافي المبكّر من الهجمات السيبرانية

تسبّب الهجمات السيبرانية خسائر اقتصادية وتَعطُّل في النُّظم التشغيلية والتكنولوجية، ما يتطلَّب العمل السريع على معالجة الخسائر، وضمان عودة النُّظم للعمل، وهذا أحد أهداف الأمن السيبراني.

4

ضمان استمرارية الأعمال

حماية الأنظمة الإلكترونية من الانقطاع أو التعطيل، ما يُسهم في استمرارية الأعمال من دون تعطُّل.

5

الامتثال للمعايير والقوانين

العديد من الدول والشركات مُلزمَة باتباع قوانين ولوائح خاصة بالأمن السيبراني لحماية البيانات والمعلومات.

6

حماية البنية التحتية الحيوية

مثل أنظمة الاتصالات، الطاقة، المياه، وغيرها من البنى التحتية الحيوية التي تعتمد على تكنولوجيا المعلومات.

7

تعزيز الثقة الرقمية

عبر تأمين أنظمة المعلومات، يتم تعزيز الثقة في التعاملات الرقمية والتجارة الإلكترونية.

محاور عمل الأمن السيبراني

يختـصّ الأمـن السيبرانـي بالعمـل علـى محـاور عـدة متكاملـة؛ بحيـث تتفاعـل هـذه المحـاور بمـا يُسـهم فـي تحقيـق أهـداف الأمـن السيبرانـي، وفيما يلـي تبيان لأهمها:

1 تنظيم الإستراتيجيات السيبرانية

يهتـم الأمـن السيبرانـي برسـم الإسـتراتيجيات السيبرانيـة العلاجيـة والوقائيـة. ويُقصَـد بالإسـتراتيجيات الوقائيـة التدابيـر المتَّخـذة لحمايـة المؤسسـات والبنيـة التحتيـة الحيويـة قبـل وقـوع الهجـوم السيبرانـي، بينمـا الإسـتراتيجيات العلاجيـة تهتـم بالتعامـل مـع الهجمـات بعـد حدوثهـا، والعمـل علـى تقليـل آثارها السـلبية ودعـم إجراءات التعافـي منهـا.

2 المحور التقني

يتعلـق بالتقنيـات والأدوات المسـتخدَمة لحمايـة الأنظمـة والشـبكات مثـل برامـج مكافحـة الفيروسـات وجـدران الحمايـة.

3 المحور القانوني

يركّز هذا المحور على وضع وتطبيق قوانين وسياسات تَحْكم سلوك الأفراد والشركات فيما يتعلق بالأمن السيبراني.

4 المحور التنظيمي

يتعلق المحور التنظيمي بإدارة الأمن السيبراني داخل المؤسسات، وضمان أن الجميع يتَّبع أفضل الممارسات والمعايير الأمنية.

5 بناء القُدرات

يهدف إلى تعزيز المهارات والمعرفة في مجال الأمن السيبراني عبر التدريب والتعليم.

5 التعاون الدولي

يشمل التعاون بين الدول والمنظمات الدولية لمواجهة التهديدات السيبرانية العابرة للحدود.

مجالات الأمن السيبراني

يعمل الأمن السيبراني لتحقيق أهدافه من خلال عدة قطاعات ومجالات عمل، وهذه المجالات قد تتطوَّر وتتوسَّع تبعاً لتوسُّع وتطور الفضاء السيبراني، وفيما يلي تبيان لأهم هذه المجالات:

أمن الشبكات

يهتمّ الأمن السيبراني بتأمين الشبكات من الهجمات الإلكترونية، ومن التعدّيات الرقمية عليها، ويسعى للحفاظ على فاعليتها.

أمن التطبيقات

يهدف أمن التطبيقات لتوفير بيئة رقمية آمِنة للتطبيقات؛ من خلال مراعاة معايير الأمن الرقمي عند تصميم التطبيقات؛ بحيث لا يكون اختراقها سهلاً، كما يهتمّ هذا المحور بتصميم تطبيقات للحماية من الهجمات الرقمية، والكشف عن البرمجيات الخبيثة وحذفها.

أمن المعلومات وسلامة وخصوصية البيانات

يحرص الأمن السيبراني على اتخاذ الإجراءات والتدابير اللازمة لضمان سلامة المعلومات والبيانات، وحمايتها من السرقة والقرصنة والتخريب.

أمن المستخدِم النهائي

وهو من المحاور المهمَّة والرئيسة في الأمن السيبراني، ويهتم بتوفير الأمان الرقمي للأفراد، وحمايتهم من المخاطر التي قد يتعرَّضون لها، مثل قرصنة البيانات الشخصية، وهجوم الفدية، وغيرها من المخاطر الرقمية[1].

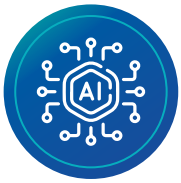
الأمن التشغيلي

يرتبط هذا المحور بتوفير معايير الأمان الرقمي اللازمة للتعامل مع مُشغّلي التقنيات الرقمية، ومنح إذن الوصول للبيانات المهمة والحسّاسة.

الأمن السحابي

في الفترة الأخيرة تمَّ الاعتماد على الذكاء الاصطناعي مِن قِبَل الأفراد والمؤسسات؛ بهدف تحسين جودة العمل، وإنجاز الكثير من المهامّ في أقلّ وقتٍ. ومن المعروف أنَّ كَمّ البيانات التي يتمّ تخزينها من الصَّعب أن يَتمّ الاحتفاظ بها؛ لذا هناك العديد من الشَّركات المختلفة تعمل على توفير أفضل الخدمات التي تساعد على حلّ تلك المشكلة في وقتٍ قياسيّ.

1. What is Cyber Security? Kaspersky, on site: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security



الذكاء الاصطناعي

مع التطورات المتسارعة التي يشهدها الذكاء الاصطناعي؛ أصبح ركناً رئيساً من أركان الأمن السيبراني، ومجالًا مُهمّاً فيه، ويمكن الاستفادة منه وتوظيفه في عدة محاور مهمَّة، من أهمها ما يلي :

- **استخدام الذكاء في مواجهة الهجمات السيبرانية:** من خلال تقنيات الذكاء الاصطناعي يمكن مواجهة الهجمات السيبرانية؛ وذلك لقدرته العالية على مُعالَجة كميات ضخمة من البيانات في وقت قياسي، ما يمكّنه من تحديد الثغرات الرقمية المحتمَلة، ومعالجتها قبل اكتشافها مِن قِبَل المهاجمين، إضافةً لاستخدام تقنياته في دعم مؤشرات التعافي عقب الهجمات السيبرانية.
- **مواجهة التهديدات السيبرانية المعتمِدة على الذكاء الاصطناعي:** تمكَّن المهاجمون السيبرانيون من استخدام الذكاء الاصطناعي في تطوير الهجمات السيبرانية، وزيادة فرص نجاحها، وذلك من خلال تحديد الثغرات الرقمية بسرعة وفاعلية، إضافةً لاستخدامه في التزييف العميق وإنشاء رسائل تصيدية صعبة الاكتشاف. وفي هذا المجال يسعى الأمن السيبراني لمواجهة هذه التهديدات وتبنّي إستراتيجيات وسياسات وإجراءات للتعامل الفعَّال مع هذه الأنماط المتقدّمة من التهديدات السيبرانية.

مفهوم السلامة الرقمية وأبعادها

يُقصَد بالسلامة الرقمية جملة الممارسات التي تتّبعها الشركات والأفراد للحماية من المخاطر السيبرانية، وهي تُعنَى بشكل رئيس بالتثقيف والتوعوية، كما يُقصَد بها قدرة الأفراد والمجتمع عموماً على التعرُّف على المخاطر السيبرانية، وكيفية التعامل معها وأُسس الوقاية منها.

وتقوم السلامة الرقمية على مجموعة من الأبعاد، فيما يلي تبيان لأهمها:

1 الخصوصية

يُقصَد بها حماية المعلومات الشخصية والبيانات الحسّاسة عند استخدامها أو مشاركتها عبر الإنترنت.

2 الأمان

تُركّز السلامة الرقمية على الأمان؛ من خلال تجنُّب التهديدات السيبرانية مثل البرمجيات الخبيثة والاختراقات.

3 التوعية والتثقيف

تُعدّ التوعية والتثقيف عماد السلامة الرقمية، وركنها الرئيس؛ وذلك بهدف تعزيز القدرة على التعرُّف على التهديدات السيبرانية، مثل التصيد الاحتيالي، والاحتيال عبر الإنترنت وتجنّبها.

4 السلوك المسؤول

وذلك بهدف التفاعل بشكلٍ آمِن ومسؤول مع الآخرين عبر الإنترنت، سواء على وسائل التواصل الاجتماعي أو في البيئات الرقمية الأخرى.

أهداف السلامة الرقمية

تهدف السلامة الرقمية لتحقيق جملة من الأهداف، تتركّز بشكلٍ رئيس حول حماية الأفراد من المخاطر السيبرانية؛ من خلال التوعية والتثقيف، وفيما يلي تبيان للأهداف التفصيلية لها.

1 حماية الخصوصية

بهدف التأكد من أن الأفراد قادرون على التحكُّم في كيفية استخدام ومشاركة بياناتهم الشخصية، وضمان عدم استغلالها مِن قِبَل الجهات غير المصرَّح لها.

2 التوعية بقواعد الاستخدام الآمِن للإنترنت

من خلال نَشْر الوعي بين الأفراد حول كيفية حماية أنفسهم من التهديدات السيبرانية، مثل: التصيد الاحتيالي، وسرقة الهوية، وغيرهما.

3 الحدّ من الجرائم الإلكترونية

تهدف السلامة الرقمية للحدّ من الجرائم الإلكترونية؛ من خلال التثقيف والممارسات السيبرانية الآمِنة، كما تهدف إلى تقليل فُرَص تعرُّض الأفراد للهجمات السيبرانية، مثل: الاحتيال الإلكتروني، وسرقة البيانات.

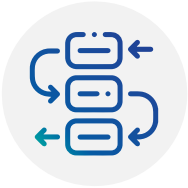
4 تعزيز السلوك السيبراني الأخلاقي

من خلال تشجيع المستخدِمين على اتّباع سلوكيات آمِنة ومسؤولة عند التفاعُل عبر الإنترنت، بما في ذلك عدم نشر أو مشاركة محتويات ضارَّة أو غير آمِنة.

5 حماية الفئات الهشَّة

تُوصَف العديد من الشرائح الاجتماعية، بأنها هشَّة سيبرانياً، بمعنى أن خبرتها في التعامل مع الإنترنت ودرايتها بمخاطره منخفضة، ما يجعلها أهدافاً مفضَّلة للمجرمين، مثل الأطفال والمراهقين الذين قد يكونون أكثر عُرْضَة لمخاطر الإنترنت. وتُسهم برامج السلامة الرقمية في توعية الآباء والمعلمين بكيفية حماية هؤلاء الأفراد.

مع تزايد الاعتماد على الإنترنت والتكنولوجيا في الحياة اليومية؛ أصبحت السلامة الرقمية أكثر أهمية من أيّ وقتٍ مضى. وتهدف إلى حماية الأفراد من الأخطار التي قد تُؤثِّر على حياتهم الشخصية والمالية والاجتماعية، ما يُعزّز الثقة في التكنولوجيا، ويساعد على خَلْق بيئة رقمية آمِنة ومستدامة.



التقاطع والاختلاف بين الأمن السيبراني والسلامة الرقمية

يتقاطع مفهوم الأمن السيبراني مع السلامة الرقمية في بعض النقاط والمحاور، لكنّه يختلف معها في أخرى، فهو يختلف في المفهوم العام والأهداف والنطاق، وغيرها من المحاور، وفي الجدول التالي تبيان للاختلافات بين المفهومين وفقاً لعدة محاور.

محور المقارنة	الأمن السيبراني	السلامة الرقمية
المفهوم العام	يركّز المفهوم على حماية النُّظم والشبكات، والبيانات المُهمّة والحسّاسة من الهجمات والتهديدات السيبرانية. كما يهدف إلى تأمين المعلومات والبنية التحتية الحيوية من الاختراقات والتهديدات.	يركّز المفهوم على توعية وتثقيف الأفراد بكيفية الحماية من المخاطر السيبرانية في أثناء استخدامهم للتكنولوجيا والإنترنت. كما يُركز على السلوكيات الآمِنة والوعي بالمخاطر الشخصية التي يمكن أن تُواجه المستخدِمين.
النطاق	يهتم الأمن السيبراني بقضايا تتعلّق بتأمين الشبكات، وحماية البيانات، وإعداد إستراتيجيات سيبرانية، والتعاون مع الجهات الحكومية والشركات في مجال الأمن السيبراني.	تُركّز السلامة الرقمية بشكلٍ أساسي على توعية وتثقيف الأفراد، بما يشمل حماية الخصوصية، وتجنُّب الاحتيال، والتعامل بأمان مع الإنترنت.

محور المقارنة	الأمن السيبراني	السلامة الرقمية
الأهداف	• حماية المعلومات الحسّاسة. • ضمان استمرارية الأعمال من خلال حماية النُّظم والبنية التحتية الحيوية. • رسم الإستراتيجيات السيبرانية الوقائية والعلاجية. • وضع خُطط لمواجهة الهجمات السيبرانية. • الامتثال للقوانين والمعايير التنظيمية.	• تعزيز الوعي السيبراني لدى الأفراد حول المخاطر السيبرانية. • تعزيز قدرة الشرائح الاجتماعية الهشَّة سيبرانياً على مُواجهة المخاطر السيبرانية. • تشجيع السلوكيات السيبرانية المسؤولة والأخلاقية.
الجمهور المستهدَف	يُركِّز بشكلٍ رئيس على المؤسسات، الحكومات، والشركات التي تحتاج إلى تأمين معلوماتها وأنظمتها.	تستهدف المجتمع بشكلٍ عام، بما في ذلك المستخدمون غير المتخصصين في الأمن السيبراني وتكنولوجيا المعلومات؛ لتوعيتهم بكيفية حماية أنفسهم ومعلوماتهم الشخصية.
التقنيات والأدوات المستخدَمة	يستخدم الأمن السيبراني تقنيات متقدّمة مثل التشفير، الذكاء الاصطناعي، جدران الحماية، وأنظمة كشف التسلل (IDS)، وتحليل النُّظم والتهديدات المستجدَّة لمراقبة وحماية الأنظمة.	تستخدم أساليب التعليم والتوعية، مثل ورش العمل والدورات التدريبية؛ لتمكين الأفراد من التعرُّف على المخاطر السيبرانية، واتخاذ خطوات لحماية أنفسهم.
التعامل مع التهديدات	يتعامل مع التهديدات المعقَّدة والمتقدّمة التي تتطلَّب استجابةً فوريةً وتكنولوجيا متطورة، مثل الهجمات المتقدمة المستمرة (APTs).	تتعامل السلامة الرقمية مع التهديدات الأكثر شيوعاً، والتي تستهدف الأفراد، مثل التصيد الاحتيالي، من خلال التثقيف والتوعية.

ختاماً لهذا الفصل، يُعدّ الأمن السيبراني والسلامة الرقمية من المفاهيم المُهمّة بالنسبة للدول والمؤسسات والمجتمعات والأفراد؛ فالتهديدات السيبرانية أصبحت تطال الجميع من دون استثناء، ما جعَل الثقافة السيبرانية أولوية وطنية واجتماعية.

وهنا لا بدّ من التأكيد على أن المؤسسات والهيئات الرسمية المعنية بالأمن السيبراني والسلامة الرقمية لا تستطيع بمفردها تحقيق الأمن السيبراني والسلامة الرقمية في المجتمع دون تعاون فعّال من مختلف شرائح المجتمع؛ فالسلامة الرقمية مسؤولية جماعية، تتطلّب تعاون وتضافُر مختلف الجهود.

أنشطة

النشاط الأول

ابحث في أنشطة وفعاليات وبرامج ومبادرات الوكالة الوطنية للأمن السيبراني في دولة قطر، وحدِّد أهمّ أنشطتها التي تندرج تحت نطاق الأمن السيبراني أو السلامة الرقمية.

النشاط الثاني

ابحث في أكثر التهديدات السيبرانية التي تُواجِه كلاً من المؤسسات والأفراد، مع توضيح الاختلاف في طبيعة الهجمات التي تَستهدف كلاً منهما.

النشاط الثالث

يُواجِه الأفراد مخاطر سيبرانية متعدّدة، ابحث في هذه المخاطر وحدِّد الأثر السلبي لكل منها.

الفصل الثاني
مفهوم المخاطر السيبرانية وأنواعها

- **مقدمة**
- **الجرائم الإلكترونية**
- **مفهوم المخاطر السيبرانية**
- **أنواع المخاطر السيبرانية**
  * برمجيات الفدية (Ransomware)
  * برمجيات التّجسُّس (Spyware)
  * التصيد الاحتيالي (Phishing)
  * الهندسة الاجتماعية (Social Engineering)
- **التهديدات السيبرانية للشبكات**
- **أنشطة**

مقدمة

مـع الانتشـار المتسـارع للإنترنـت واتّسـاع رُقعـة اسـتخدام الحوسـبة السـحابية، والبيانـات الضخمـة، والـذكاء الاصطناعـي؛ تتزايـد أهميـة السلامـة الرقميـة، خاصـةً أن الثـورة التقنيـة جعلـت المجتمـع والأفراد أكثـر عُرْضَـة للمخاطـر السيبرانيـة التـي يمكـن أن تُـؤدّي إلـى خسـائر متعـدّدة، تشـمل الخسـائر الماليـة، فقـدان البيانـات، تعطيـل البنيـة التحتيـة الحيويـة، وغيرهـا.

يُعـدّ مفهـوم المخاطـر السيبرانيـة (Cyber Risks) مـن الموضوعـات التـي تشـهد اهتمامـاً متزايـداً علـى مسـتوى الأفراد والمؤسسـات علـى حـدّ سـواء؛ إذ أصبحـت الهجمـات السيبرانيـة أكثـر خطـورة، وأكثـر تنوعـاً، بمـا يشـمل برمجيـات الفديـة، والتّجسُّـس، ومخاطـر التصيـد الاحتيالـي، والهندسـة الاجتماعيـة، وقرصنـة البيانـات، وغيرهـا مـن المخاطـر السيبرانيـة.

وبشـكلٍ عـامّ، لا يمكـن تعزيـز الوعـي بالسلامـة الرقميـة فـي المجتمـع دون الوعـي التامّ بمفهـوم المخاطـر السيبرانيـة وآثارهـا السـلبية. وانطلاقـاً مـن هـذا الـطرح سـيتم فـي هـذا الفصـل تحديـد مفهـوم المخاطـر والتهديـدات السيبرانيـة، وتبيـان أنواعهـا المختلفـة، وكيفيـة الوقايـة منهـا.

الجرائم الإلكترونية

اهتمّ التشريع في دولة قطر بالجرائم الإلكترونية، وفرَض عقوبات على مرتكبيها؛ بهدف ردعهم. وهذه القوانين تُعزّز من مؤشرات السلامة الرقمية في الدولة، فقانون الجرائم الإلكترونية الذي صدر عام 2014م، عرَّف الجريمة الإلكترونية بأنها:

> أيّ فِعْل يتم باستخدام الشبكة المعلوماتية أو أنظمة المعلومات بطرق غير مشروعة، سواء أكان الهدف منها الحصول على بيانات، أم تدميرها، أم التلاعب بها دون تصريح[1]

1 . تفاصيل قانون الجرائم الإلكترونية في قطر، محامي قطر، متاح على الرابط: https://2u.pw/wga1FQvG.

وبشكلٍ عامّ تتميّز الجرائم الإلكترونية بخصائص تجعلها مختلفة عن الجرائم التقليدية، وفيما يلي تبيان لأهم هذه الخصائص وأبرزها:

1. تُعدّ هذه الجرائم خفيةً إلى حدّ كبير؛ حيث يمكن إخفاء آثارها بسهولةٍ، أو قد لا يتم الإبلاغ عنها نتيجة الخوف أو لأسباب اجتماعية وثقافية.

2. تتميز الجرائم الإلكترونية بسرعتها الشديدة؛ حيث يمكن تنفيذها في غضون ثوانٍ معدودة.

3. يمكن تنفيذ الجرائم الإلكترونية عن بُعْد، ما يعني أنها لا تعرف حدوداً جغرافية، خاصةً في ظِل العولمة الرقمية.

4. تُواجه الملاحقة القانونية للجرائم الإلكترونية تحديات عديدة، خاصةً عندما يكون المجرم في بلد مختلف عن بلد الضحية.

5. تُعدّ الجرائم الإلكترونية صعبة الإثبات؛ حيث لا يترك المجرمون عادةً أيّ أدلّة مادية على جرائمهم.

6. تُعدّ هذه الجرائم «ناعمة»؛ حيث يتم تنفيذها باستخدام أدوات تقنية دون الحاجة إلى القوة البدنية.

مفهوم المخاطر السيبرانية

المخاطر السيبرانية تشير إلى التهديدات والتحدّيات التي تُواجه الأنظمة المعلوماتية والشبكات التقنية. تتراوح هذه المخاطر من الهجمات السيبرانية التي تهدف إلى سرقة البيانات أو تدميرها، إلى تعطيل الخدمات الحيوية. وتشمل المخاطر السيبرانية عوامل داخلية وخارجية، مثل الهجمات الخبيثة التي يقوم بها المتسللون أو الأخطاء البشرية التي تؤدي إلى تسريب البيانات.

من الضروري أن نفهم أن المخاطر السيبرانية لا تقتصر فقط على الأنشطة الخبيثة مثل الفيروسات أو الهجمات على الأنظمة، بل تمتدّ إلى جوانب متعددة؛ مثل: ضعف البنية التحتية التكنولوجية، والاستخدام السيئ لأنظمة الأمان، وحتى السلوك البشري غير الواعي، والذي يمكن أن يؤدّي إلى اختراق الأنظمة.

أنواع المخاطر السيبرانية

يندرج تحت المخاطر السيبرانية أنواع متعددة، وجميعها تُسبّب مخاطر وأضراراً على المستخدِمين، وفيما يلي تبيان لأهمّ هذه الأنواع:

1

برمجيات الفدية (Ransomware)

تُعدّ برمجيات الفدية واحدةً من أخطر أشكال الهجمات السيبرانية في العصر الحالي. يقوم هذا النوع من البرمجيات الضّارّة بتشفير ملفّات النظام أو البيانات، ومِن ثَم يطالب المهاجم بفدية مالية مقابل استعادة الوصول إلى تلك الملفات. ويتم توزيع برمجيات الفدية غالباً عبر رسائل البريد الإلكتروني الاحتيالية، أو عن طريق استغلال الثغرات الأمنية في الأنظمة غير المحمية بشكلٍ كافٍ.

لقد أصبحت برمجيات الفدية تهديداً عالمياً يتزايد باستمرار؛ حيث تَستهدف المؤسسات الكبرى، مثل: المستشفيات، والشركات متعددة الجنسيات، وتتسبَّب في خسائر مالية ضخمة.

أنواع برمجيات الفدية

- **Crypto Ransomware:** يقوم هذا النوع من البرمجيات بتشفير الملفّات المهمّة للمُستخدِم، ويمنع الوصول إليها حتى يتم دفع الفدية. ويُعدّ هذا النوع الأكثر شيوعاً.
- **Locker Ransomware:** هذا النوع لا يقوم بتشفير الملفات، بل يغلق النظام بالكامل ويمنع المستخدِم من الوصول إليه، وغالباً ما يطالب بدفع الفدية لاستعادة السيطرة على الجهاز[1].
- **Scareware:** نوع من البرمجيات الخبيثة التي تتظاهر بأنها برامج حماية مشروعة، لكنّها تقوم بإخافة المستخدِم عبر إظهار رسائل تُنذر بوجود مشكلات أمنية مزيَّفة، وتطلب منه دفع فدية لحل المشكلة.

أُسُس الوقاية من البرمجيات الضّارّة

على الرغم خطورة البرمجيات الضّارّة، يمكن الوقاية منها بسهولةٍ؛ من خلال اتباع مجموعة من الإجراءات الاحترازية، والتي تشمل:

- **النسخ الاحتياطي للبيانات:** يُعدّ من أهم إجراءات الحماية؛ حيث يُمكّن المستخدِم من استعادة بياناته في حال تعرُّضها للتشفير.
- تحديث أنظمة التشغيل وبرامج مكافحة الفيروسات: وهذا التحديث يُقلّل من الثغرات الأمنية، ويساعد في حماية الأجهزة من الهجمات الإلكترونية.
- **استخدام جدران الحماية:** تُسهم جدران الحماية في منع هجمات البرمجيات الضّارّة التي تستهدف الأجهزة.
- **الوعي بآلية عمل البرمجيات الضّارّة:** الوعي الكامل بآليات عمل هذه البرمجيات الضّارّة وأنواعها المختلفة هو الأساس لحماية المجتمع.

1 . What Is Ransomware? Proofpoint, on site: https://www.proofpoint.com/us/threat-reference/ransomware.

2

برمجيات التّجسُّس (Spyware)

برمجيات التّجسُّس هي نوع من البرمجيات الخبيثة التي تتسلل إلى النظام دون عِلْم المستخدِم، لجمع المعلومات والبيانات الشخصية، مثل معلومات الحسابات المصرفية، وكلمات المرور، والتاريخ الشخصي للمستخدِم. غالباً ما يتمّ تثبيت هذه البرمجيات عن طريق الروابط المشبوهة أو التطبيقات المزيَّفة.

برمجيات التّجسُّس تُستخدم غالباً في العمليات الاحتيالية لسرقة الهوية، أو التّجسُّس على نشاط الأفراد والشركات؛ مما يجعلها واحدةً من أخطر أنواع الهجمات السيبرانية.

أنواع برمجيات التّجسُّس

- **برمجيات تسجيل نقرات لوحات المفاتيح Keyloggers:** تسجّل هذه البرمجيات كل ضغطة على لوحة المفاتيح لتسجيل معلومات حسّاسة، مثل كلمات المرور، أو تفاصيل بطاقات الائتمان.
- **برمجيات الإعلانات Adware:** تقوم بعرض إعلانات غير مرغوبة على جهاز المستخدِم بغرض جمع المعلومات الشخصية من خلال التفاعل مع هذه الإعلانات.
- **أحصنة طروادة Trojans:** تعمل على فتح ثغرة في النظام للسماح للمتسللين بالوصول إلى الجهاز عن بُعْد.

3

التصيد الاحتيالي (Phishing)

التصيد الاحتيالي هو أحد أشكال الهجمات السيبرانية التي تعتمد على الهندسة الاجتماعية؛ لخداع المستخدمين للكشف عن معلومات حسّاسة، مثل: كلمات المرور، أو بيانات البطاقات الائتمانية، وغيرها. ويتم ذلك عادةً من خلال رسائل بريد إلكتروني مزيَّفة تبدو كأنها مُرسَلة من مصادر موثوقة[1].

أنواع التصيد الاحتيالي

التصيد الاحتيالي يُعدّ واحداً من أكثر الهجمات الإلكترونية شيوعاً وأشدّها خطراً بسبب بساطة تنفيذه وسهولة خداع الأفراد به. ويشمل عدّة أنواع، منها

- **التصيد عبر البريد الإلكتروني Email Phishing:** يتم إرسال رسائل بريد إلكتروني تحتوي على روابط أو مرفقات خبيثة تهدف إلى خداع المستخدِم للكشف عن بياناته الشخصية.
- **التصيد الاحتيالي المستهدَف Spear Phishing:** في هذا النوع من التصيد يتم توجيه الرسالة التصيدية إلى شخص أو مؤسسة بعينها بهدف الحصول على معلومات حسّاسة محدَّدة.
- **التصيد الاحتيالي المُوجَّه لكبار الشخصيات Whaling:** يستهدف التصيد الاحتيالي من هذا النوع الأفراد ذوي المناصب العليا في الشركات، مثل المدراء التنفيذيين، ويكون الهجوم عادةً معقَّداً وأكثر إقناعاً.

1. نظراً لخطورة التصيد الاحتيالي سيتم تخصيص فصل مستقلّ له في سياق هذا الدليل.

4

الهندسة الاجتماعية (Social Engineering)

الهندسة الاجتماعية هي مصطلح يشير إلى نوعٍ من التقنيات الحديثة التي يتم استخدامها مِن قِبَل المهاجمين الرقميين، ومن خلال هذه التقنية يقوم المهاجمون بإقناع الضحايا لتقديم بياناتهم الشخصية، ودَفْع الضحايا للتعامل مع المهاجمين؛ فقد يتم تشجيعهم لفتح روابط محددة، تكون هذه الروابط خاصة بتثبيت برمجيات خبيثة، وغالباً ما يستغل المهاجمون ضعف خبرة مستخدمي الإنترنت بقواعد الأمان. وتعتمد على استغلال السلوك البشري لخداع المستخدمين لتقديم المعلومات أو القيام بأفعالٍ تُسهّل على المهاجمين تنفيذ هجمات سيبرانية. ويقوم المهاجمون بتحليل سلوك الضحية لجمع المعلومات التي يمكن أن تساعد في اختراق النظام.

تقنيات الهندسة الاجتماعية

تُعدّ الهندسة الاجتماعية من الأساليب الاحتيالية التي يصعب اكتشافها؛ نظراً لاعتمادها الكبير على استغلال السلوكيات البشرية بدلاً من الثغرات التقنية، وهي تشمل عدة تقنيات، فيما يلي تبيان لأهمها وأشهرها:

- **الاصطياد «Baiting»:** من التقنيات المستخدَمة في هجمات الهندسة الاجتماعية، يقوم على جذب المستخدِم إلى الفخّ لسرقة بياناته الشخصية، وإلحاق الضرر بأنظمته بواسطة البرمجيات الضّارَّة، معتمداً في ذلك على مشاعر الفضول والطمع عند الضحايا.
- **الذريعة Pretexting:** إحدى أدوات الهندسة الاجتماعية التي يستخدمها المهاجمون، وهي مجموعة من الأكاذيب والإشاعات المصمَّمة باحترافية، تُوهِم الضحية بأنه مُضطرّ إلى تقديم بيانات مُهمّة وحسّاسة لإنقاذه من خطرٍ ما؛ تمهيداً لبدء عملية الاحتيال.

وبشكلٍ عامّ تُعدّ الهندسة الاجتماعية من الأساليب المفضَّلة لمجرمي الإنترنت؛ لأنها تُمكّنهم من الوصول إلى الشبكات والأجهزة والحسابات دون الحاجة إلى القيام بأعمال تقنية صعبة، مثل كسر جدار الحماية؛ أو تخطّي برامج مكافحة الفيروسات؛ وغيرها من تقنيات الحماية.

الوقاية من الهجمات المعتمِدة على الهندسة الاجتماعية

يمكن الوقاية من الهجمات المعتمدة على الهندسة الاجتماعية من خلال الحرص على اتباع النصائح والإجراءات التالية:

- **التوعية والتثقيف**

تُعدّ التوعية بالسلامة الرقمية وقواعد التصفُّح الآمِن للإنترنت من أهم أُسس الوقاية من الهجمات المعتمدة على الهندسة الاجتماعية، إضافةً لضرورة وعي مختلف شرائح المجتمع بمفهوم الهندسة الاجتماعية، وكيفية استغلالها في التصيد الاحتيالي والهجمات الأخرى التي تعتمد على التلاعب النفسي. إضافةً للتوعية بكيفية التعرُّف على المحاولات المشبوهة، والبقاء في حالة يقظة تجاه المواقف غير المعتادة، مثل الرسائل التي تطلب معلومات شخصية أو كلمات مرور.

- **التحقُّق من الهوية**

التحقُّق من الهوية يُعدّ من الوسائل المُهمّة والفعَّالة للوقاية من مخاطر الهندسة الاجتماعية؛ وذلك من خلال استخدام وسائل التحقُّق المزدوج (Two-factor authentication) للتأكد من هوية الأشخاص الذين يحاولون الوصول إلى الأنظمة أو البيانات الحسّاسة. إضافةً للتحقُّق من مصادر الرسائل الإلكترونية أو المكالمات الهاتفية، خاصةً إذا كانت تحتوي على طلبات مشبوهة.

- **حماية المعلومات الشخصية**

لا بدّ من تقليل مُشارَكة المعلومات الشخصية عبر الإنترنت أو عبر وسائل التواصل الاجتماعي؛ فالمهاجمون قد يَستخدمون هذه المعلومات لجعل هجماتهم أكثر إقناعاً، كما يُفضّل تجنُّب نشر بيانات حسّاسة في الأماكن العامة أو عبر القنوات غير المشفَّرة.

- **استخدام برامج الحماية من الفيروسات**

لا بدّ من تثبيت برامج مكافحة الفيروسات وتحديثها بانتظام للكشف عن البرمجيات الضّارّة التي يتم نقلها لأجهزة المستخدِمين من خلال تقنيات الهندسة الاجتماعية، إضافةً لضرورة تفعيل جدران الحماية (Firewalls) والأنظمة الأمنية التي تمنع الوصول غير المصرَّح به إلى الشبكات.

- **السياسات الأمنية الصارمة**

فيما يتعلق بالحماية من مخاطر الهندسة الاجتماعية في المؤسسات، لا بدّ من وضع سياسات أمنية واضحة للتعامل مع طلبات الوصول إلى المعلومات الحسّاسة. وتطبيق مبدأ أقل الصلاحيات (Least Privilege Principle) ؛ بحيث يحصل الموظفون على الحد الأدنى من الصلاحيات التي يحتاجون إليها لأداء عملهم.

- **التعامل بحذر مع البريد الإلكتروني**

يُعدّ البريد الإلكتروني من أكثر القنوات استخداماً في الهندسة الاجتماعية؛ لذلك لا بدّ من الحذر عند فتح الرسائل الإلكترونية غير المتوقَّعة أو التي تحتوي على مرفقات غير معروفة، خاصةً تلك الواردة من أشخاص مجهولين، وتجنُّب النقر على الروابط التي تبدو مشبوهة، حتى لو كانت من جهات معروفة، والتحقُّق منها أولاً.

- **الإبلاغ عن الحوادث**

عند التعرُّض لخطرٍ أو حادثةٍ متعلّقة بالهندسة الاجتماعية، على مستوى الأفراد أو الموظفين، لا بدّ من الإبلاغ الفوري عن الحادثة، حتى يتمّ اتخاذ التدابير اللازمة. وعلى مستوى الأفراد ينبغي إعلام الجهات المتخصّصة، أما في المؤسسات، فينبغي اتباع البروتوكولات المرعية في هذا الصدد.

التهديدات السيبرانية للشبكات

تُشكّل الجرائم التي تَستهدف الشبكات الإلكترونية تهديداً خطيراً للأفراد والشركات على حدّ سواء؛ إذ يتمثّل الهدف الرئيس لهذه الجرائم في سرقة البيانات أو إحداث ضرر على الشبكة بطرق غير مشروعة. تعتمد هذه الجرائم غالباً على استخدام البرمجيات الخبيثة التي تنتشر بشكل تلقائيّ، مُحدِثةً أضراراً متنوعة مثل سرقة المعلومات الشخصية أو المالية، الابتزاز عبر الإنترنت، أو تعطيل الخدمات الإلكترونية.

أبرز أهداف هجمات الشبكات

تشمل الأهداف غير القانونية لهجمات الشبكات ما يلي:

- **الاحتيال عبر البريد الإلكتروني والإنترنت.**
- **سرقة الهوية باستخدام معلومات شخصية حسّاسة.**
- **الاستيلاء على البيانات المالية أو بيانات البطاقات الائتمانية.**
- **سرقة بيانات الشركات أو العملاء لبيعها أو ابتزاز الشركات بها.**
- **الابتزاز الإلكتروني باستخدام تهديدات مالية مقابل عدم تنفيذ الهجمات.**
- **هجمات الفدية لطلب دفع مالي من أجل فكّ تشفير البيانات.**
- **التّجسُّس عبر الإنترنت الذي يستهدف الحكومات أو الشركات أو الأفراد.**
- **التسلل إلى الأنظمة مما يُهدّد سلامة الشبكات.**
- **انتهاك حقوق الطبع والنشر.**
- **تعطيل الخدمات العامة المقدَّمة عبر الإنترنت.**

أنواع هجمات الشبكات

تحت عنوان هجمات الشبكات تُوجد عدة أنواع من الهجمات، فيما يلي تبيان لأهمها:

1

هجمات رفض الخدمة (DDoS)

هذه الهجمات تهدف إلى تعطيل الخدمات الإلكترونية التي تعتمد على الشبكات عبر إغراق النظام بعددٍ ضخمٍ من الطلبات، مما يجعله غير قادر على الاستجابة. ويسبّب هذا النوع من الهجمات أضراراً كبيرة للمؤسسات؛ مثل: إيقاف الخدمات الحكومية عبر الإنترنت.

2

هجمات الشبكات اللاسلكية (Wireless Attacks)

يستهدف هذا النوع من الهجمات الشبكات اللاسلكية مثل شبكات الهواتف المحمولة، بهدف تعطيل الخدمات أو سرقة بيانات العملاء، مما قد يُؤدّي إلى تهديدات مثل الابتزاز لاحقاً.

3

هجمات التوأم الشرير (Evil Twin)

تركّز هذه الهجمات على شبكات Wi-Fi؛ حيث يقوم المهاجم بإنشاء صفحة مزيَّفة تشبه الصفحة الأصلية للخادم الذي يتصل به المستخدمون، فيخترق الشبكة، ويستولي على المعلومات الحسّاسة مثل كلمات المرور والبيانات الشخصية.

4

هجمات البلوتوث (Bluejacking)

تعتمد هذه الهجمات على تقنية البلوتوث لاختراق الأجهزة المتَّصلة بالشبكة؛ حيث يتم إرسال برمجيات خبيثة إلى أجهزة الضحايا من خلال الشبكة، مما يُمكّن المهاجم من التحكم في الجهاز أو سرقة البيانات منه.

من وسائل الحماية من هجمات الشبكات

للوقاية من هجمات الشبكات يمكن اتباع الإجراءات التالية:

- استخدام برامج مكافحة الفيروسات وجدران الحماية.
- تحديث أنظمة التشغيل بانتظام لسدّ الثغرات الأمنية.
- توعية المستخدمين حول أساليب الهجمات مثل رسائل التصيد والمواقع المزيَّفة.
- تفعيل أنظمة التحقق المزدوج لحماية الوصول إلى الحسابات.

تظلّ هذه التدابير الوقائية ضرورية للحدّ من تأثير هجمات الشبكات وضمان سلامة المعلومات والبيانات الحيوية.

ختاماً لهذا الفصل؛ تتطوَّر المخاطر السيبرانية بشكلٍ مستمر ومتسارع، ما يعني أنّ طُرق الوقاية الفعَّالة حالياً لن تكون بذات الفاعلية في المستقل القريب، خاصةً أن المهاجمين يعملون بشكلٍ مستمرّ على تطوير أدوات التهديد، لذلك لا بدّ من السعي المستمرّ لتعزيز الوعي بهذه المخاطر، ونشر الوعي بمفاهيم الأمن السيبراني والسلامة الرقمية، فمن الناحية التطبيقية لا يمكن تحقيق مؤشرات مرتفعة في الأمن السيبراني والسلامة الرقمية دون تعاون مختلف شرائح المجتمع، وهذا التعاون يعتمد بشكلٍ رئيسٍ على التوعية والتثقيف السيبراني.

أنشطة

النشاط الأول

اجمع بيانات حول أعداد الجرائم السيبرانية التي تمَّت في العالم في عام 2023م، وقارنها ببيانات عام 2022م... ماذا تستنتج؟

النشاط الثاني

تستفيد الهجمات المعتمِدة على الهندسة الاجتماعية من التطورات المتسارعة في مجال الذكاء الاصطناعي... ابحث في كيفية استفادة المهاجمين السيبرانيين من الذكاء الاصطناعي.

النشاط الثالث

يهتم القانون بتوفير الحماية من الجرائم الإلكترونية، كما يهتم بخصوصية البيانات، اذكر أمثلة على هذا.


SYSTEM HACKED
SYSTEM HACKED
SYSTEM HACKED

الفصل الثالث
التصيد الاحتيالي

- مقدمة
- آلية تنفيذ هجمات التصيد الاحتيالي
- أهداف التصيد الاحتيالي وآثاره
- أنواع التصيد الاحتيالي
- علامات التعرُّض لهجمات التصيد الاحتيالي
- أنشطة

مقدمة

يُعدّ التصيد الاحتيالي من التهديدات السيبرانية الشائعة؛ وذلك لكون هذا النوع من التهديدات لا يتطلّب خبرات تقنية مرتفعة، كما أن تكلفته منخفضة بالنسبة للمهاجمين مقارنةً بالهجمات السيبرانية الأخرى، إضافةً إلى إمكانية استهداف عدد كبير من الضحايا في الوقت ذاته.
وفي التصيد الاحتيالي يتم استغلال شبكة الإنترنت لخداع الضحايا بهدف سرقة بياناتهم الشخصية، مثل كلمات المرور وأرقام بطاقات الائتمان، وذلك من خلال طُرق وأدوات عدّة؛ منها: إنشاء موقع إلكتروني مزيَّف لاستدراج الضحية؛ ويتم إرسال الرابط عبر البريد الإلكتروني أو رسائل على منصات التواصل الاجتماعي؛ تتضمّن هذه الرسائل روابط خبيثة، وفي حال دخل المستخدِم على هذه الروابط يتم قرصنة بياناته الشخصية والمالية الحسّاسة من خلال برمجيات خبيثة يتم تثبيتها عن طريق تلك الروابط.

يعتمد التصيد الاحتيالي بشكلٍ رئيسٍ على أساليب الضغط النفسي لإقناع الضحايا بالتصرُّف دون تفكير، عبر انتحال شخصية مألوفة أو كيان معروف، ثم خَلْق شعور زائف بالرغبة أو الحاجة، مستغلّين مشاعر مثل الخوف والقلق والفضول والرغبة والطموح للحصول على ما يريدون، حينها قد يتَّجه المستخدمون إلى اتخاذ قرارات سريعة، وهذا يتم عبر إرسال رسالة تطلب من المستخدِم «اتخاذ إجراء فوري»، فهذه خدعة احتيالية تهدف إلى دفع المستخدِمين للتصرُّف السريع دون وَعْي كافٍ.

وتُشير الإحصائيات الدولية إلى زيادة مستمرة في أعداد هجمات التصيد الاحتيالي، وفي حجم الخسائر الناجمة عنها؛ لأن مسألة خداع الأفراد للضغط على الروابط الضّارّة الواردة في رسائل البريد الإلكتروني الاحتيالية أمر يسهل فِعْله مقارنةً بالأنواع الأخرى من الهجمات السيبرانية؛ فقد كشف التقرير الصادر عن شركة Cisco حول تهديدات الأمن السيبراني، عن مسؤولية التصيد الاحتيالي عن 90 % من الاختراقات الأمنية للبيانات في العالم. وفي بحث لـ IBM عام 2022، تم ربط التصيد الاحتيالي بـ 550 هجوماً سيبرانياً خلَّف خسائر قُدِّرت بـ 4,9 مليون دولار[1].

1 . What Is Phishing? IBM, 17 May 2024. On site: https://www.ibm.com/topics/phishing.

آلية تنفيذ هجمات التصيد الاحتيالي

يقوم التصيد الاحتيالي بشكلٍ رئيسٍ على انتحال المهاجم شخصية أخرى عبر البريد الإلكتروني، أو أيٍّ من وسائل التواصل أو الرسائل النصية لخدمة الرسائل القصيرة (SMS)، بغرض الحصول على معلومات حسّاسة عن الضحية، ومن أجل القيام بذلك، يستخدم المهاجِم مصادر مفتوحة للحصول على معلومات شخصية عن الضحية، فعلى سبيل المثال، قد تتضمّن الرسالة التصيدية معلومات شخصية عن الضحية لا يعرفها إلا المقرّبون، ووجود مثل هذه المعلومات في الرسالة يَدْفع المستخدِم إلى الاعتقاد بأنها واردة من شخص يعرفه؛ ما يَدْفعه إلى تنفيذ طلبات المهاجِم.
وهذه المعلومات يَجْمعها المهاجِم من مصادر عدّة؛ منها: المعلومات الشخصية والمهنية التي يُشارِكها المستخدمون على منصات التواصل الاجتماعي. لذلك، يمكن التقليل من مخاطر التعرُّض للتصيد الاحتيالي من خلال تقليل معدّل مشاركة البيانات الشخصية على منصات التواصل الاجتماعي.

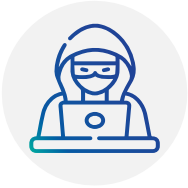
يتلقَّى المستخدِم الضحية في هذا النوع من الهجمات رسالةً يبدو ظاهرياً أنها تابِعة لجهة موثوقة، مثل صديق أو مؤسسة رسمية، وبمجرد نَقْر المستخدِم على الملفات المرفَقة بالرسالة، وهي في الغالب رابط تشعّبي يَربطه بموقع ويب ضارّ، يبدأ الهجوم من خلال تثبيت برمجيات ضارة على جهازه أو توجيهه إلى مواقع إنترنت مزيَّفة، لتبدأ عملية قرصنة المعلومات الحسّاسة، مثل كلمات المرور وأرقام البطاقات البنكية وغيرها.

أهداف التصيد الاحتيالي وآثاره

تهدف هجمات التصيد الاحتيالي إلى تحقيق عدّة أهداف للمهاجمين، فيما يلي أبرزها:

- **سرقة البيانات، مثل سرقة معلومات الحسابات البنكية وكلمات المرور.**
- **تثبيت البرمجيات الضّارّة على أجهزة المستخدِمين المستهدَفين.**
- **استغلال البيانات المسروقة في عمليات أخرى، مثل هجمات الفدية أو التّجسُّس عبر الإنترنت.**
- **مدخل لتنفيذ عمليات أخرى لتخريب أنظمة المؤسسات المستهدَفة.**
- **دَفْع الضحية للدخول إلى موقع مزيَّف على الإنترنت لإكمال خطة الهجوم الاحتيالي.**

وفيما يتعلّق بآثار هجمات التصيد الاحتيالي، فعلى مستوى المؤسسات، يمكن أن تؤدي هجمات التصيد الاحتيالي إلى تعطيل الأنظمة الداخلية؛ ما يُسبّب خسائر مالية كبيرة ويُضعف سُمعة المؤسسة، نتيجة تعرُّض بيانات العملاء للخطر، وهو ما يضع المؤسسات في مواجهة مع اللوائح التنفيذية الهادِفة إلى حماية البيانات داخل الدول. أما على مستوى الأفراد، فقد تتسبّب الهجمات في سرقة الهُويّة أو استخدام المعلومات الشخصية في جرائم أخرى؛ مما يؤدي إلى أضرار طويلة الأمد، مثل تشويه السُّمعة أو سرقة الأموال.



أنواع التصيد الاحتيالي

يمكن أن يتم التصيد الاحتيالي عبر عدّة أنواع، فيما يلي تبيان لأهمّها:

التصيد المُوجَّه Spearfishing

هذا النوع من التصيد يكون مُوجّهاً لفرد محدّد داخل مؤسسة بعينها؛ بغرض سرقة بيانات اعتماد تسجيل الدخول الخاصة به؛ حيث يقوم المهاجِم بجَمْع المعلومات الشخصية عن الفرد المستهدَف قبل بدء الاحتيال، مثل الاسم والمنصب وتفاصيل الاتصال الخاصة به. ويهدف هذا النوع إلى سرقة الهُويّة، أو الاحتيال المالي، أو التلاعُب في البيانات المالية للمؤسسة، أو التّجسُّس، أو سرقة البيانات السّرية من أجل إعادة بيعها للمهتمين بها مثل المنافِسين؛ وبشكلٍ عامٍّ يتم استهداف الأفراد الذين يملكون بيانات مهمة، مثل الرؤساء التنفيذيين.

وهنا لا بدّ من الإشارة إلى أن التصيد المُوجَّه يُعدّ أحد أنواع التصيد الاحتيالي، وهو يختلف عنه في عدّة نقاط، من أهمّها أن التصيد المُوجَّه يستهدِف مستخدِماً بعينه، أما هجمات التصيد الاحتيالي فهي هجمات واسعة النطاق تستهدِف البيانات الحسّاسة للمستخدِمين بشكلٍ عامٍّ دون تخصيص[1].

1. What is spear phishing? Definition and risks. Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/spear-phishing.

التصيد الصوتي Vishing

يعتمد هذا النوع من التصيد على المكالمات الهاتفية أو الرسائل الصوتية، بغرض الاحتيال على المستهدَفين وسرقة بياناتهم الشخصية والمالية؛ ويعتمد هذا النوع بشكلٍ رئيسٍ على الهندسة الاجتماعية، وهي تقنية حديثة تعتمد على الغرائز البشرية الطبيعية، مثل الثقة أو الخوف وغيرها من مشاعر يستغلّها المهاجمون للتأثير في الضحايا لدَفْعهم إلى اتخاذ قرار معيّن يقود إلى تحقيق هدف المهاجِم، مثل سرقة المال أو المعلومات الحسّاسة.
وغالباً ما يتظاهر المهاجِم بأنه أحد الأفراد الذين يعرفهم الضحية، أو بأنه مسؤول في إحدى المؤسسات التي يتعامل معها الضحية بشكلٍ عامٍّ؛ ليبدأ في استدراجه للحصول على المعلومات المهمَّة منه لتنفيذ باقي خطة الاحتيال[1]. ويمكن تنفيذ التصيد الصوتي من خلال اللّعب على وتر الرغبة الشخصية للضحية في تحقيق مكاسب مادّية، مثل إغرائه بعروض شرائية هائلة بأسعار رمزية، أو الإعلان عن مسابقة وهمية ذات عائد مالي كبير.

التصيد عبر البريد الإلكتروني Email Phishing

وهو من أكثر أنواع التصيد الاحتيالي شيوعاً، وفيه يعتمد المهاجِم على البريد الإلكتروني في إرسال رسالة التصيد، من خلال صياغتها على أنها من مصدرٍ موثوقٍ؛ بهدف التسلُّل إلى الجهاز لسرقة البيانات الحسّاسة والمالية أو سرقة الهُويّة.

وبشكلٍ عامٍّ، توجد عدّة دلائل أو علامات تُميّز رسائل البريد الإلكتروني التصيدية، منها:

- **أسلوب الكتابة غير المألوف**

فعلى سبيل المثال، إذا وَرَدَت رسالة إلى المستخدِم من شخص يعرفه، يمكن أن يُلاحِظ اختلاف أسلوب الكتابة فيها، فهذه تُعدّ إشارة أوَّلية إلى أن الرسالة تحتمل أن تكون محاولة تصيد.

1. Vishing: The Growing Threat and How to Protect Yourself. TOPSEC. On site: https://www.topsec.com/vishing-voice-phishing-the-growing-threat-and-how-to-protect-yourself/.

- **الأخطاء النحوية والإملائية**

الأخطاء النحوية والإملائية من العلامات المميّزة للرسائل الاحتيالية، خاصّةً في الرسائل التي يَدَّعي مرسلوها أنها واردة من مؤسسات رسمية؛ لأن هذه المؤسسات تَحْرص على التدقيق اللغوي لرسائلها قبل إرسالها للمستخدِمين.

- **التناقُض في عناوين البريد الإلكتروني والروابط**

التناقُض في عناوين البريد الإلكتروني والروابط أحد دلائل الرسائل الاحتيالية، لذلك على المستخدِم مطابقة عنوان البريد الإلكتروني الوارد من المؤسسة مع العنوان الأصلي المُعْلَن في موقعها الرسمي.

- **الإلحاح وإثارة مشاعر الخوف**

تحرص الرسائل التصيدية على التلاعُب بمشاعر الضحايا؛ من خلال إثارة الخوف والقلق لديهم حيال تعاملاتهم البنكية أو معلوماتهم الشخصية، ثم طَلب إمدادهم بالبيانات الحسّاسة للضحايا، وهنا يجب التيقُّظ وتغليب الحذر، والتمهُّل قبل إرسال أيّ بيانات أو معلومات مهمة عبر الإنترنت.

- **المرفَقات المشبوهة**

في حال كانت رسائل البريد الإلكتروني تحتوي على مرفَقات، فقد تكون امتدادات المرفَقات إشارة إلى عملية احتيال، مثل zip، exe، scr ونحوها من امتدادات غير مألوفة؛ لذا يجب فَحْص المرفَقات قبل فَتْحها بواسطة برامج مكافحة الفيروسات[1].

- **طلب تحميل برامج وروابط**

الشركات والمؤسسات نادراً ما تَطْلب من المستخدِمين تحميل برامج أو فَتْح روابط مُحدَّدة، لذلك في حال طَلَب المُرسِل تثبيت برامج معيَّنة أو روابط على الأجهزة فيجب التيقُّظ؛ إذ في الأغلب تكون رسائل احتيالية، ويجب عدم الاستجابة لهذه الأوامر.

1. 10 Most Common Signs of a Phishing Email. On site: https://www.titanhq.com/blog/10-tell-tale-signs-that-spam-email-is-a-phishing-scam/.

التصيد الاحتيالي عبر HTTPS

في هذا النوع من التصيد الاحتيالي يتم تنفيذ الهجوم عبر HTTPS ؛ من خلال إرسال رسالة بريد إلكتروني إلى المستخدِم المستهدَف، تتضمَّن رابطاً إلى موقع ويب مزيَّف، بهدف خداع الضحية لإدخال معلوماته الخاصة؛ وتُعدّ مواقع HTTPS الاحتيالية المَنْفَذ المُفضَّل للمهاجمين الذين لديهم القدرة على إيهام الضحايا بأنهم مصدر موثوق به. وهذا النوع من الهجمات الاحتيالية يُوصَف بأنه منخفض المخاطر ومرتفع المكاسب.

ومن الجدير بالذِّكر أن 91 % من الهجمات السيبرانية تبدأ برسالة بريد إلكتروني تصيدية يتم إرسالها إلى المستخدِمين، ويتم جَذْبهم إلى المواقع عبر رابط في الرسالة المُرسَلة من عنوان شرعي، مثل شركة معروفة أو شخص معروف؛ ومن الأمثلة على هذا النوع من الهجمات الاحتيالية: ما حَدَث مع شركة Sony Pictures، التي تعرَّضت في عام 2014 لهجومٍ عن طريق إرسال رسائل بريد مزيَّفة تَمكَّن خلالها المهاجمون من التسلُّل إلى الشركة، وسرقة كلمات المرور وبيانات مهمَّة؛ نتيجة فَتْح الموظفين لروابط مزيَّفة أُرْسِلَت إليهم عبر البريد الإلكتروني[1].

التصيد الاحتيالي المعروف بـ Pharming

يُعدّ هذا النوع الأكثر شيوعاً في استهداف المؤسسات المالية والمصرفية، Pharming وهو عبارة عن مزيجٍ من الكلمتين «Phishing» و «farming»؛ حيث يتم تصميم موقع ويب مزيَّف ثم إعادة توجيه المستخدِمين المستهدَفين إليه لسرقة المعلومات السِّرية؛ وتهدف هذه المواقع المزيَّفة إلى جَمْع المعلومات الشخصية عن الضحية مثل كلمات المرور وأرقام الحسابات البنكية وغيرها، أو محاولة تثبيت برمجيات ضارّة على أجهزة الحاسوب الخاصة بالضحايا.

1. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://www.keyfactor.com/blog/https-phishing-attacks-how-hackers-use-ssl-certificates-to-feign-trust/.

التصيد الاحتيالي المنبثق Pop-up Phishing

تُعرّف الرسائل الاحتيالية المنبثقة بأنها رسائل تَظْهر للمستخدِمين في أثناء تصفُّحهم للإنترنت، نتيجة استغلال المهاجمين لمواقع الويب المُصابة ببرمجيات خبيثة. وتَظْهر هذه الرسائل على شكل تحذيرات حول وجود تهديدات على الجهاز، مما يُقْلِق المستخدِم ويُوحي له بأنّ جهازه معرَّض للخطر. وغالباً ما تَطْلب هذه الرسائل من المستخدِمين تنزيل برامج «مضادّة للفيروسات» لإصلاح المشكلة، لكن في الواقع تكون هذه البرامج ضارّة وتَهْدف إلى اختراق أجهزة المستخدِمين وسرقة بياناتهم أو الاحتيال عليهم.

تصيد التوأم الشرير Evil Twin

يهدف هذا النوع من التصيد الاحتيالي إلى خداع المستخدِمين للاتصال بشبكة Wi-Fi مزيَّفة يتم إعدادها لتبدو مثل الشبكة الأصلية، وبعد أن يتَّصل المستخدِمون بالشبكة المزيَّفة، يَتمكَّن المهاجِمون من اختراق أجهزتهم والوصول إلى البيانات المُخزَّنة. ويتم تنفيذ الهجوم عبر عدّة خطوات كالتالي:

- **اختيار موقع عامّ يحتوي على شبكة Wi-Fi مجانية، مثل المقاهي أو المطارات، لبدء الهجوم.**
- **إعداد نقطة وصول Wi-Fi مزيَّفة تحمل اسماً مشابهاً أو مألوفاً؛ لجَذْب المستخدِمين للاتصال بها.**
- **إنشاء صفحة مزيَّفة تَطْلب من المستخدِمين إدخال بياناتهم الشخصية أو كلمات المرور للاتصال بالشبكة.**
- **تَوْجيه الأجهزة بالقرب من الضحايا لزيادة قوة الإشارة المزيَّفة، مما يَدْفع المستخدِمين إلى اختيار الشبكة المزيَّفة دون معرفة.**
- **مُراقَبة أنشطة المستخدِمين وسرقة البيانات بمجرد اتصالهم بالشبكة؛ حيث يبدأ المهاجِمون جَمْع المعلومات المهمة مثل الأرقام وكلمات المرور والبيانات الشخصية.**

فهذا النوع من الهجمات يُشكِّل تهديداً كبيراً للخصوصية والأمان الشخصي، ويستهدف استغلال ثقة المستخدِمين بشبكات Wi-Fi العامة[1].

1. What is an Evil Twin Attack? Evil Twin Wi-Fi Explained, Kaspersky. On site: https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks.

التصيد الاحتيالي المُوجَّه لكبار الشخصيات Whaling

يستهدف هذا النوع من التصيد الاحتيالي كبار المسؤولين التنفيذيين في المؤسسات العالمية؛ حيث يتم استهدافهم برسائل بريد إلكتروني تبدو موثوقة ومألوفة، لكنّ الهدف الرئيسي منها هو تحفيز الضحايا على اتخاذ إجراءات معيَّنة مثل تحويل أموال أو تقديم معلومات حسّاسة. وغالباً ما تستهدِف هذه الهجمات المؤسسات المالية وخدمات الدفع؛ حيث تتوفَّر معلومات مهمة حول الأفراد أو المؤسسات المعنيَّة.
وتشمل أهداف هذا النوع من التصيد ما يلي:

- **إغراء الضحايا بالنقر على روابط تؤدي إلى مواقع تحتوي على برمجيات ضارَّة.**
- **طلب تحويل أموال إلى الحسابات المصرفية للمهاجِمين.**
- **جَمْع بيانات حسّاسة عن الأفراد أو المؤسسات؛ لاستخدامها في هجمات أخرى مثل هجمات الفدية.**

مؤخراً، ومع التطورات التكنولوجية المتسارعة وزيادة الاعتماد على الذكاء الاصطناعي، أصبحت هجمات التصيد الاحتيالي أكثر تعقيداً وصعوبةً في الكشف عنها؛ وذلك بسبب استخدام عناوين بريد إلكتروني مزيَّفة تظهر كأنها تنتمي إلى مصادر موثوقة، بالإضافة إلى ذلك، يَعْتمد المهاجِمون على مصطلحات تجارية ويَجْمعون بين عدّة أساليب احتيالية مختلفة لجَعْل الهجمات تبدو حقيقية. هذا التعقيد قد يجعل حتى المسؤولين التنفيذيين الذين لديهم خبرة تقنية يقعون ضحايا لهذه الهجمات.

علاوةً على ذلك، يَعتمِد المهاجِمون أحياناً على هجوم مزدوج؛ حيث يتم إرسال بريد إلكتروني مزيَّف إلى الضحية، متبوعاً بمكالمة هاتفية لإقناع الضحية بمصداقية الرسالة والطَّلب. كما تُعدّ وسائل التواصل الاجتماعي مصدراً مهماً للمهاجِمين؛ حيث يتم جَمْع معلومات مهنية وشخصية عن الضحايا المستهدَفين لاستخدامها في تحسين مصداقية الهجمات[1].

1. Whaling: how it works, and what your organization can do about it. On site: https://serviceteamit.co.uk/news/whaling-how-it-works-and-what-your-organisation-can-do-about-it/.

استنساخ التصيد Clone Phishing

هو نوع من التصيد الاحتيالي الذي يَستخدِم فيه المهاجِم نسخةً طبق الأصل من رسالة بريد إلكتروني تم إرسالها مسبقاً من جهة موثوقة إلى الضحية؛ حيث يتم «استنساخ» الرسالة الأصلية وإعادة إرسالها إلى الضحية مع تعديلات طفيفة، مثل استبدال الروابط الأصلية بروابط ضارة، أو إدراج مرفَقات خبيثة.

يتمثَّل الخطر في أن الرسالة المُستنسَخة تبدو مألوفة وموثوقة لدى الضحية؛ لأنها نسخة من رسالة سبَق أن تلقَّاها[1]، مما يزيد من احتمال قيام الضحية بالنقر على الروابط أو فَتْح المرفَقات دون حذر. غالباً ما تُستخدَم هذه الطريقة لاستغلال الثقة بين المرسِل والضحية لتحقيق أهداف مثل سرقة المعلومات الشخصية أو تثبيت برمجيات خبيثة على جهاز الضحية.

ويهدف هذا النوع من التصيد إلى سرقة معلومات حسّاسة مثل بيانات الحسابات أو كلمات المرور، إضافةً إلى تثبيت البرمجيات الضّارّة التي تُمكِّن المهاجِم من اختراق الأنظمة أو التسلُّل إلى بيانات الضحية؛ ويتم هذا الهجوم عبر عدّة خطوات، هي:

- **نَسْخ البريد الإلكتروني الأصلي:** يتم أَخْذ نسخة من رسالة بريد إلكتروني سبق أن تم إرسالها من مصدر موثوق.
- **تعديل الروابط أو المرفَقات:** يقوم المهاجِم بتغيير الروابط أو المرفَقات لتوجيه المستخدِم إلى مواقع خبيثة أو برمجيات ضارة.
- **إعادة إرسال الرسالة:** تُرسَل الرسالة إلى الضحية، الذي قد يثق بالبريد الإلكتروني؛ لأنه يبدو مألوفاً.

1.Clone Phishing: Here's What You Need to Know to Protect Your Organization. On site: https://hoxhunt.com/blog/clone-phishing#:~:text=Clone%20phishing%20is%20when%20hackers,strategies%20to%20safeguard%20your%20organizatio.

علامات التعرُّض لهجمات التصيد الاحتيالي

توجد عدّة علامات تُشير إلى تعرُّض المستخدِمين لهجمات تصيد احتيالي، فيما يلي تبيان لأهمّها:

1

استلام إشعارات غير متوقَّعة حول محاولات تسجيل الدخول

تلقّي إشعارات عبر البريد الإلكتروني قد تكون إشارة لمحاولات تسجيل الدخول إلى الحسابات، وفي حال لم يكن المستخدِم هو مَن قام بهذه المحاولات فقد يكون هناك شخص يُحاوِل الوصول غير المصرَّح به إلى حسابات المستخدِم.

2

تباطؤ الجهاز وارتفاع حرارته بشكلٍ غير عادي

في حال أصبح جهاز الحاسوب أو الهاتف المحمول بطيئاً بشكلٍ ملحوظٍ، وارتفاع حرارته دون مبرّر، فقد يكون السبب هو وجود برمجيات ضارة تعمل في الخلفية وتستهلك موارد الجهاز.

3

ظهور نوافذ منبثقة مزعجة

ظهور نوافذ منبثقة بشكلٍ مفاجئ تَدَّعي أن الجهاز مصاب بالفيروسات يُعدّ علامة على وجود برمجيات خبيثة، أو ظهور إعلانات (adware) تحاول دَفْع المستخدِم إلى تنزيل برمجيات ضارة، أو محاولة خداعه من خلال عملية تصيد احتيالي.

4

فَتْح المتصفِّح والتطبيقات بشكلٍ تلقائيّ

إذا كانت نوافذ المتصفِّح أو التطبيقات تَفْتح وتُغْلق من تلقاء نفسها دون تدخُّل من المستخدِم، فهذا قد يشير إلى أن الجهاز مُختَرَق، وأن هناك برمجيات ضارة تتحكَّم في النظام.

5

إرسال رسائل غريبة إلى الأصدقاء

إذا أبلغ الأصدقاء أو زملاء العمل عن تلقِّيهم رسائل غير مألوفة أو مشبوهة من المستخدِم؛ فقد يكون حساب البريد الإلكتروني أو منصات التواصل الاجتماعي قد تم خَرْقها واستخدامها لإرسال رسائل غير مشروعة.

6

تلقِّي رسائل بريد إلكتروني عشوائية

زيادة في عدد الرسائل العشوائية أو المزعجة (Spam) في صندوق البريد الوارد، فقد تكون معلومات البريد الإلكتروني قد تم تَسْريبها؛ ما يعني أن المستخدِم تعرَّض لتصيد احتيالي أو إلى هجوم بالبرمجيات الضّارّة مثل برمجيات التّجسُّس.

للوقاية من هجمات التصيد الاحتيالي، لا بدّ من اتِّباع النصائح التالية:

- استخدام برامج مكافحة الفيروسات وتَحْديثها بانتظام.
- تفعيل خاصية التحقُّق بخطوتين في حساباتك؛ لزيادة مستوى الأمان.
- تجنُّب فَتْح الروابط المشبوهة أو تحميل الملفات غير الموثوقة من الإنترنت.
- تغيير كلمات المرور بشكلٍ دوريّ، واستخدام كلمات مرور قوية ومُعقَّدة.

ختاماً لهذا الفصل، تُعدّ هجمات التصيد الاحتيالي أكثر أنواع الهجمات السيبرانية شيوعاً، وتزداد أعداد الضحايا بشكلٍ متسارعٍ، كما تزداد الخسائر المالية والاجتماعية الناجمة عنها، والحلّ الأفضل للتعامل معها والوقاية منها هو اتّباع قواعد التصفُّح الآمِن للإنترنت، فالوقاية من هذه المخاطر أكثر فاعلية مقارنةً بالتدخُّل بعد وقوعها، وهذا مبدأ أصيل في الأمن السيبراني والسلامة الرقمية، فالنَّهج الوقائي في التعامل مع المخاطر السيبرانية أكثر فاعلية مقارنةً بالنَّهج العلاجي.

أنشطة

النشاط الأول

في جدول من تصميمك؛ اذكر أهمّ أنواع التصيد الاحتيالي، مع تبيان آلية عمل كل نوع، وكيفية الوقاية منه.

النشاط الثاني

تعتمد الاتجاهات الحديثة في التصيد الاحتيالي بشكلٍ متزايدٍ على الذكاء الاصطناعي، ابحث في كيفية الوقاية من التصيد الاحتيالي المُعتمِد على الذكاء الاصطناعي.

النشاط الثالث

ابحث في الإنترنت عن نماذج دولية لحالات تصيد احتيالي، وحدّد الخطأ الذي ارتكبه المستخدِمون حتى وقعوا ضحايا للاحتيال.

الفصل الرابع
المخاطر السيبرانية في بيئة العمل

- مقدمة
- المخاطر السيبرانية في بيئة العمل: طبيعتها وأنواعها
- تأثير المخاطر السيبرانية على بيئة العمل
- العمل عن بُعد والمخاطر السيبرانية
- إستراتيجيات مواجهة المخاطر السيبرانية في بيئة العمل عن بُعد
- تحديات إدارة المخاطر السيبرانية في المستقبل
- بروتوكول الإبلاغ عن الحوادث السيبرانية
- أنشطة

مقدمة

فـي عصـرٍ يعتمـد بشـكلٍ متزايـد علـى التكنولوجيـا والاتصـال الرقمـي، ومـع اعتمـاد الشـركات الحكوميـة والخاصـة علـى الخدمـات السـحابية ونقـل البيانـات عبـر الشـبكات وانتشـار ثقافـة العمـل عـن بُعـد؛ تُواجـه بيئـة العمـل تهديـدات سيبرانيـة مسـتمرّة، تشـمل الشـركات ككيانـات تجاريـة والعامليـن فيهـا؛ ممـا يُهـدّد اسـتقرار العمـل ويُؤثّـر علـى الإدارة والعامليـن، ويُهـدّد الاسـتقرار الاقتصـادي فـي الدولـة والمجتمـع.

هـذا الواقـع يتطلـب الاهتمـام المتزايـد بالحمايـة السيبرانية فـي بيئات العمل، ونشـر ثقافة السلامـة الرقميـة، وتحويلهـا إلـى ثقافـة تنظيميـة سـائدة لـدى العامليـن فـي مختلـف المسـتويات الإداريـة، فالحمايـة السيبرانيـة للشـركات لا تقـع علـى عاتـق المتخصّصيـن فـي الأمـن السيبرانـي وتكنولوجيـا المعلومـات فحسـب، بـل تمتـد لتشـمل العامليـن مـن غيـر المتخصّصيـن، خاصـةً أن العديـد مـن الهجمـات السيبرانيـة التـي تسـتهدف الشـركات قـد تبـدأ بـخرق أجهـزة أحـد الموظفيـن، وينتقـل الـخرق إلـى الشـركة بالكامـل.

إن الهجمـات السيبرانيـة أصبحـت أكثـر تعقيـداً وتنظيمـاً مـع مرور الوقـت؛ ممـا أدّى إلـى ارتفـاع الطلـب علـى حلـول وتدابيـر حمايـة متطـوّرة. كمـا أن المخاطـر السيبرانيـة لا تؤثّـر فقـط علـى اسـتمرارية العمـل، بـل تُـؤدّي إلـى حـدوث خسـائر ماليـة فادحـة، والإضرار بالسُّـمعة، والتحديـات القانونيـة.

المخاطر السيبرانية في بيئة العمل: طبيعتها وأنواعها

المخاطر السيبرانية في بيئات العمل متنوّعة، وتشمل عدّة مستويات من التهديدات التي تستهدف الأجهزة، والشبكات، والبيانات. ويمكن تقسيم هذه التهديدات إلى الفئات الآتية:

1 الهجمات من الداخل (Insider Threats)

تحدث الهجمات الداخلية من خلال إساءة موظّف حالي أو سابق استخدام صلاحياته للوصول إلى بيانات الشركة أو تعطيل العمليات. قد يكون الدافع من وراء هذه الهجمات عدم الدّراية بقواعد الأمن السيبراني والسلامة الرقمية، أو تحقيق مكاسب مالية غير مشروعة. وتزداد خطورة هذا النّوع من الهجمات بسبب معرفة المهاجم بتفاصيل النظام الداخلي للشركة؛ مما يُسهّل عليه استغلال الثغرات بفاعلية.

2 التهديدات المُتقدّمة المستمرّة (APT)

هي هجمات مُنظَّمة تُنفَّذ على مدى طويل؛ بهدف سرقة بيانات حسّاسة أو التّجسُّس على الأنظمة، وتحدث هذه الهجمات من قِبَل مجموعات مُتقدّمة تقنياً، وتستهدف غالباً البنوك، والحكومات، أو الشركات العاملة في قطاعات البنية التحتية الحسّاسة[1].

1.Advanced persistent threat (APT), Imperva , on site: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

3 الخروقات السحابية (Cloud Security Breaches)

مـع انتقـال المزيـد مـن الشـركات إلـى الحوسـبة السـحابية، ظهـرت تحديـات جديدة تتعلـق بأمـن البيانـات المخزّنـة فـي السحابة؛ حيـث إنّ اسـتخدام خدمات التخزيـن السـحابية قـد يُعـرّض البيانـات للسـرقة؛ إذا لـم تكـن مُؤمَّنـة بشـكلٍ كافٍ. ولذلـك فالهجمـات التـي تسـتهدف مُزوّدي خدمـات السحابة قـد تـؤدّي إلـى تسريـب بيانـات حسّاسـة تخـصّ العديـد مـن العمـلاء فـي وقـت واحـد.

4 التصفُّح في المهملات (Dumpster Diving)

والمقصـود بـه المخاطـر السيبرانيـة التقليديـة التـي يسـتخدمها المهاجمـون للحصـول علـى معلومـات حسّاسـة عـن الشـركة أو الأفراد مـن خلال البحـث فـي النفايـات أو المهـملات، بمـا يشـمل مسـتندات ورقيـة تـم التخلُّـص منهـا بشـكلٍ غيـر آمِـن، مثـل:

- **كلمات مرور مكتوبة على الورق.**
- **مُسوَّدات اتفاقيات أو عقود.**
- **بيانات مصرفية أو معلومات مالية.**
- **معلومات حسّاسة عن الموظفين أو العملاء.**
- **ملاحظات تحتوي على تفاصيل الدخول إلى الأنظمة.**

يسـتغل المهاجـم حقيقـة أن العديـد مـن الشـركات أو الأفراد قـد يتخلّصـون مـن المسـتندات أو الأجهـزة الإلكترونيـة (مثـل الأقراص الصلبـة أو الهواتـف القديمـة) دون اتخـاذ الاحتياطـات المناسبة، مثـل: الإتلاف الكامـل؛ حيـث يقـوم المهاجمـون بتجميـع تلـك المعلومـات واسـتغلالها فـي هجمـات أكثـر تعقيـداً، مثـل: الهندسـة الاجتماعيـة أو سـرقة الهويـة[1].

1. Ramonas, Lukas. What is a dumpster diving attack, Nordvpn, may 2023, on site: https://nordvpn.com/blog/dumpster-diving-attack/

كيفية الحماية من التصفُّح في المهملات

- **إتلاف المستندات:**

يجب على الشركات والأفراد استخدام ماكينات تمزيق الورق؛ للتخلُّص من المستندات التي تحتوي على معلومات حسّاسة.

- **التخلُّص الآمِن من الأجهزة الإلكترونية:**

ينبغي التأكد من مسح جميع البيانات بشكلٍ نهائيّ من الأجهزة القديمة قبل التخلُّص منها، أو تدميرها بشكلٍ ماديّ إذا لزم الأمر.

- **التوعية والتدريب:**

ينبغي توعية الموظفين حول أهمية التخلُّص الآمِن من المستندات والأجهزة التي تحتوي على معلومات سريّة.

إنّ التصفُّح في المهملات يُمثّل تهديداً بسيطاً ظاهرياً، لكنّه يمكن أن يكون مدخلاً للحصول على معلومات قد تُسهّل تنفيذ هجمات أخرى.

تأثير المخاطر السيبرانية على بيئة العمل

يمكـن للتهديـدات السيبرانيـة التـي تُواجـه بيئـة العمـل أن تُؤثّـر بشـكلٍ حـادّ علـى المؤسسـات بـطرق متعـددة، فيمـا يلـي تبيـان لأهمهـا:

1 الخسائر المالية

تُعـدّ الخسـائر الماليـة مـن أخطـر النتائـج المترتبـة علـى الهجمـات السـيبرانية، وقـد تكـون هـذه التكاليـف ناتجـة عـن عـدة عوامـل، مثـل:

- **إصـلاح الأضـرار:** بعـد الهجـوم، يتعيّـن علـى الشـركات إصـلاح أنظمتهـا واسـتعادة البيانـات المتضـرّرة.
- **دفـع الفديـة:** فـي حالـة هجمـات الفديـة، قـد تضطـرّ الشـركات إلـى دفـع مبالـغ ضخمـة لاسـتعادة بياناتهـا.
- **خسـارة الإيـرادات:** إذا تسـبّبت الهجمـات فـي تعطيـل العمليـات لفتـرة طويلـة، قـد تتأثّـر الإيـرادات بشـكلٍ كبيـرٍ.

2 التأثير على السُّمعة

عندما تتعرَّض شركة لهجوم سيبراني يتسبّب في تسرُّب بيانات العملاء، قد تتأثّر سُمعتها بشكلٍ لا يمكن إصلاحه؛ حيث إنّ فقدان ثقة العملاء والشركاء يمكن أن يؤدي إلى خسارة العملاء والفرص التجارية المستقبلية، كما حدث مع شركة Sony Pictures Entertainment في نوفمبر 2014، فقد تعرّضت الشركة لهجوم سيبراني كبير نُسِب إلى مجموعة تُدعَى «Guardians of Peace». الهجوم أدّى إلى تسريب كميات كبيرة من البيانات الحسّاسة بما في ذلك رسائل البريد الإلكتروني، والمعلومات الشخصية للموظفين[1].

3 التّبعات القانونية والتنظيمية

تفرض العديد من الدول تشريعات صارمة حول حماية البيانات الشخصية، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي؛ وذلك لأنّ أيّ تسرُّب للبيانات قد يؤدّي إلى عقوبات قانونية وغرامات مالية[2].

1. Cieply, Michael and Brooks Barnes, Sony Cyberattack, first a Nuisance, Swiftly Grew Into a Firestorm, The New York Times, December 2014, on site: https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

2 . What-is-gdpr? Gdpr, on site: https://gdpr.eu/what-is-gdpr/.

العمل عن بُعد والمخاطر السيبرانية

مع تبنّي العديد من الشركات لسياسات العمل عن بُعد، أصبحت المخاطر السيبرانية المتعلّقة بهذا النموذج من العمل أكثر شيوعاً. ومن أبرز التحديات التي تُواجه المؤسسات ما يلي:

1 الوصول غير الآمِن إلى البيانات

عندما يعمل الموظّفون من منازلهم، يعتمدون على شبكات الإنترنت الشخصية للوصول إلى بيانات الشركة. في كثيرٍ من الأحيان، تكون هذه الشبكات أقل أماناً من شبكات الشّركات المحمية بجدران حماية (Firewalls)، وأنظمة كشف التسلُّل (IDS). بالإضافة إلى استخدام شبكات Wi-Fi غير مؤمَّنة تُعرِّض بيانات الشركة لخطر الخرق.

كما أن استخدام الأجهزة الشخصية في العمل يُشكّل خطراً كبيراً على أمان البيانات وسلامة الأنظمة؛ حيث إن الأجهزة الشخصية غالباً ما تكون أقل حماية من الأجهزة المخصّصة من قِبَل الشركة، فهي تفتقر إلى البرامج الأمنية المناسبة، وقد لا تخضع للتحديثات الدورية؛ مما يجعلها عُرْضَة للهجمات السيبرانية التي قد تؤدّي إلى تسريب بيانات حسّاسة أو اختراق أنظمة العمل.

إضافةً إلى ذلك، فإن نقل الملفات الحسّاسة إلى الأجهزة الشخصية يزيد من احتمالية تسرُّب المعلومات، خاصةً إذا تم تخزينها أو مشاركتها عبر وسائل غير آمِنة. لهذا السبب، يجب على الموظفين الالتزام بتخزين الملفات على خوادم الشركة الداخلية، واستخدام الأنظمة المعتَمَدة فقط. كما أن استخدام شبكة الإنترنت العامة أو المنزلية للعمل يُعرّض البيانات لخطر التّجسُّس أو الاعتراض. لذا يُنصَح بالاعتماد على شبكة الشركة الداخلية التي تُوفّر مستويات عالية من الأمان. كما يمكن للشركات تفعيل خدمات الشبكات الافتراضية الخاصة (VPN) لضمان الاتصال الآمِن للعاملين عن بُعد؛ مما يتيح لهم الوصول الآمِن إلى الملفات والأنظمة دون المساس بسريّة البيانات.

2 الأجهزة الشخصية غير المؤمَّنة

في أثناء العمل عن بُعد، قد يستخدم الموظفون أجهزة شخصية غير مُؤمَّنة بشكلٍ كافٍ، فقد تفتقر هذه الأجهزة إلى أحدث تحديثات الأمان أو برامج مكافحة الفيروسات؛ مما يجعلها أهدافاً سهلة للبرمجيات الخبيثة. كما أن مشاركة هذه الأجهزة مع أفراد العائلة قد تؤدّي إلى زيادة المخاطر.

3 إدارة الهوية والوصول (IAM)

من أكبر التحديات التي تُواجِه الشركات في أثناء العمل عن بُعْد: ضمان أن الوصول إلى البيانات يتم بطريقة آمِنَة؛ حيث تُعدّ إدارة الهوية والوصول (Identity and Access Management) أمراً بالغ الأهمية لضمان أن الأفراد الذين يصلون إلى الأنظمة لديهم الصلاحيات المناسبة فقط[1]، كما أن استخدام كلمات مرور ضعيفة أو عدم تفعيل المصادقة الثنائية (2FA) يُعرّض الأنظمة لخطر الاختراق.

1. Microsoft, on site: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam.

4 استخدام التطبيقات السحابية

مع اعتماد العديد من الشركات على التطبيقات السحابية في أثناء العمل عن بُعد، يجب أن تكون هذه التطبيقات مُؤمَّنة بشكلٍ كافٍ؛ وذلك لأنّ أيّ ثغرة في أمان هذه التطبيقات يمكن أن تؤدّي إلى تسرّب البيانات.

5 زيادة التعرُّض لهجمات الهندسة الاجتماعية

بسبب ابتعاد العاملين في نظام العمل عن بُعد عن زملائهم ورؤسائهم، قد يكون من الصعب عليهم التحقُّق من رسائل البريد الإلكتروني التي تصلهم، أو المكالمات الهاتفية فيما إذا كانت حقيقية أو مزيَّفة؛ مما يؤدّي إلى زيادة تعرُّضهم لأساليب الهندسة الاجتماعية، مثل التصيد الاحتيالي.

إستراتيجيات مواجهة المخاطر السيبرانية في بيئة العمل عن بُعْد

لتقليل المخاطر السيبرانية في بيئة العمل عن بُعد، يتعيّن على الشركات اتباع إستراتيجيات متعددة الأوجه تشمل الآتي:

1

التدريب والتوعية

لا بدّ للشركات من تنظيم برامج تدريبية منتظمة لتعريف الموظفين بالمخاطر السيبرانية وأفضل الممارسات لتجنُّبها. وتوعيتهم بالسلامة الرقمية في بيئة العمل، وكيفية الإبلاغ عن الحوادث، وغيرها من أُسس الأمن السيبراني والسلامة الرقمية.

2

حماية البيانات المُهمّة والحسّاسة

إنّ إدارة حقوق الوصول من خلال منح الموظفين صلاحيات محدودة واستخدام المصادقة متعددة العوامل (MFA) أمر ضروريّ. ولحماية البيانات الحسّاسة في بيئة العمل، يجب تصنيفها وفق حساسيّتها وتطبيق التشفير لحمايتها في أثناء النقل والتخزين. كما يجب التأكد من الحذف الآمِن للبيانات عند عدم الحاجة إليها باستخدام برامج متخصّصة أو تدمير وسائط التخزين.

وتُعدّ النُّسخ الاحتياطية المشفّرة، والمراقبة المستمرة عبر أنظمة كشف التهديدات (IDS/IPS)، وتدريب الموظفين على الأمن السيبراني أدوات فعّالة لحماية البيانات. وفي البيئات السحابية، يجب اختيار مُقدّمي خدمات سحابية آمِنة تعتمد على التشفير وسياسات صارمة لإدارة الوصول. كما أن الامتثال للتشريعات مثل اللائحة العامة لحماية البيانات (GDPR) أمر أساسيّ، ومن المُستحسَن إجراء تدقيق أمني دَوري للتأكُّد من فاعلية السياسات الأمنية.

3

استخدام الشبكات الافتراضية الخاصة (VPN)

على الشركات التأكُّد من أن جميع الموظفين الذين يعملون عن بُعْد يستخدمون شبكات VPN آمِنة، فهذه الشبكات تقوم بتشفير الاتصال بين الجهاز والشبكة الداخلية للشركة؛ مما يجعل من الصعب على المهاجمين اعتراض البيانات[1].

وللتحكُّم في الوصول إلى البيانات والأنظمة الحسّاسة، يمكن استخدام نظام إدارة الهوية والوصول (IAM) الذي يعتمد على الصلاحيات القائمة على الأدوار لضمان أن الموظفين لا يمكنهم الوصول إلا إلى المعلومات التي يحتاجون إليها لأداء مَهامّهم. كما يمكن تفعيل المصادقة الثنائية (2FA) لزيادة مستوى الأمان ومنع الوصول غير المصرَّح به.

1. What is a VPN? Microsoft, on site: https://linksshortcut.com/oFBiU.

4

تشفير البيانات

يُعدّ تشفير البيانات من أفضل الأساليب لحمايتها سواء أكانت البيانات مخزّنة على أجهزة الموظفين أو في أثناء نقلها عبر الشبكة. ولذلك يجب تشفير جميع البيانات الحسّاسة؛ مما يعني أن المهاجمين لن يتمكّنوا من قراءتها حتى لو تمكّنوا من الوصول إليها؛ حيث يُعدّ تطبيق التشفير المُتقدّم على مستوى النظام الأساسي والتطبيقات المستخدَمة خطوةً حاسمةً لضمان حماية المعلومات.

5

تطبيق حلول إدارة الأجهزة المحمولة (MDM)

في أثناء العمل عن بُعد، يستخدم الموظّفون في كثير من الأحيان أجهزة محمولة للوصول إلى أنظمة الشركة. ولتأمين هذه الأجهزة، يمكن استخدام حلول إدارة الأجهزة المحمولة (Mobile Device Management - MDM)، التي تسمح للشركات بالتحكُّم في الأجهزة، وتفعيل القيود، وتتبُّعها في حالة فقدانها أو سرقتها[1].

6

استمرار المُراقَبة والتحليل الأمني

من الضروري أن تُراقِب الشركات، بشكلٍ مستمرٍّ، جميع الأنظمة والبنية التحتية للتعرُّف على أي نشاط مشبوه أو اختراقات محتملة. كما يمكن استخدام أنظمة كشف التسلُّل (IDS)، ومنع التسلُّل (IPS) لمراقَبة حركة المرور على الشبكة وتحليلها للكشف عن أي سلوك غير معتاد.

1. What is mobile device management (MDM)? IBM, on site: https://www.ibm.com/topics/mobile-device-management.

7

السياسات الصارمة لاستخدام التطبيقات السحابية

لا بـدّ للشـركات التـي تعتمـد علـى الحوسـبة السـحابية مـن وضـع سياسـات صارمـة لاسـتخدام التطبيقـات السـحابية، بمـا فـي ذلـك التأكُّـد مـن أن جميـع التطبيقـات المستخدَمة مُؤمَّنة بشكلٍ جيدٍ، وأن تدعم معايير الأمان، مثل: تشفير البيانات، وتطبيق إدارة الهويـات، والمصادَقـة.

8

التحديثات الدورية وصيانة الأنظمة

مـن الـضروري الحـرص علـى التحديـث المسـتمر لجميـع الأنظمـة والتطبيقـات لضمـان وجـود أحـدث التصحيحـات الأمنيـة؛ وذلـك لكـون الهجمـات السيبرانيـة تسـتغلّ غالبـاً الثـغرات التـي يتـم اكتشـافها فـي التطبيقـات القديمـة. لذلـك فـإن التحديـث المُنتظِـم للأجهـزة والبرمجيـات يُعـدّ خطـوةً مُهمّـةً للحمايـة مـن هـذه التهديـدات.

9

إدارة الاجتماعات وأمانها

تُعدّ إدارة الاجتماعات وأمانها من الجوانب الحيوية في تعزيز الأمن السيبراني في أثناء العمل عن بُعد. ومع الاعتماد المتزايد على أدوات الاجتماعات الافتراضية، مثل: Zoom وMicrosoft Teams، يُصبح من الضروري تطبيق ممارسات أمان صارمة لضمان أن الاجتماعات تحدث في بيئة آمِنة. كما ينبغي حماية الاجتماعات بكلمات مرور قوية وتفعيل ميزات الأمان مثل غرف الانتظار (Waiting Rooms)، التي تُتيح للمُنظّمين التحكُّم فيمَن يُسمَح له بالانضمام. كذلك، ومن المهم أيضاً استخدام تشفير شامل (End-to-End Encryption) للمحادثات؛ لضمان أن البيانات المتداوَلة خلال الاجتماعات، سواء أكانت ملفات أو محادثات، تبقى مُشفَّرة ومحجوبة عن المتسلّلين أو الجهات الخارجية غير المصرّح لها. وللحفاظ على أمان الاجتماعات، هناك عدّة توجيهات عملية؛ أهمّها:

- **استخدام كلمات مرور قوية:** لضمان خصوصية الاجتماعات وحَصْر الوصول على المدعوّين فقط.
- **تفعيل المصادقة الثنائية (2FA):** للتحقُّق من هويّة المشاركين وضمان أن الوصول يتم من خلال الأفراد المصرّح لهم فقط.
- **إغلاق الاجتماع بعد بدئه:** لمنع أي محاولات للانضمام بعد انطلاق الاجتماع.

بالإضافة إلى ذلك، يُعدّ استخدام سطح مكتب معزول (Virtual Desktop Infrastructure - VDI) من الحلول الفعّالة لتوفير بيئة عمل آمِنة ومستقلّة. هذا النظام يسمح للموظفين بالوصول إلى موارد الشركة عبر سطح مكتب افتراضي يُدار بالكامل من قِبَل الشركة، مما يَحدّ من تعرُّض البيانات الحسّاسة لأي برمجيات ضارَّة قد تكون موجودة على الأجهزة الشخصية للموظفين. وفيما يلي تبيان لفوائد سطح المكتب المعزول:

- **توفير حماية من البرمجيات الضّارَّة:** تضمن أن البرامج المثبتة محميّة وتُدار بشكلٍ مركزي دون تدخُّل من المُستخدِم.
- **فصل بيئة العمل عن الجهاز الشخصي:** مما يُقلّل من خطر تسريب البيانات أو استخدامها خارج إطار سياسات الأمان.
- **إدارة مركزية للتحديثات:** مما يضمن تطبيق آخر التحديثات الأمنية عبر جميع المُستخدِمين دون تأخير.

10

إدارة الهوية والوصول
(Identity and Access Management - IAM)

تُعدّ إدارة الهوية والوصول من الركائز الأساسية في الأمن السيبراني، خاصةً في ظل التحوُّل الكبير نحو العمل عن بُعد. وتُعنَى (IAM) بإدارة وتحديد الأفراد الذين يحق لهم الوصول إلى موارد وأنظمة المؤسسة، مع ضمان أن هؤلاء الأفراد لديهم الصلاحيات الضرورية فقط لأداء مَهامّهم؛ حيث يُساعد نظام IAM في التحكُّم في هوية المُستخدِمين، وتحديد صلاحياتهم، ويُعزّز من قُدرة الشركة على مراقبة الأنشطة وتفادي الانتهاكات، وتشتمل إدارة الهوية والوصول على أُسُس ومبادئ؛ من أهمّها:

- **مبدأ الحد الأدنى من الامتيازات (Principle of Least Privilege)**

واحدة من أفضل ممارسات IAM هي تطبيق مبدأ الحد الأدنى من الامتيازات، والذي يعني أن كل مُستخدِم يجب أن تكون لديه فقط تلك الصلاحيات الضرورية لأداء وظيفته. كما أن تقليل الصلاحيات غير الضرورية يُقلّل من فرص التعرُّض للاختراق أو إساءة الاستخدام. على سبيل المثال، موظّف في قسم المحاسبة لا يحتاج إلى الوصول إلى قواعد بيانات التسويق أو تطوير البرمجيات.

- **المصادقة متعددة العوامل (Multi-Factor Authentication - MFA)**

تُعدّ المصادقة متعددة العوامل (MFA) عنصراً أساسياً في تعزيز الأمان ضمن IAM؛ حيث تعتمد MFA على استخدام أكثر من وسيلة لتأكيد هويّة المُستخدِم، مثل شيء يعرفه المُستخدِم (كلمة المرور) وشيء يمتلكه (هاتف محمول لتلقّي رمز تحقق). كما يُعدّ استخدام MFA من أفضل الوسائل لدرء هجمات التصيد الاحتيالي (phishing)، وهجمات تخمين كلمات المرور. حتى إذا سُرِقَت كلمة المرور، فإن خطوة التحقق الإضافية تمنع أيّ محاولة دخول غير مُصرّح بها.

- **المراقبة والتدقيق المستمر (Continuous Monitoring and Auditing)**

مـن المهـامّ الرئيسـة لإدارة الهويـة والوصـول: مراقبـة جميـع الأنشـطة المتعلقـة بالدخـول إلـى الأنظمـة وتسـجيلها؛ حيـث يجـب مراقبـة سـجلات الوصـول باسـتمرار وتحليلهـا للكشـف عـن أي أنشـطة مشـبوهة أو محـاولات وصـول غيـر مُـبرّرة. علـى سبيـل المثـال، يمكـن كشـف المُسـتخدِمين الذيـن يحاولـون الوصـول إلـى مـوارد غيـر مسـموحة لهـم، أو أولئـك الذيـن يحاولـون الوصـول خـارج سـاعات العمـل المعتـادة إنّ التدقيـق المسـتمر يُمكّـن المؤسسـات مـن مراجعـة أنظمـة الوصـول، والتحقـق مـن الـتزام الموظفيـن بالسياسـات المحـدّدة. كمـا يمكـن إجراء اختبـارات دوريـة لمراجعـة الصلاحيـات، والتحقـق مـن أن الموظفيـن لا يمتلكـون صلاحيـات أكثـر ممـا يحتاجـون.

- **إدارة الهويات المؤتمتة (Automated Identity Management)**

فـي ظـل زيـادة تعقيـد الأنظمـة وعـدد المُسـتخدِمين العامليـن عـن بُعـد، أصبحـت إدارة الهويـات المؤتمتـة أمراً بالـغ الأهميـة؛ حيـث يمكـن للأنظمـة المؤتمتـة أن تُبسّـط عمليـات منـح وإلغـاء الصلاحيـات بشـكلٍ فعّـال وسريـع، ممـا يضمـن توفيـر المـوارد الصحيحـة للأفراد المناسبيـن دون تأخيـر. علـى سبيـل المثـال، عنـد تعييـن موظـف جديد، يمكـن للنظـام المؤتمـت إنشـاء حسـاب جديـد بسـرعة وإعطـاء الموظّـف الصلاحيـات المناسـبة بنـاءً علـى وظيفتـه.

بالمثـل، عنـد انتهـاء عقـد موظّـف أو انتقالـه إلـى وظيفـة أخـرى، يمكـن للنظـام إلغـاء صلاحياتـه أو تعديلهـا تلقائيـاً، ممّـا يَحـدّ مـن خطـر بقـاء الصلاحيـات غيـر الضروريـة مُتاحـة أمـام المُسـتخدِمين السـابقين.

- **إدارة الوصول القائم على الأدوار (Role-Based Access Control - RBAC)**

تُعدّ إدارة الوصول القائم على الأدوار (RBAC) أحد أساليب IAM الفعّالة التي تقوم على منح الصلاحيات بناءً على الدور الوظيفي للمُستخدِم بدلاً من منحه صلاحيات فردية. بمعنًى آخر، تُعطى الصلاحيات لمجموعة معيّنة من الأدوار التي يشغلها الموظفون، وكل مَن يشغل هذا الدور يحصل تلقائياً على الصلاحيات نفسها.

كما يُمكّن RBAC المؤسسات من تقليل تعقيدات إدارة الوصول، وضمان التوزيع العادل والمُنظَّم للصلاحيات. على سبيل المثال، جميع موظفي قسم المالية يحصلون على صلاحيات معيّنة، بينما قسم تكنولوجيا المعلومات لديه صلاحيات مختلفة.

- **إدارة الهوية في السحابة (Cloud IAM)**

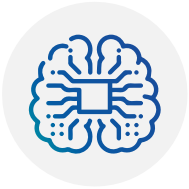
مع زيادة الاعتماد على الحوسبة السحابية، أصبحت إدارة الهوية والوصول في البيئة السحابية جزءاً أساسياً من إستراتيجية الأمان؛ حيث إنّها تُسهّل التحكم في الوصول إلى الموارد السحابية وإدارة الصلاحيات عبر العديد من المنصات السحابية المختلفة.

تُوفّر حلول Cloud IAM ميزات، مثل:

* **إدارة الوصول الموحَّدة:** يمكن للشركات استخدام منصة واحدة لإدارة الصلاحيات عبر عدّة خدمات سحابية.
* **التكامل مع خدمات المصادَقة:** مثل Google Cloud Identity أو Azure Active Directory لتوفير المصادَقة الموحَّدة، والتحكُّم المركزي في المُستخدِمين.
* **التقارير والتحليلات:** لمراقَبة وإدارة سجلات الوصول إلى الموارد السحابية.

- **تقليل الهجمات القائمة على سرقة الهوية (Identity Theft)**

تساعد IAM في حماية الشركات من الهجمات القائمة على سرقة الهوية. ومن الجدير بالذّكر أنّ سرقة الهوية من أساليب الاختراق الشهيرة التي يحاول فيها المهاجِم استخدام بيانات الدخول الخاصة بأحد الموظفين للوصول إلى الأنظمة الحسّاسة. ومن خلال استخدام IAM، يمكن تطبيق سياسات صارمة مثل مراجعة السلوكيات غير العادية للمُستخدِم، والتأكُّد من أن جميع عمليات الوصول تتم وفقاً للسياسات الأمنية.



تحديات إدارة المخاطر السيبرانية في المستقبل

مع التطور السريع للتكنولوجيا وزيادة الاعتماد على الذكاء الاصطناعي وإنترنت الأشياء (IoT) في بيئات العمل، تتزايد التهديدات السيبرانية بشكلٍ مستمرّ. ومن المتوقَّع أن تزداد الهجمات المعقَّدة التي تعتمد على الذكاء الاصطناعي واستخدام الروبوتات في المستقبل القريب. هذا يفرض على المؤسسات التعامل مع تحديات جديدة، وإيجاد طرق مُبتكَرة لتعزيز الأمن السيبراني.

1 الأمن السيبراني وإنترنت الأشياء (IoT)

أصبحت الأجهزة المتصلة بالإنترنت جزءاً لا يتجزّأ من حياة العديد من الشركات؛ مما أضاف طبقة جديدة من التعقيد إلى إدارة المخاطر؛ حيث إنّ كل جهاز متَّصل يُمثّل نقطة دخول محتَمَلة يمكن استغلالها من قِبَل المهاجمين. ولذلك يحتاج مدراء الأمن السيبراني إلى ضمان أن تكون جميع هذه الأجهزة مُؤمَّنة بشكلٍ كافٍ وتحت المراقَبة المستمرّة.

2 الذكاء الاصطناعي والهجمات المُتقدّمة

على الرغم من أنّ تقنيات الذكاء الاصطناعي تُقدّم فرصاً هائلة لتحسين الأمن السيبراني؛ إلا أنها تُوفّر أيضاً أدوات قوية للقراصنة؛ حيث يمكن استخدام الذكاء الاصطناعي لأتمتة الهجمات، وتحليل البيانات بسرعة كبيرة لاكتشاف الثغرات الأمنية. ولمواكَبة هذا التطور، تحتاج المؤسسات إلى تطوير تقنيات دفاعية تعتمد هي الأخرى على الذكاء الاصطناعي والتعلُّم الآلي؛ للكشف عن التهديدات بشكلٍ استباقيّ.

3 إدارة البيانات في بيئات العمل الهجينة

مع الانتقال المستمر بين العمل المكتبي والعمل عن بُعد، يُصبح من الضروري للشركات إدارة بياناتها بشكلٍ مَرِن وآمِن. كما يجب أن تضع الشركات إستراتيجيات تجعل من السهل على الموظفين الانتقال بين العمل في المكتب والعمل عن بُعد دون التأثير على الأمان. إنّ أحد الحلول الفعّالة في هذا السياق هو تبنّي البيئات الافتراضية (VDI) التي تسمح للموظفين بالوصول إلى بيئات العمل الخاصة بهم من أيّ مكان؛ مما يُقلّل من المخاطر المرتبطة بتخزين البيانات محلياً على الأجهزة الشخصية.

ومـع تقـدُّم التكنولوجيـا وتزايـد التهديـدات السيبرانيـة، أصبـح مـن الـضروري أن تتَّخـذ الشركات تدابير وقائية شاملة لحماية بيئات العمل التقليدية والبعيدة على حدّ سواء؛ حيـث يُعـدّ العمـل عـن بُعْـد تحديـاً إضافيـاً يتطلَّـب تطويـر إسـتراتيجيات أمنيـة مُتعـدّدة الأبعـاد تشـمل حمايـة البيانـات، والأجهـزة، والاتصـالات.

فالشـركات التـي تهمـل التعامـل مـع المخاطـر السيبرانيـة تجـد نفسـها عُرْضَـة لخسـائر ماليـة كبيـرة، وفقـدان ثقـة العـملاء، والتبعـات القانونيـة. لذلـك، لا يمكـن التعامـل مـع الأمـن السيبرانـي كخيـار، بـل هـو جـزء أساسـي مـن اسـتمرارية ونجـاح أيّ مؤسسـة فـي العصـر الرقمـي.

إنّ الأمـان السيبرانـي ليـس مهمّـة يمكـن القيـام بهـا مـرة واحـدة والانتهـاء منهـا، بـل عمليـة مسـتمرّة تتطلَّـب مراقبـة وتطـويراً مسـتمراً لمواجهـة التهديـدات المتغيِّرة باسـتمرار.

بروتوكول الإبلاغ عن الحوادث السيبرانية

عبارة عن مجموعة من الإجراءات والعمليات التي تتّبعها المؤسسات عند اكتشاف حادث أمني أو اختراق إلكتروني. والهدف من هذا البروتوكول هو ضمان التعامل الفوريّ والفعّال مع الحوادث السيبرانية لتقليل الأضرار، وحماية البيانات الحسّاسة، والحدّ من تأثير الحادث على العمليات التجارية.

العناصر الأساسية لبروتوكول الإبلاغ عن الحوادث

الكشف عن الحادث

تبدأ العملية عند اكتشاف خلل أمني؛ قد يكون ذلك من خلال مراقبة أنظمة الأمان، وتتبُّع تنبيهات الأمان من الأدوات السيبرانية، مثل جدران الحماية، أو أنظمة الكشف عن التسلُّل (IDS/IPS)، أو تلقِّي تقارير من الموظفين.

الإبلاغ الفوري

يجب أن يَتْبع الاكتشاف الإبلاغ الفوري للفِرَق المختصّة، مثل فريق أمن المعلومات (Security Operations Center - SOC) أو فريق الاستجابة للحوادث (Incident Response Team - IRT). ومن الضروري وجود نظام تواصُل واضح ومُحدَّد للإبلاغ عن الحوادث، سواء عبر البريد الإلكتروني أم عبر تطبيقات مخصَّصة للإبلاغ.

التصنيـف والتقييـم

بعـد الإبلاغ، يتـم تقييـم الحـادث لتحديـد خطورتـه وتصنيفـه وفقـاً لمعاييـر مُحـدّدة، مثـل تأثيـره علـى العمليـات الحيويـة للمؤسسـة، ونـوع البيانـات التـي تعرَّضـت للخطـر، ومـدى انتشـار الحـادث؛ حيـث تُساعد هـذه الخطـوة فـي تحديـد أولويـات الاسـتجابة.

الاستجابة الأوّلية

تتضمَّـن هـذه المرحلـة اتخـاذ الإجراءات الأوَّليـة للحـدّ مـن تأثيـر الحـادث. قـد تشـمل هـذه الإجراءات عزل النظـام المتأثّـر، أو إغلاق بعـض الأنظمـة، أو حظـر الاتصـالات المشـبوهة؛ وذلـك بهـدف منـع الانتشـار السريـع للهجـوم وتقليـل الأضرار.

التحليل والتحقيق

بمجـرّد التحكُّـم فـي الحـادث، يتـم إجراء تحقيـق شـامل لتحليـل كيفيـة حـدوث الحـادث، ومَـن الـذي يقـف وراءه، ومـا هـي نقـاط الضعـف التـي اسـتغلّها المهاجمـون. كمـا يتضمّـن التحليـل فحـص السـجلات، واسـتخراج الأدلَّـة الرقميـة، وإجراء مقابَلات مـع الشـهود إذا لـزم الأمـر.

التعافي واستعادة الأنظمة

بعـد احتـواء الحـادث وتحليلـه، يبـدأ العمـل علـى اسـتعادة الأنظمـة المتـضرّرة وإعادتهـا إلـى العمـل بشـكلٍ طبيعـي. وهنـا لا بـدّ مـن التأكُّـد مـن أن جميـع الأنظمـة تعمـل بأمـانٍ، وأنـه تـم القضـاء علـى أي نقـاط ضعـف تسـبّبت فـي الحـادث.

التوثيق

توثيق الحادث وجميع الخطوات المتَّخذة في أثناء الاستجابة يُعدّ جزءاً أساسياً من البروتوكول. ويتضمن ذلك كتابة تقرير شامل يُوضّح نوع الحادث، والإجراءات المتّخذة، والتوصيات لتحسين الأمان ومنع الحوادث المستقبلية.

الإبلاغ القانوني والتواصل مع الأطراف المعنيّة

قد يتطلّب الأمر -في بعض الحالات- إبلاغ السلطات المختصة، مثل: وكالات حماية البيانات أو هيئات إنفاذ القانون، خاصةً إذا كانت البيانات الشخصية قد تعرّضت للاختراق. أيضًا، قد يكون من الضروري التواصل مع العملاء أو الشُّركاء المتأثّرين بالحادث لإعلامهم بالوضع.

المراجعة والتحسين

بعد انتهاء المعالَجة، لا بدّ من عَقْد اجتماع لفريق الاستجابة لمراجعة الأداء والتأكُّد من فاعلية البروتوكول. تهدف هذه المرحلة إلى تحسين الخطط وتحديث السياسات لمنع وقوع حوادث مُشابِهة مستقبلاً.

وختاماً لهذا الفصل، ينبغي التأكيد على أن المخاطر السيبرانية في بيئة العمل ليست ثابتة، بل مُتطوّرة ومُتغيّرة تبعاً للتطورات السيبرانية، وعليه، لا بدّ من الحرص الدائم على تعزيز وعي العاملين بمفاهيم الأمن السيبراني والسلامة الرقمية؛ فإدارة المؤسسات عموماً وإدارة الأمن السيبراني وتكنولوجيا المعلومات بشكلٍ خاصٍّ ليست قادرة بمفردها على تعزيز استقرار بيئة العمل.

ولذا لا بدّ من تعاون جميع العاملين من المُتخصّصين وغير المُتخصّصين وفي مختلف المستويات الإدارية؛ لأن ثغرة تقنية أو معرفية واحدة قد تؤثّر على المؤسسة بالكامل؛ ممّا يُعزّز من أهمية مؤشرات الأمن السيبراني والسلامة الرقمية في بيئة العمل التقليدية وبيئة العمل عن بُعد.

أنشطة

النشاط الأول

ابحث عن أمثلة لهجمات سيبرانية تعرّضت لها بعض المؤسسات، ووَضِّح السبب الذي أدّى إلى الاختراق.

النشاط الثاني

في جدول من تصميمك؛ وضِّح الفرق بين التهديدات السيبرانية التي تُواجه نظام العمل عن بُعْد، ونظام العمل التقليدي.

النشاط الثالث

مهامّ تعزيز السلامة الرقمية في المؤسسات تقع على عاتق جميع العاملين في مختلف المستويات الإدارية. اكتب بحثاً عن كيفية تكامُل الأدوار بين المُتخصّصين في الأمن السيبراني وتكنولوجيا المعلومات في المؤسسات، وغير المُتخصّصين.

الفصل الخامس
اللائحة العامة لحماية البيانات (GDPR)

- مقدمة
- اللائحة العامة لحماية البيانات (GDPR)
- المبادئ الأساسية للائحة العامة لحماية البيانات (GDPR)
- العقوبات في اللائحة العامة لحماية البيانات (GDPR)
- متطلبات الموافقة على اللائحة العامة لحماية البيانات (GDPR)
- دور اللائحة العامة لحماية البيانات (GDPR) في تعزيز السلامة الرقمية
- القانون رقم 13 لسنة 2016 بشأن حماية البيانات الشخصية في قطر
- حقوق الأفراد في القانون القطري
- دور القانون في تعزيز السلامة الرقمية في قطر
- قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم (14) لسنة 2014
- دور قانون مكافحة الجرائم الإلكترونية في تعزيز السلامة الرقمية
- أنشطة

مقدمة

تضطلع قوانين حماية البيانات بدَوْر مُهمّ في حماية خصوصية الأفراد، وتعزيز الثقة بالمؤسسات؛ من خلال ضمان حقوق الأفراد في التحكُّم في معلوماتهم الشخصية، كما تُسهم هذه القوانين في خلق بيئة عمل آمِنة، كما تُحدّد المسؤوليات والالتزامات للمؤسسات، ما يُسهّل عملية الامتثال.

كما تُعزّز هذه القوانين أيضاً من السلامة الرقمية؛ من خلال توفير تدابير لحماية البيانات من الانتهاكات، كما تُسهم في دعم التنمية الاقتصادية والابتكار من خلال توفير إطار قانوني واضح وموثوق. ولذلك تحرص غالبية الدول على تطوير قوانين خاصة بها لحماية البيانات، إضافةً إلى وجود لوائح وبروتوكولات دولية تهتمّ بأمن البيانات.

وانطلاقاً من أهمية هذه اللوائح؛ سيتم تخصيص هذا الفصل لدراسة وتحليل هذه اللوائح وتحديد دورها في حماية البيانات على المستويين الفردي والمؤسسي.

اللائحة العامة لحماية البيانات (GDPR)

تُعدّ اللائحة العامة لحماية البيانات (GDPR) واحدةً من أهم التشريعات في مجال حماية البيانات الشخصية في العالم، وقد تم اعتمادها مِن قِبَل الاتحاد الأوروبي في أبريل 2016، ودخلت حيّز التنفيذ في 25 مايو 2018. وتهدف GDPR إلى تعزيز حماية البيانات الشخصية للأفراد داخل الاتحاد الأوروبي، وتوفير إطار عمل موحَّد لحماية الخصوصية.

العناصر الأساسية لبروتوكول الإبلاغ عن الحوادث

تهدف اللائحة العامة لحماية البيانات إلى تحقيق ما يلي:

1 حماية البيانات الشخصية

- **الهدف الرئيس:** تهدف GDPR إلى حماية المعلومات الشخصية للأفراد، مثل: الاسم، والعنوان، ورقم الهاتف، والبريد الإلكتروني، والمعلومات المالية.
- **التأكيد على الخصوصية:** يسعى القانون إلى ضمان أن تبقى البيانات الشخصية سريّة، ولا تُستخدَم بطرقٍ تتعارض مع حقوق الأفراد.

2 تعزيز الشفافية

- **الإفصاح عن المعلومات:** يتطلب من الشركات إبلاغ الأفراد بكيفية جمع بياناتهم، والأغراض التي تُستخدَم من أجلها، والأطراف التي قد تُشارك معها.
- **المعلومات الواضحة:** يجب أن تكون المعلومات المقدَّمة سهلة الفهم، ما يُساعد الأفراد على اتخاذ قرارات مستنيرة بشأن بياناتهم.

3 تمكين الأفراد

- **حقوق الأفراد:** يمنح GDPR الأفراد مجموعة من الحقوق، بما يشمل اطلاعهم على كيفية استخدام بياناتهم، والحقّ في استعادتها، ما يَمنحهم السيطرة على بياناتهم الشخصية.
- **المشاركة الفعَّالة:** تُعزّز من قدرة الأفراد على اتخاذ قرارات بشأن كيفية استخدام معلوماتهم، ما يزيد من شعورهم بالأمان والثقة.

4 توحيد القوانين في الاتحاد الأوروبي

- **إطار قانوني موحَّد:** يهدف GDPR إلى توحيد تشريعات حماية البيانات عبر الدول الأعضاء في الاتحاد الأوروبي، ما يُسهّل على الشركات الالتزام بالقوانين المختلفة.
- **تقليل التعقيد:** يُسهم في تقليل التعقيد الإداري والتنظيمي الذي قد تُواجهه الشركات عند العمل في دُوَل متعدّدة.

5 تعزيز الأمان

- **متطلبات الأمان:** يشدّد GDPR على ضرورة اتّخاذ تدابير أمان قوية لحماية البيانات الشخصية من الوصول غير المصرَّح به، والتسريبات، والهجمات الإلكترونية.
- **التقييم المنتظم:** يتعيَّن على الشركات إجراء تقييمات منتظمة لمخاطر البيانات واتباع أفضل الممارسات في حماية المعلومات.

6 الحدّ من البيانات

- **جمع البيانات الضرورية فقط:** يُشدّد GDPR على ضرورة جمع البيانات فقط بالقَدْر اللازم لتحقيق الأغراض المصرَّح بها، ما يُقلّل من حجم البيانات المخزَّنة والمخاطر المرتبطة بها.
- **التقليل من التخزين:** يَحُدّ من الاحتفاظ بالبيانات لفترات طويلة، ما يُقلّل من تعرُّض الأفراد لمخاطر التسريبات.

7 توفير حقوق إضافية للأفراد

- **الحق في الوصول:** يحقّ للأفراد معرفة ما إذا كانت بياناتهم تُعالَج، وما هي هذه البيانات.
- **الحق في التصحيح:** يمكن للأفراد طلب تصحيح أيّ معلومات غير دقيقة.
- **الحق في الحذف:** يمكنهم طلب حذف بياناتهم في حالات معينة.
- **الحق في نقل البيانات:** يمكنهم نقل بياناتهم إلى مزوّد خدمة آخر؛ إذا رغبوا في ذلك.
- **الحق في الاعتراض:** يمكنهم الاعتراض على مُعالَجة بياناتهم لأغراض معيَّنة، مثل التسويق المباشر.

8 تطوير ثقافة الامتثال

- **تعزيز الالتزام بالقوانين:** يهدف GDPR إلى تعزيز ثقافة الامتثال داخل المؤسسات من خلال توفير إطار عمل واضح.
- **التدريب والتوعية:** يُتطلّب من الشركات توفير تدريب لموظفيها حول أهمية حماية البيانات وحقوق الأفراد، ما يُسهم في تحسين مستوى الوعي لدى العاملين.

9 زيادة الثقة بين الأفراد والشركات

- **بناء الثقة:** من خلال حماية البيانات الشخصية وتعزيز الشفافية، يُسهم GDPR في بناء الثقة بين الأفراد والشركات.
- **تحسين العلاقات:** تُعزّز هذه الثقة من العلاقات بين المستهلكين والشركات، ما يؤدي إلى تجربة مستخدِم أفضل.

10 التكيُّف مع البيئة الرقمية المتغيرة

- **استجابة للتطورات التكنولوجية:** يهدف GDPR إلى مواكبة التطورات السريعة في مجال تكنولوجيا المعلومات وحماية البيانات، ما يضمن حماية الأفراد في عالَم رقميّ متزايد التعقيد.
- **المرونة:** يُتيح للإدارات التكيُّف مع التغيرات في كيفية معالجة البيانات الشخصية.

المبادئ الأساسية للائحة العامة لحماية البيانات (GDPR)

تتضمَّن GDPR مجموعة من المبادئ الأساسية التي يجب على المؤسسات الالتزام بها:

1 الشرعية والشفافية

- **معالجة قانونية:** يجب أن تتمّ معالجة البيانات الشخصية بطريقة قانونية وعادلة.
- **الإفصاح:** يتعيَّن على المؤسسات إبلاغ الأفراد بطريقةٍ واضحةٍ عن كيفية معالجة بياناتهم، بما في ذلك الأغراض والوسائل المستخدَمة.

2 الحدّ من جمع البيانات

- **جمع مُحدّد للبيانات:** يجب أن تُجمَع البيانات الشخصية لأغراض مُحدَّدة ومشروعة، ولا يمكن استخدامها لأغراض أخرى غير مقبولة.
- **الوضوح في الأغراض:** يجب أن تكون الأغراض التي يتم جمع البيانات من أجلها واضحة ومُعلَنة للأفراد.

3 الحدّ من البيانات

- **المعالجة المناسبة:** يجب أن تكون البيانات الشخصية ملائمة وضرورية فقط لتحقيق الأهداف المحدَّدة.
- **تقليل البيانات:** يجب تجنُّب جمع البيانات الزائدة عن الحاجة.

4 الدقَّة

- **تحديث البيانات:** يجب أن تكون البيانات دقيقة ومحدَّثة. يتعيَّن على المؤسسات اتخاذ الخطوات اللازمة لتصحيح أيّ معلومات غير دقيقة دون تأخير.
- **المسؤولية عن الدقَّة:** تقع مسؤولية الحفاظ على دقَّة البيانات على عاتق المؤسسات.

4 الاحتفاظ بالبيانات

- **فترة الاحتفاظ:** يجب عدم الاحتفاظ بالبيانات الشخصية لفترةٍ أطول مما هو ضروري لتحقيق الغرض الذي تم جمعها من أجله؛ وذلك لكون طول مدة الاحتفاظ يزيد من مستوى المخاطر التي تتعرَّض لها هذه البيانات.
- **تحديد الفترات:** يجب على المؤسسات تحديد الفترات الزمنية للاحتفاظ بالبيانات بناءً على الغرض من المعالجة. بمعنى أنه يجب على المؤسسات أن تُحدّد بشكلٍ مُسبقٍ المدة التي سيتم الاحتفاظ خلالها بالبيانات.

5 الأمان

- **حمايـة البيانـات:** يجـب اتخـاذ تدابيـر فنيـة وتنظيميـة مناسـبة لضمـان حمايـة البيانـات الشـخصية مـن المعالَجـة غيـر المصـرَّح بهـا أو الضيـاع.
- **الإبـلاغ عـن الانتهـاكات:** يتعيـن علـى المؤسسـات الإبـلاغ عـن أيّ انتهـاكات محتَمَلـة للبيانـات فـي الوقـت المناسـب، وفقـاً للقوانيـن.

6 المسؤولية

- **الامتثال:** يجـب علـى المؤسسـات أن تكـون قـادرة علـى إثبـات امتثالهـا لمبـادئ GDPR، مـا يعنـي وجـود إجـراءات داخليـة وتوثيـق جيـد.
- **تقييـم المخاطـر:** يتعيَّـن علـى المؤسسـات إجـراء تقييمـات منتظِمـة لمخاطـر البيانـات واتخـاذ الإجـراءات اللازمـة للتقليـل مـن هـذه المخاطـر.

العقوبات في اللائحة العامة لحماية البيانات (GDPR)

تفرض GDPR عقوبات صارمة على المؤسسات التي تنتهك القواعد، وتهدف هذه العقوبات إلى تعزيز الامتثال والحثّ على احترام حقوق الأفراد.

أنواع العقوبات

تتضمّن العقوبات المفروضة بموجب GDPR نوعين رئيسين:

1 الغرامات المالية

- قد تصل إلى 20 مليون يورو، أو 4 % من الإيرادات العالمية السنوية، بحسب القيمة الأكبر[1].
- تُفرَض الغرامات بناءً على خطورة الانتهاك، ومدى تأثيره على الأفراد، ومدى تعاون المؤسسة مع السلطات.

2 الإجراءات التصحيحية

يمكن للسلطات فرض إجراءات تصحيحية، مثل:

- وقف معالجة البيانات، وذلك في حال وجود أيّ خطر عليها.
- إلزام المؤسسات بتصحيح البيانات أو حذفها.
- اتخاذ تدابير أخرى لتعزيز الامتثال.

1. What are the GDPR Fines? on site: https://gdpr.eu/fines/.

معايير تحديد العقوبات

تأخذ السلطات في الاعتبار عدة عوامل عند تحديد العقوبات، منها:

1

طبيعة الانتهاك

مدى خطورة الانتهاك وتأثيره على حقوق الأفراد.

2

الامتثال السابق

ما إذا كانت المؤسسة قد قامت بانتهاكات سابقة.

3

التعاون مع السلطات

مدى تعاون المؤسسة مع السلطات في أثناء التحقيق.

4

التدابير المتَّخذة

ما إذا كانت المؤسسة قد اتَّخذت تدابير لمنع الانتهاكات المستقبلية.

الإبلاغ عن الانتهاكات

يتعيَّن على المؤسسات الإبلاغ عن أيّ انتهاكات للبيانات خلال 72 ساعة من معرفتها بالحادثة إذا كان هناك خطر على حقوق الأفراد، وإذا كان الانتهاك خطيراً، يجب إبلاغ الأفراد المتأثرين أيضاً.

أمثلة عن العقوبات

- أصـدر منظّمـو **اللائحـة العامـة لحمايـة البيانـات (GDPR)** مئـات الغرامـات علـى الشـركات، بمـا فـي ذلـك جوجـل وفيسـبوك، بأكثـر مـن **114** مليـون يـورو فـي أول 20 شـهراً مـن عـام 2020[1].

- فـي 17 ينايـر 2020، أعلنـت هيئـة الإشـراف الإيطاليـة أنهـا فرضـت غرامتيـن منفصلتين بقيمـة **8,5** مليـون يـورو، و**3** ملاييـن يـورو علـى شـركة Eni Gas e Luce EGL، وهـي شـركة توريـد الكهربـاء والغـاز الإيطاليـة، جـاءت هـذه الغرامـات ردّاً علـى انتهاكيـن منفصليـن للقانـون العـام لحمايـة البيانـات[2].

1. How the GDPR could change in 2020? on site: https://gdpr.eu/gdpr-in-2020/.

2. Italy fines Eni Gas e Luce €11.5 million for multiple GDPR violations, on site: https://gdpr.eu/italy-fines-energy-company-for-multiple-gdpr-violations/.

متطلبات الموافقة على اللائحة العامة لحماية البيانات (GDPR)

تتضمَّن متطلبات الموافقة في اللائحة العامة لحماية البيانات (GDPR) عدة عناصر أساسية لضمان أن تكون الموافقة صحيحة وقابلة للتطبيق، من أهمها:

1 الوضوح

- **المعلومات واضحة:** يجب أن تكون المعلومات المقدَّمة للأفراد حول المعالجة واضحة وسهلة الفهم، ما يساعدهم على اتخاذ قرار سليم.
- **اللغة مفهومة:** يجب استخدام لغة سهلة ومباشرة، دون مصطلحات قانونية معقَّدة.

2 حرية الاختيار

- **عدم الضغط:** يجب أن يكون لدى الأفراد حرية كاملة في قبول أو رفض الموافقة على استخدام بياناتهم دون أيّ ضغوط أو تأثير.
- **عدم الربط:** لا يمكن اشتراط تقديم خدمة أو مُنتَج بموافقة الأفراد على معالجة بياناتهم، إلا إذا كانت المعالجة ضرورية لتقديم تلك الخدمة.

3 موافقة مُحدَّدة

- **أغـراض مُحـدَّدة:** يجـب أن تكـون الموافَقـة مُعطـاة لأغـراض معيَّنـة ومُحـدَّدة، وليسـت موافَقـة عامَّـة أو غيـر مُحـدَّدة.
- **التمييـز بيـن الأغـراض:** يجـب أن يتـمّ طلـب الموافَقـة بشـكلٍ منفصـلٍ لـكل غـرض مـن أغـراض المعالَجـة.

4 قابلية السحب

- **الحـقّ فـي سـحب الموافقـة:** يجـب أن يكـون للأفـراد الحـق فـي سـحب موافقتهـم فـي أيّ وقـت، ويجـب أن تكـون عمليـة السـحب سـهلة مثـل عمليـة إعطـاء الموافقـة.
- **إبلاغ الأفراد:** يجب إبلاغ الأفراد بأن لهم الحق في سحب موافقتهم.

5 تسجيل الموافقة

- **تأكيـد الموافقـة:** يجـب علـى المؤسسـات الاحتفـاظ بسـجلات تُؤكّـد أن الأفـراد قـد أعطـوا موافقتهـم، مـع توثيـق كيفيـة إعطائهـا.
- **التاريـخ والوقـت:** يجـب أن تتضمَّـن السـجلات تاريـخ ووقـت تقديـم الموافقـة.

6 الشفافية

- **إبـلاغ الأفـراد:** يجـب أن يتـم إبـلاغ الأفـراد بوضـوح عـن كيفيـة اسـتخدام بياناتهـم، بمـا فـي ذلـك حقوقهـم.
- **تحديـث المعلومـات:** يجـب تحديـث المعلومـات المتعلّقـة بالموافقـة إذا تغيَّـرت طـرق المعالَجـة.

دور اللائحة العامة لحماية البيانات (GDPR) في تعزيز السلامة الرقمية

تضطلع اللائحة العامة لحماية البيانات (GDPR) بدَوْر مُهِمّ في تعزيز الأمن السيبراني والسلامة الرقمية، وفيما يلي بعض الجوانب الرئيسة لهذا الدور:

1 تحديد معايير الأمان

- **متطلَّبات الأمان:** تفرض GDPR على المؤسسات اتخاذ تدابير تقنية وتنظيمية مناسبة لحماية البيانات الشخصية. يتضمَّن ذلك حماية البيانات من الوصول غير المصرَّح به، والتسريبات، والخروقات.
- **تقييم المخاطر:** يتعيَّن على المؤسسات إجراء تقييمات منتظمة لمخاطر البيانات وتحديث تدابير الأمان وفقاً لذلك.

2 الإبلاغ عن الانتهاكات

- **الالتزام بالإبلاغ:** تفرض GDPR على المؤسسات الإبلاغ عن أيّ انتهاكات للبيانات خلال ٧٢ ساعة من اكتشافها، ما يُعزّز من سرعة الاستجابة، ويُقلّل من الأضرار المحتمَلة.
- **شفافية أكبر:** من خلال الإبلاغ عن الانتهاكات، تُسهم GDPR في تعزيز الشفافية والثقة بين الأفراد والمؤسسات.

3 تعزيز ثقافة الامتثال

- **التوعية والتدريب:** تشجّع GDPR المؤسسات على توفير التدريب والتوعية للموظفين حول أهمية حماية البيانات وأفضل الممارسات في الأمن السيبراني.
- **المسؤولية الإدارية:** تُعزّز من ثقافة المسؤولية داخل المؤسسات، ما يؤدّي إلى اتخاذ تدابير استباقية لحماية البيانات.

4 تطوير إستراتيجيات الأمان

- **إستراتيجيات شاملة:** تشجّع GDPR على تطوير إستراتيجيات شاملة للأمن السيبراني، تشمل جميع جوانب معالجة البيانات الشخصية.
- **الاستجابة للتهديدات:** يجب على المؤسسات أن تكون مستعدَّة للتعامل مع التهديدات السيبرانية، ما يُعزّز من مستوى الأمان بشكلٍ عامّ.

5 تعزيز حقوق الأفراد

- **تمكين الأفراد:** تمنح GDPR الأفراد حقوقاً أكبر في التحكُّم في بياناتهم، ما يُشجّعهم على اتخاذ خطوات لحماية معلوماتهم الشخصية.
- **توفير الشفافية:** من خلال إبلاغ الأفراد عن كيفية استخدام بياناتهم، تُعزّز GDPR من شعور الأفراد بالأمان والثقة.

6 الامتثال مع المعايير العالمية

- **مع القوانين الأخرى:** تُسهم GDPR في مواءمة المعايير الأمنية مع القوانين والتشريعات العالمية، ما يساعد المؤسسات على الامتثال لمتطلبات الأمن السيبراني الدولية.

إنـه فـي عصـر التكنولوجيـا الرقميـة المتقدّمـة، أصبحـت البيانـات الشـخصية مـن أهـم الأصـول التـي تحتـاج إلـى حمايـة، ولـذا برزت أهميـة حمايـة البيانـات فـي دولة قطـر كأحد الأبعـاد الأساسـية لتطويـر المجتمـع الرقمـي، وتعزيـز الثقـة بيـن الأفراد والمؤسسـات. وتسـعى الدولـة إلـى مواكبـة التطـورات العالميـة فـي مجـال حمايـة البيانـات، مـا يعكـس التزامهـا بحمايـة حقـوق الأفراد، وتعزيـز بيئـة آمِنـة للتعـاملات الرقميـة؛ مـن خلال وضـع إطـار قانونـي شـامل، مثـل القانـون رقـم 13 لسـنة 2016 بشـأن حمايـة البيانـات الشـخصية، والـذي يهـدف إلـى تنظيـم عمليـة جمـع واسـتخدام البيانـات، وضمـان حمايـة الخصوصيـة.

إن الاهتمـام بحمايـة البيانـات فـي الدولـة يُمثّـل جـزءاً مـن رؤيـة للتقـدُّم نحـو مجتمـع قائـم علـى المعرفـة، حيـث تُعـدّ الخصوصيـة وحمايـة البيانـات مـن العناصـر الأساسـية لتحقيـق التنميـة المسـتدامة وتعزيـز الثقـة فـي المؤسسـات.

القانون رقم 13 لسنة 2016 بشأن حماية البيانات الشخصية في قطر

يُمثّل إطاراً قانونياً مهمّاً يهدف إلى حماية البيانات الشخصية وضمان الخصوصية، تسري أحكام هذا القانون على البيانات الشخصية عندما تتم معالجتها على نحو إلكتروني، أو يتم الحصول عليها أو جمعها أو استخراجها على أيّ نحوٍ آخر؛ تمهيداً لمعالجتها إلكترونياً، أو تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية.

ويعرّف القانون «البيانات الشخصية» على أنها:

> أيّ معلومات تتعلّق بشخص طبيعي يمكن تحديد هويته بشكلٍ مباشرٍ أو غير مباشرٍ من خلال هذه المعلومات، أو عند الجمع بين هذه المعلومات مع بيانات أخرى. وهذا يشمل جميع البيانات التي يمكن من خلالها التعرّف على الفرد؛ سواء تم جمعها أو معالجتها إلكترونياً أو تقليدياً، مثل الأسماء، أرقام الهوية، البيانات الصحية، والعناوين

وتظهر أهمية القانون رقم 13 لسنة 2016 بشأن حماية البيانات الشخصية في الدولة؛ من خلال النقاط والمحاور التالية:

1 حماية خصوصية الأفراد

- **ضمان الحقوق:** يضمن القانون حقوق الأفراد في التحكُّم في معلوماتهم الشخصية؛ ما يُعزّز الخصوصية.
- **حماية المعلومات الحسّاسة:** يحمي البيانات الحسّاسة -مثل: المعلومات الصحية والمالية- من الاستخدام غير المصرَّح به.

2 تعزيز الثقة

- **بناء الثقة بين الأفراد والمؤسسات:** وجود إطار قانوني يحمي البيانات يُعزّز من شعور الأفراد بالأمان عند التعامل مع المؤسسات.
- **تحفيز التفاعل الرقمي:** يسهّل ذلك التفاعل الرقمي، ويساعد على تطوير خدمات جديدة.

3 تنظيم المعالَجة

- **إطار قانوني واضح:** يوفّر التنظيم اللازم لكيفية جمع واستخدام البيانات، ما يُسهّل على المؤسسات فَهْم التزاماتها.
- **تحديد المسؤوليات:** يُحدّد المسؤوليات المطلوبة من المؤسسات والأفراد عند التعامل مع البيانات.

4 الامتثال للمعايير الدولية

- **مواءمة التشريعات العالمية:** يُعزّز من مواءمة القوانين المحلية مع المعايير الدولية مثل اللائحة العامة لحماية البيانات(GDPR) .
- **تعزيز التعاون الدولي:** يُسهّل التعاون مع الدول الأخرى في مجال حماية البيانات.

حقوق الأفراد في القانون القطري

لكلّ فرد الحق في حماية خصوصية بياناته الشخصية، ولا يجوز معالجة تلك البيانات إلا في إطار الشفافية واحترام كرامة الإنسان والممارسات المقبولة، كما لا يجوز معالجة البيانات الشخصية إلا بعد الحصول على موافقة الفرد، ومن حقوق الفرد ما يلي:

- **سحب موافقته السابقة على معالجة بياناته الشخصية.**
- **الاعتراض على معالجة بياناته الشخصية إذا كانت غير ضرورية لتحقيق الأغراض التي جُمعت لأجلها.**
- **طلب حذف بياناته الشخصية أو محوها عند انتهاء الغرض الذي جُمعت لأجله معالجة تلك البيانات.**
- **طلب تصحيح بياناته الشخصية، مرفقاً به ما يُثبت صحة طلبه.**

وبشكلٍ عامٍّ ووفقاً للقانون القطري وقبل معالجة البينات الشخصية؛ يجب إخطار الأفراد بمجموعة من المعلومات، تشمل معلومات عن الجهة التي تقوم بمعالجة البيانات؛ والأغراض المشروعة لمعالجة البيانات الشخصية. إضافةً إلى الوصف الشامل والدقيق لأنشطة المعالجات، ودرجات الإفصاح عن البيانات الشخصية للأغراض المشروعة.

واجبات وحدات التحكُّم في البيانات الشخصية

- مراجعة إجراءات خصوصية البيانات.
- تحديد أجهزة المعالَجة المسؤولة عن حماية خصوصية البيانات الشخصية.
- التدريب ورفع الوعي بين مُعالِجي المعلومات.
- إنشاء النُّظم الداخلية الآمِنة لاستلام الشكاوى والنظر فيها.
- الإدارة الفعَّالة للبيانات الشخصية، واستخدام التقنيات المناسبة.
- إجراء مراجعة شاملة لتحديد مستوى الامتثال.
- التحقُّق من امتثال المعالِج للبيانات بالتعليمات الصادرة.

دور القانون في تعزيز السلامة الرقمية في قطر

يعمل هذا القانون على خَلْق بيئة رقمية آمِنة ومستدامة تدعم الابتكار والنمو في الدولة، كما يهدف إلى حماية المعلومات الشخصية للأفراد، ما يُعزّز من شعور الأمان لدى المستخدِمين عند التعامل مع الخدمات الرقمية، كما يُلزم المؤسسات بتطبيق تدابير أمنية لحماية البيانات، ما يضمن عدم تعرُّض المعلومات للاختراق أو الاستخدام غير المصرَّح به.

يُعزّز القانون أيضاً من الشفافية من خلال مَنْح الأفراد حقّ الاطلاع على كيفية استخدام بياناتهم، ما يُعزّز من قدرتهم على التحكُّم في معلوماتهم الشخصية، ويُسهم في رفع مستوى الوعي بأهمية حماية البيانات، ما يُعزّز ثقافة الأمان الرقمي في المجتمع.

قانون مكافحة الجرائم الإلكترونية الصادر بالقانون رقم (14) لسنة 2014

يهدف القانون إلى ضبط التصرُّفات غير القانونية على الإنترنت، وفَرْض عقوبات صارمة على مَن يقوم بارتكاب هذه الجرائم. ويتضمَّن القانون مواجَهة مجموعة من التصرُّفات غير القانونية، مثل: الاحتيال الإلكتروني، والتشهير بالأشخاص عبر الإنترنت، وغيرها. ويهدف القانون إلى حماية المستهلكين وضحايا الجرائم الإلكترونية، وتعزيز الأمان الإلكتروني في الدولة.

الأنواع المختلفة لجرائم الإنترنت في قانون مكافحة الجرائم الإلكترونية

يسعى القانون لمكافحة مجموعة واسعة من الجرائم الإلكترونية؛ بما يشمل: التحرش الإلكتروني، التشهير بالأشخاص عبر الإنترنت، إرسال الرسائل غير المرغوب فيها، التعليقات المسيئة، نشر المعلومات الشخصية دون إذن، سرقة الهوية الرقمية، القرصنة الإلكترونية، الاحتيال عبر التجارة الإلكترونية، والتلاعُب بالبيانات الشخصية للأفراد.

ولتعزيز الردع ضد الجرائم الإلكترونية؛ فَرَضَ القانون جملة عقوبات صارمة للأفراد الذين يرتكبون هذه الجرائم، فعلى سبيل المثال: يُعاقَب الشخص الذي يقوم بالتحايل على حسابات البنوك أو الدفع الإلكتروني بعقوبة تصل إلى السجن لمدة تتراوح بين ستة أشهر وخمس سنوات، ودفع غرامة تتراوح بين 10,000 و50,000 ريال قطري [1].

1. تفاصيل قانون الجرائم الإلكترونية في قطر، 2024، على الموقع: https://2u.pw/wga1FQvG.

أهمية قانون الجرائم الإلكترونية في قطر

يحمل القانون أهمية كبيرة في عدَّة جوانب، من أهمها ما يلي:

1 **حماية المجتمع:**

يوفّر القانون آلية قانونية لمكافحة الجرائم الإلكترونية التي تُهدّد الأفراد والمؤسسات.

2 **تعزيز الأمن السيبراني:**

يُحدّد القانون أنواع الجرائم والعقوبات، ما يُعزّز من الأمن السيبراني في البلاد.

3 **حماية البيانات الشخصية:**

يتضمَّن القانون نصوصاً تحمي البيانات الشخصية والمعلومات الحسّاسة من الانتهاك.

4 **رفع مستوى الوعي:**

يُسهم القانون في نشر الوعي حول مخاطر الجرائم الإلكترونية وطرق الحماية.

5 **تعزيز الثقة بالبيئة الرقمية:**

يُوفّر القانون إطاراً يُعزّز من ثقة الأفراد والشركات باستخدام الخدمات الرقمية.

6 **التعاون الدولي:**

يُشجّع القانون على التعاون مع الدول الأخرى لمواجَهة الجرائم الإلكترونية.

7 **ردع الجرائم:**

من خلال سنّ عقوبات صارمة؛ حيث تُسهم العقوبات في ردع الأفراد عن ارتكاب الجرائم الإلكترونية.

دور قانون مكافحة الجرائم الإلكترونية في تعزيز السلامة الرقمية

يُسهم هذا القانون في تعزيز السلامة الرقمية في الدولة من خلال عدة جوانب مهمَّة، ويهدف إلى مكافحة الجرائم التي تحدث في الفضاء السيبراني، ما يسهم في حماية الأفراد والمجتمع بشكلٍ عامّ.

كما يُحدّد القانون أنواع الجرائم الإلكترونية؛ مثل: القرصنة، والاحتيال، والتشهير، ما يساعد على توعية المجتمع بالمخاطر المحتَمَلة؛ من خلال تحديد العقوبات الرادعة للمخالِفين، ويُعزّز القانون من مبدأ الردع، ما يُقلّل من احتمالية ارتكاب الجرائم الإلكترونية.

ويُسهم القانون أيضاً في تعزيز التعاون بين الجهات المحلية والدولية لمكافحة الجرائم الإلكترونية، ما يُتيح تبادل المعلومات والخبرات لمواجَهة الجريمة بشكلٍ أكثر فاعلية، كما يتضمَّن القانون آليات لمراقبة الجرائم والتحقيق فيها، ما يُعزّز من قُدرة السلطات على التصدّي للمخاطر.

ختاماً لهذا الفصل، تزداد المخاطر السيبرانية التي تواجهها البيانات على المستوى الشخصي والمؤسسي، ما يُعزّز من أهمية القوانين واللوائح الناظمة لها، والتي تضع المعايير اللازمة لضمان أمنها وسلامتها، فالبيانات تُعدّ العماد الرئيس للفضاء السيبراني، وتعرُّضها للمخاطر يُهدّد الاستقرار الاجتماعي والاقتصادي.

وبشكلٍ عامّ، وعلى الرغم من أهمية القوانين في تعزيز أمن البيانات؛ إلا أنها لا تستطيع تحقيق الأمن دون تعاون فعَّال من الشركات والمؤسسات والأفراد؛ فالقوانين واللوائح هي ناظِم ومُوجِّه للجهود الفردية والمؤسسية وليست بديلاً عنها.

أنشطة

النشاط الأول

في جدول من تصميمك؛ وضّح نقاط الاتفاق ونقاط الاختلاف بين القانون رقم 13 لعام 2016 في دولة قطر، والخاص بحماية البيانات الشخصية، وبين اللائحة العامة لحماية البيانات (GDPR).

النشاط الثاني

يُعدّ قانون مكافحة الجرائم الإلكترونية في دولة قطر من القوانين المهمة في مجال تعزيز الأمن السيبراني.. وضّح كيف يُسهم هذا القانون في الحدّ من الجريمة الإلكترونية.

النشاط الثالث

البيانات الشخصية للأطفال من القضايا المهمَّة التي تسعى القوانين واللوائح العامة لتوفير الحماية لها.. ابحث في دور هذه القوانين واللوائح في حماية بيانات الأطفال، مُدَعِّماً إجابتك بالأمثلة اللازمة.


Ai Chatbot
Ai

الفصل السادس
مخاطر الذكاء الاصطناعي: التحديات في عصر التكنولوجيا المتقدّمة

- مقدمة
- الذكاء الاصطناعي وتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية
- مخاطر الذكاء الاصطناعي
- أمثلة عملية حقيقية على عمليات احتيال وتزييف باستخدام الذكاء الاصطناعي
- التصيد الاحتيالي المدعوم بالذكاء الاصطناعي
- مخاطر الذكاء الاصطناعي التوليدي
- أنشطة


Ai

مقدمة

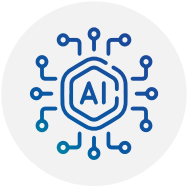
الـذكاء الاصطناعـي (AI) هـو أحـد الـفروع المُتقدّمـة فـي مجـال التكنولوجيـا الحديثـة، والـذي يهـدف إلـى تمكيـن الآلات مـن أداء مهـامّ تتطلَّـب عـادةً الـذكاء البشـري، مثـل التعلُّـم، الاسـتدلال، واتخـاذ الـقرارات.

ظهـرت فكـرة الـذكاء الاصطناعـي للمـرة الأولـى فـي منتصـف الـقرن العشريـن، وتحديـداً فـي عـام 1956، حينمـا اسْـتُخدِم المصطلـح لأول مـرَّة فـي مؤتمـر عِلمـي بالولايـات المتحـدة. منـذ ذلـك الحيـن، شـهد الـذكاء الاصطناعـي تطـورات هائلـة، ليتحـوَّل مـن مجـرد نظريـة إلـى تكنولوجيـا تُستخدَم فـي العديـد مـن المجـالات، مثـل: الرعايـة الصحيـة، والنقـل، والتجـارة، والقطـاع المالـي والمصرفـي، والصناعـة.

ولكـن وعلـى الرغـم مـن فوائـده الكثيـرة؛ إلا أن الـذكاء الاصطناعـي يحمـل معـه مخاطـر جمَّـة، فمَـع تقدُّمـه المتسـارع، ظهـرت تحديـات تتعلّـق بالأمـن، والخصوصيـة، والمخاطـر الاقتصاديـة. علاوةً علـى ذلـك، أصبـح الـذكاء الاصطناعـي أداةً تُسـتغَل فـي عمليـات احتيـال وتزييـف مُتقدّمـة؛ ممـا يزيـد مـن الحاجـة إلـى التحذيـر مـن مخاطـره ووضـع ضوابـط لتقنيـن اسـتخدامه. لا سـيَّما أنـه بـات يُسـتخدَم فـي تطويـر أدوات الهجـوم السيبرانـي، مـن خلال إمكانيـة تحديـد الثـغرات الرقميـة بشـكلٍ أسرع، إضافـةً إلـى اسـتخدامه فـي تطويـر أدوات الهندسـة الاجتماعيـة، مثـل تقنيـات التزييـف العميـق، وغيرهـا مـن التقنيـات المُسـتخدَمة فـي الهجمـات السيبرانيـة.

هـذا الـطرح لا ينبغـي أن يُفْهَـم فـي سـياق أن الـذكاء الاصطناعـي لـه سـلبيات فقـط، علـى العكـس مـن ذلـك، فـإن المؤسسـات المعنيَّة بالأمـن السيبرانـي والسلامـة الرقميـة تعتمـد بشـكلٍ متزايـدٍ علـى الـذكاء الاصطناعـي فـي تطويـر الأدوات والإسـتراتيجيات السيبرانيـة؛ مـن خلال القـدرة علـى معالَجـة كمّيّـات ضخمـة جـداً مـن البيانـات دفعـةً واحـدةً، واسـتخدام نتائج التحليـل فـي تطويـر المنـاورات السيبرانيـة ومحـاكاة الهجمـات، وتحديـد الثـغرات الرقميـة ومعالَجتهـا قبـل اكتشـافها مـن قِبَـل المهاجميـن.

ويمكـن القـول: إنّ الـذكاء الاصطناعـي فـي مجـال الأمـن السيبرانـي سلاح ذو حدَّيـن، فمِـن الممكـن اسـتخدامه لتعزيـز مـؤشرات الأمـن السيبرانـي والسلامـة الرقميـة علـى مسـتوى الـدول والمؤسسـات والمجتمعـات، كمـا يمكـن اسـتخدامه فـي تطويـر أدوات الهجـوم والتهديـد السيبرانـي، فالأمـر مُتوقّـف علـى الهـدف مـن اسـتخدامه، وعلـى الجهـة التـي تسـتخدمه.



الذكاء الاصطناعي وتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية

يُقدّم الذكاء الاصطناعي قيمةً مضافةً مهمّةً لجهود تعزيز الأمن السيبراني والسلامة الرقمية على مستوى المؤسسات والمجتمعات؛ حيث يساعد في الاكتشاف المبكّر للهجمات السيبرانية بشكلٍ أكثر فاعلية مقارنةً بالأدوات التقليدية. كما تتميَّز تقنيات الذكاء الاصطناعي بقدرتها على معالَجة كمّيّات ضخمة من البيانات بسرعة عالية ودقَّة كبيرة، مما يُقلّل من مخاطر الأخطاء البشرية في التحليل، وتُستخدَم هذه التقنيات من خلال أدوات متعددة تشمل نماذج تعلُّم الآلة والتحليلات التنبؤية، **وفيما يلي تبيان لطبيعة استفادة جهود سياسات الأمن السيبراني والسلامة الرقمية من تقنيات الذكاء الاصطناعي:**

استخدام تعلُّم الآلة للكشف عن التهديدات:

تقنيات تعلُّم الآلة تُمكّن من تحليل كمّيّات هائلة من البيانات بسُرعة للكشف عن مؤشّرات الاختراق. وهذا يساعد في تسريع التحقيقات وكشف الأنماط غير الواضحة للتهديدات. على سبيل المثال، تُستخدَم أدوات مثل Cisco Secure Endpoint & Cisco Umbrella لاكتشاف السلوكيات المشبوهة.

إسناد النشاط الإجرامي إلى المهاجمين:

الـذكاء الاصطناعـي يسـاعد فـي تحديـد هويـة المهاجميـن حتـى عندمـا يسـتخدمون تقنيـات مُتقدّمـة لإخفـاء هويَّاتهـم، مثـل الإسـناد المُضلّـل. ومـن خلال تحليـل بيانـات الهجمـات السـابقة وتوقيعـات البرمجيـات الضّـارَّة، يمكـن للنظـام تحديـد الأنمـاط التـي تقـود إلـى تحديـد هويـة المهاجِـم وموقعـه المحتمَـل.

التحليلات التنبؤية:

تُتيـح الخوارزميـات المُعتمِـدة علـى الـذكاء الاصطناعـي تحليـل البيانـات مـن مصـادر متعـددة، مثـل: الويـب المظلـم والمصـادر المفتوحـة؛ للكشـف عـن التهديـدات المحتَمَلـة، والتنبـؤ بهـا قبـل وقوعهـا؛ ممـا يُسـهم فـي الحـدّ مـن آثـار الهجمـات السيبرانيـة المحتَمَلـة.

اختبارات اختراق تطبيقات الويب:

الـذكاء الاصطناعـي يمكنـه محـاكاة الهجمـات المحتَمَلـة علـى الأنظمـة لتحديـد مـدى قـوة الإجراءات الدفاعيـة فـي مُواجَهـة الهجمـات. كمـا يسـاعد ذلـك فـي اكتشـاف الثـغرات فـي النظـام وإصلاحهـا قبـل أن يتمكَّـن المهاجمـون مـن اسـتغلالها.

تحليل حركة مرور البيانات عبر الشبكة:

الـذكاء الاصطناعـي قـادر علـى تحليـل حركـة مرور البيانـات بشـكلٍ دقيـقٍ وسريـعٍ؛ ممـا يُمكِّـن مـن اكتشـاف الهجمـات مُبكراً، وكشـف البرمجيـات الضّـارَّة المُتقدّمـة التـي قـد لا تكتشـفها الأدوات التقليديـة.

تدريب وتأهيل مُتخصّصي الأمن السيبراني والسلامة الرقمية:

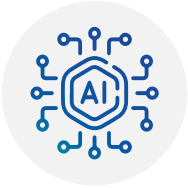
تقنيات الذكاء الاصطناعي تسهم في تدريب العاملين في مجال الأمن السيبراني عن طريق تحديد نقاط الضعف في معارفهم، وتقديم أدوات تدريب مُخصّصة لتغطية هذه الثغرات، بالإضافة إلى محاكاة سيناريوهات اختراق واقعية لتدريبهم على التعامل مع المواقف الحقيقية.

إدارة المناورات السيبرانية:

تُعدّ المناورات السيبرانية وسيلة فعّالة لاكتشاف نقاط الضعف في الأنظمة الدفاعية واختبار مدى جاهزية فِرَق العمل لمواجهة الهجمات. كما يمكن للذكاء الاصطناعي تنظيم هذه المناورات بشكلٍ يحاكي الهجمات الحقيقية؛ مما يجعلها أكثر واقعية وفاعلية.

الكشف عن محاولات التصيد الاحتيالي:

من خلال تقنيات الذكاء الاصطناعي يمكن الكشف عن محاولات التصيد الاحتيالي، مثل الفيديوهات المُصمّمة وفق تقنيات التزييف العميق.



مخاطر الذكاء الاصطناعي

استخدام الذكاء الاصطناعي من قِبَل مجرمي الإنترنت أسهم في زيادة مخاطر الهجمات السيبرانية وزيادة تكاليفها المادية والاجتماعية، وفيما يلي تبيان لأهم هذه المخاطر:

1

فقدان الخصوصية

مع تزايد استخدام الذكاء الاصطناعي في تحليل البيانات الضخمة، تبرز مشكلة الخصوصية كأحد أكبر المخاطر؛ حيث تعتمد أنظمة الذكاء الاصطناعي الحديثة على كميات هائلة من البيانات لتتعلّم وتُطوّر نفسها، ممّا يتطلب جمع بيانات المستخدِمين ومعلوماتهم الشخصية. ويتسبّب هذا في اختراق خصوصية الأفراد واستغلال بياناتهم بطرق غير مُتوقَّعة. فعلى سبيل المثال، قد تتعرض البيانات الشخصية للمُستخدِمين للسرقة أو البيع دون علمهم؛ مما يُؤدّي إلى انتهاك خصوصياتهم.

2

الاحتيال باستخدام الذكاء الاصطناعي

أصبح الذكاء الاصطناعي وسيلةً فعّالةً في عمليات الاحتيال الحديثة؛ حيث يُستخدَم لتوليد رسائل وهمية أو إنشاء حسابات مزيَّفة عبر الإنترنت، مما يسهل على المجرمين تنفيذ مخطّطات احتيالية. على سبيل المثال، استخدام تقنيات "التزييف العميق"[1] (Deepfake) لإنشاء مقاطع فيديو صوتية مزيَّفة، تُظهر أشخاصاً حقيقيّين، وهم يقولون أو يفعلون أموراً لم يقوموا بها فعلياً.

3

أتمتة الجريمة الإلكترونية (Cybercrime Automation)

مع تطوُّر الذكاء الاصطناعي؛ أصبح من الممكن استخدامه في أتمتة الهجمات السيبرانية. كما يمكن لتقنيات التعلم الآلي (Machine Learning) أن تتعلم نقاط ضعف الأنظمة وتهاجمها بشكلٍ أسرع وأكثر كفاءة؛ مما قد يتمكّن الإنسان من القيام به. مثال حي: هو استخدام الذكاء الاصطناعي في تطوير برمجيات الفدية (Ransomware) التي يمكنها تحديد الملفات الأكثر قيمة في النظام وتشفيرها لابتزاز الضحايا. ففي عام 2021، تمّ تسجيل زيادة كبيرة في هجمات الفدية على مستوى العالم؛ مما يوضّح التأثير الكبير للذكاء الاصطناعي على تسهيل تنفيذ الجرائم الإلكترونية.

1 . تكنولوجيا الديب فيك: كيف تعمل وكيفية اكتشافها، مجلة الأمن السيبراني. متاح على الرابط: https://shorturl.at/XFSMk.

4

تمكين الجرائم السيبرانية

تساعد تقنيات الذكاء الاصطناعي في جعل الجرائم السيبرانية أكثر تعقيداً وخطورةً من خلال تقليل الحاجة إلى التدخل البشري في عدة مراحل، مثل تطوير البرمجيات الضّارَّة أو إدارة عمليات الاحتيال. بالإضافة إلى أن الذكاء الاصطناعي يُتيح للمجرمين تحليل كميات كبيرة من البيانات بسُرعة وفاعلية، مما يسمح لهم بتحديد نقاط الضعف والأهداف ذات القيمة العالية. كما يمكن لهذه التقنيات دراسة الإستراتيجيات الدفاعية الحالية لتحديد الثغرات فيها؛ مما يجعل من السهل تجاوزها وتنفيذ هجمات دقيقة.

5

تطوُّر هجمات التصيد الاحتيالي والهندسة الاجتماعية

الهجمات الاحتيالية، خاصةً التصيد الاحتيالي والهندسة الاجتماعية، استفادت بشكلٍ كبيرٍ من الذكاء الاصطناعي؛ حيث يمكن للتقنيات الحديثة إنشاء مواقع ويب مزيَّفة أو صور واقعية لخداع الضحايا، بالإضافة إلى روبوتات التصيد المدعومة بالذكاء الاصطناعي. على سبيل المثال، تمَّ استنساخ صوت الرئيس التنفيذي لشركة بريطانية للطاقة باستخدام الذكاء الاصطناعي؛ مما دفع موظفاً لتحويل 240,000 دولار لحساب المهاجم[1]. هذه التقنيات تُتيح للمهاجمين إقناع الضحايا بسهولةٍ، وقد تزايدت الهجمات التي تعتَمِد على تقنيات انتحال الصوت والصورة بشكلٍ ملحوظٍ.

1 . "الذكاء الاصطناعي والاحتيال الصوتي: كيف قام المحتالون باستنساخ صوت الرئيس التنفيذي لخداع شركة لتحويل 243,000 دولار.". فوربس، متاح على الرابط: https://shorturl.at/a4l2z.

6

استغلال الروبوتات في الهجمات السيبرانية

يمكـن للمهاجميـن اسـتغلال الروبوتـات لأداء مجموعـة مـن المهـامّ الاحتياليـة، مثـل التقـدُّم بطلبـات للحصـول علـى قروض احتياليـة أو التلاعُب بالأسـعار في الأسـواق المالية. إن الروبوتـات المدعومـة بالـذكاء الاصطناعـي تجعـل هـذه العمليـات تكتمـل بشـكلٍ أسرع وأكثـر دقَّـة؛ ممـا يزيـد مـن خطـر الهجمـات الإلكترونيـة والاحتيـال عبـر الإنترنـت.

أمثلة عملية حقيقية على عمليات احتيال وتزييف باستخدام الذكاء الاصطناعي

1 الابتزاز بتقنية التزييف العميق (2020)

في عام 2020، تمّ استخدام تقنية التزييف العميق (Deepfake) لابتزاز سياسي أمريكي؛ حيث أنشأ المجرمون مقاطع فيديو مزيَّفة تُظهره في مواقف مُحرِجة وغير أخلاقية، وهدَّدوا بنشر هذه المقاطع إذا لم يدفع مبلغاً كبيراً من المال. وعلى الرغم من أن الفيديو كان مُزيفاً، إلا أن تأثيره كان قوياً بما يكفي لدفع الضحية للنظر بجديَّة في التهديد. هذه الحادثة تُعدّ مثالاً حياً على كيفية استخدام الذكاء الاصطناعي للابتزاز والإضرار بسُمعة الأفراد.

2 هجمات الذكاء الاصطناعي على البنوك

شهدت البنوك العالمية تصاعداً في الهجمات السيبرانية المُعقّدة التي استُخدمت فيها تقنيات الذكاء الاصطناعي بشكلٍ مُبتكَرٍ وخطيرٍ؛ فلم تَعُد الهجمات تقليدية أو تعتمد فقط على اختراق الشبكات باستخدام الأساليب اليدوية، بل تمّ دمج الذكاء الاصطناعي بشكلٍ يسمح بتحليل الأنظمة المصرفية وتحديد الثغرات الأمنية بدقَّة فائقة. وقد تطوّرت تقنيات الهجوم لدرجة أن الذكاء الاصطناعي أصبح قادراً على استكشاف الأنظمة بشكلٍ ذاتي، معتمِداً على خوارزميات تعلُّم الآلة لتحديد الأنماط غير الطبيعية واستغلال الثغرات في هذه الأنظمة.

الـذكاء الاصطناعـي لـم يُسـتخدَم فقـط لتحليـل الأنظمـة، بـل سـاعد أيضـاً فـي تنفيـذ هجمـات متزامنـة علـى عـدة بنـوك فـي وقـت واحـد؛ ممـا جعَـل مـن الصعـب علـى فِـرَق الأمـن السيبرانـي التعامـل معهـا. هـذا الأسـلوب الـذي يعتمـد علـى الضغـط المتزامـن علـى الأنظمـة أدّى إلـى نجـاح الهجمـات بشـكلٍ كبيـرٍ، حيـث تـمّ اسـتهداف عـدّة بنـوك فـي آسـيا وأوروبـا خلال فتـرة قصيـرة مـن الزمـن، وتنفيـذ الهجمـات بدقـة بحيـث تمـت سـرقة مـا يقـرب مـن 100 مليـون دولار قبـل أن تتمكّـن البنـوك مـن اكتشـاف الاخـتراق ووقـف النشـاط الخبيـث[1].

ومـن أخطـر جوانـب هـذه الهجمـات هـو قـدرة المهاجميـن علـى إخفـاء نشـاطاتهم الخبيثـة باسـتخدام الـذكاء الاصطناعـي. بعـد اخـتراق الأنظمـة، اسـتُخدِمت تقنيـات الـذكاء الاصطناعـي لتعديـل البيانـات الماليـة بطريقـة تجعـل مـن الصعـب اكتشـاف الهجـوم، والتلاعـب بالمعـاملات والتحـويلات البنكيـة لتبـدو شـرعية تمامـاً، مـا سـمح بسـرقة الأمـوال دون أن تُثـار الشـبهات. حتـى بعـد اكتشـاف بعـض الأنشـطة غيـر الطبيعيـة، كانـت الأنظمـة الأمنيـة تجـد صعوبـةً كبيـرةً فـي تتبُّـع مصـدر الهجـوم أو تحديـد النقطـة التـي تـم عندهـا الاخـتراق.

1 . الهجمات السيبرانية على منظمات الصناعة المصرفية في عام 2021. RSI Security، متاح على الرابط: https://rb.gy/rainop.

التصيد الاحتيالي المدعوم بالذكاء الاصطناعي

من خلال الذكاء الاصطناعي، ازدادت حدّة مخاطر التصيد الاحتيالي، وصارت نسبة الوقوع ضحية لهذا النوع من الجرائم الإلكترونية أعلى، وفيما يلي تبيان لكيفية استفادة جرائم التصيد الاحتيالي من تقنيات الذكاء الاصطناعي:

استخدام الهندسة الاجتماعية المُتقدّمة:

يعتمد المهاجمون على تقنيات الهندسة الاجتماعية لتصميم رسائل بريد إلكتروني تصيدية مُخصّصة لكل ضحية بشكلٍ فرديّ. توفّر البيانات الضخمة للمهاجمين إمكانية الوصول إلى معلومات دقيقة عن كل مُستهدَف؛ مما يجعل من الصعب على المستلِمين التعرُّف على النِّيَّات الخبيثة للرسائل.

إنشاء محتوى تصيّدي واقعي أو شِبه واقعي:

باستخدام خوارزميات الذكاء الاصطناعي، يمكن إنشاء محتويات واقعية تُحاكي الرسائل القانونية في أسلوبها وشكلها، سواء أكانت بريداً إلكترونياً أم مواقع ويب. هذا يجعل من الصعب على الأنظمة الأمنية التمييز بين الأنشطة الاحتيالية والمشروعة.

قابلية التوسُّع في الهجوم:

تُتيح الأتمتة التي يُوفّرها الذكاء الاصطناعي للمهاجمين تنفيذ هجمات تصيُّد واسعة النطاق، تشمل تصميم الرسائل وتوزيعها على آلاف الأشخاص والتفاعُل مع ردودهم؛ مما يزيد من احتمالية خداع عدد أكبر من الضحايا.

التخفّي عن برامج الأمان:

خوارزميات الذكاء الاصطناعي تتعلّم من ردود فعل الأنظمة الأمنية؛ مما يجعلها قادرةً على التحايُل على برامج الكشف عن التصيد والبرمجيات الضّارَّة. كما يتم تعديل أساليب الهجوم باستمرار لتجنُّب اكتشافها من قِبَل المُرشّحات الأمنية التقليدية.

الاستهداف الدقيق:

بفضل قدرات الذكاء الاصطناعي على جمع وتحليل البيانات، يمكن للمهاجمين تصميم هجمات تصيُّد مُخصّصة لأفراد أو مجموعات معيّنة بناءً على اهتماماتهم ونقاط ضعفهم؛ مما يزيد من فاعلية الهجوم وفرص نجاحه.

التعرُّف الآلي على نقاط الضعف:

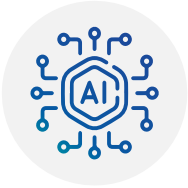
بدلاً من البحث اليدوي عن نقاط الضعف في الأنظمة، يمكن للذكاء الاصطناعي أتمتة عملية فحص الشبكات لتحديد الثغرات ونقاط الدخول المحتَمَلة التي يمكن استغلالها في هجمات التصيد الاحتيالي.

تخمين كلمات المرور بسهولة:

باستخدام خوارزميات تعلُّم الآلة، يمكن تطوير نماذج لتخمين كلمات المرور بشكلٍ أكثر دقَّة. تعمل هذه النماذج على تحليل الأنماط وزيادة احتمالية النجاح في الوصول إلى حسابات الضحايا.

استخدام تقنية التزوير العميق (Deepfake):

من خلال مقاطع الفيديو والتسجيلات الصوتية المزيَّفة التي يتم إنشاؤها بواسطة الذكاء الاصطناعي، يمكن للمهاجمين انتحال شخصيات مهمّة؛ مما يُسهّل سرقة الهوية أو التلاعُب بالرأي العام.



مخاطر الذكاء الاصطناعي التوليدي

الذكاء الاصطناعي التوليدي (Generative AI) هو نوع من الذكاء الاصطناعي القادر على إنشاء محتوى جديد أو توليد مخرجات مُبتكَرة بناءً على الأنماط التي تمّ تعلُّمها من البيانات السابقة. يستخدم نماذج تعلُّم الآلة مثل الشبكات العصبية العميقة (Deep Learning) لتوليد نصوص، صُوَر، موسيقى، برمجة أكواد، وحتى تصميمات معقّدة.

وبشكلٍ عامّ يتّسم الذكاء الاصطناعي التوليدي بجملةٍ من الخصائص والسّمات، فيما يلي تبيان لأهمّها:

1 **توليد المحتوى:**

يمكنه إنشاء محتوى أصلي مثل المقالات، أو الصُّوَر، أو الموسيقى، أو الفيديوهات. مثل «ChatGPT» الذي ينتج نصوصاً استجابةً للمدخلات النصية.

2 **تعلُّم الأنماط:**

الذكاء الاصطناعي التوليدي يعمل من خلال التعلم من كميات كبيرة من البيانات واكتشاف الأنماط الأساسية، ثم استخدام تلك الأنماط لإنشاء مخرجات جديدة ومُبتكَرة.

3 التطبيقات العملية:

يُستخدَم في العديد من المجالات مثل الفن الرقمي، والكتابة الإبداعية، وإنشاء تصميمات المنتجات، وتوليد التعليمات البرمجية، وكذلك في تطوير المحادثات التلقائية مع الروبوتات.

> الذكاء الاصطناعي التوليدي (Generative AI) يُعدّ أداة فعَّالة ومبتكرة، لكنه في الوقت نفسه يُسهم في تفاقم التهديدات السيبرانية بعدَّة طرق؛ حيث يتم استغلاله مِن قِبَل المهاجمين لتحسين أساليبهم وزيادة فاعلية الهجمات.

وفيما يلي بعض الآثار الرئيسية للذكاء الاصطناعي التوليدي على التهديدات السيبرانية:

1 زيادة دقَّة هجمات التصيد الاحتيالي (Phishing)

الذكاء الاصطناعي التوليدي يمكن أن يُستخدم لتوليد رسائل بريد إلكتروني احتيالية عالية الجودة، تحتوي على لغة دقيقة وواقعية، وتتناسب مع كل ضحية على حدة. وهذا يجعل من الصعب على المستخدِمين التمييز بين الرسائل الحقيقية والمزيَّفة. كما أن الذكاء الاصطناعي يمكنه أيضاً توليد مواقع إلكترونية مزيَّفة بشكلٍ أكثر إقناعاً لتسهيل عمليات التصيد الاحتيالي.

2 تطوير تقنيات التصيد الصوتي والمرئي (Deepfake)

تقنية التزييف العميق (Deepfake)، التي تعتمد على الذكاء الاصطناعي التوليدي، تُستخدم لإنشاء مقاطع فيديو وصوت مزيَّفة بشكل واقعي. وهذا يسمح للمهاجمين بانتحال شخصيات مؤثرة أو معروفة لخداع الضحايا وتحفيزهم على اتخاذ إجراءات معينة، مثل تحويل الأموال أو الكشف عن معلومات حسّاسة.

3 توليد البرمجيات الضّارّة (Malware)

الذكاء الاصطناعي التوليدي يمكنه تصميم برمجيات ضارّة جديدة قادرة على التخفّي عن برامج مكافحة الفيروسات التقليدية. باستخدام التعلُّم العميق، ويمكن للذكاء الاصطناعي تطوير أشكال جديدة من الفيروسات أو الهجمات التي تكون أكثر تطوراً وأكثر قدرةً على تجاوز أنظمة الحماية.

4 اختبار هجمات متقدّمة

يمكن للذكاء الاصطناعي التوليدي محاكاة الهجمات الإلكترونية واختبار إستراتيجيات جديدة لتحسين فاعليتها. ويمكنه أيضاً تطوير نماذج متطورة تُمكِّن المهاجمين من تحليل ردود الفعل الأمنية وتعديل أساليب الهجوم بشكلٍ مستمرّ لتفادي الكشف.

5 تخمين كلمات المرور

باستخدام الذكاء الاصطناعي التوليدي وتقنيات التعلُّم الآلي، يمكن تحسين تقنيات تخمين كلمات المرور، مما يجعل الهجمات على الحسابات أكثر دقَّة وفاعلية. ويمكن لهذه النماذج تحليل أنماط كلمات المرور الشائعة وتوقُّع كلمات المرور الجديدة بناءً على البيانات المتاحة.

6 استهداف الضحايا بشكلٍ أَدَقّ

الذكاء الاصطناعي التوليدي يمكنه تحليل البيانات الضخمة لتحديد الأشخاص والمؤسسات الأكثر عُرْضَةً للهجمات السيبرانية. هذا الاستهداف الدقيق يزيد من فُرَص نجاح الهجمات ويُقلّل من احتمالات اكتشافها.

ختاماً لهذا الفصل، يشهد الذكاء الاصطناعي تطورات متسارعة، وتشير الدلائل الحالية إلى أنه وفي المستقبل القريب سيزداد الاعتماد على الذكاء الاصطناعي والذكاء الاصطناعي التوليدي في غالبية المجالات، وهذا ما سيترافق مع استفادة الجرائم السيبرانية من هذا التطوُّر، مع يعني أن الذكاء الاصطناعي يمكن أن يكون إيجابياً أو سلبياً، فالأمر متوقّف على كيفية استخدامه. ولتعزيز الحماية من مخاطره، فيما يتعلق بالجرائم الإلكترونية وجرائم التصيد الاحتيالي، لا بدّ من تعزيز الوعي بهذه المخاطر، على المستويين المؤسسي والفردي.

أنشطة

النشاط الأول

ابحث في الإنترنت عن حالات للتصيد الاحتيالي أو الجرائم الإلكترونية التي تم تنفيذها بالاعتماد على تقنيات الذكاء الاصطناعي، واستنتج الأخطاء التي ارتكبها المستخدمون، وأدَّت إلى وقوعهم ضحايا لهذه الجرائم.

النشاط الثاني

في جدول من تصميمك؛ قارِن بين منافع ومخاطر الذكاء الاصطناعي.

النشاط الثالث

استفاد كلٌّ من الأمن السيبراني والسلامة الرقمية من جهة، والتهديدات السيبرانية من جهةٍ أخرى من تقنيات الذكاء الاصطناعي، ما يبدو أنه سباق في استثمار هذه التقنيات بين المؤسسات المعنيَّة بالأمن السيبراني والسلامة الرقمية والجهات السيبرانية الخبيثة... ابحث في كيفية استفادة كلٍّ من هذه الجهات من الذكاء الاصطناعي.

المراجع

1. يوسف، أمير. (2015م). جرائم تقنية المعلومات بدول الخليج العربي، والجهود الدولية والمحلية لمكافحتها: جرائم الإنترنت والحاسوب الإلكترونية في دول الخليج العربي. مصر: دار الكتب العربية. ص -68 74.
2. كمال، محمد. الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلاً من القنبلة، دار كليم للطباعة والنشر والتوزيع (القاهرة - مصر)، ط1، 2022م، ص11.
3. تفاصيل قانون الجرائم الإلكترونية في قطر، 2024، على الموقع: https://2u.pw/wga1FQvG.
4. تكنولوجيا الديب فيك: كيف تعمل وكيفية اكتشافها، مجلة الأمن السيبراني. متاح على الرابط: https://shorturl.at/XFSMk.
5. الذكاء الاصطناعي والاحتيال الصوتي: كيف قام المحتالون باستنساخ صوت الرئيس التنفيذي لخداع شركة لتحويل 243,000 دولار، فوربس، متاح على الرابط: https://shorturl.at/a4l2z.
6. الهجمات السيبرانية على منظمات الصناعة المصرفية في عام 2021. RSI Security، متاح على الرابط: https://rb.gy/rainop.
7. تفاصيل قانون الجرائم الإلكترونية في قطر، محامي قطر، متاح على الرابط: https://2u.pw/wga1FQvG.
8. What Is Ransomware? Proofpoint, on site: https://www.proofpoint.com/us/threat-reference/ransomware.
9. What is Cyber Security? Kaspersky, on site: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

10. What Is Phishing? IBM, 17 May 2024. On site: https://www.ibm.com/topics/phishing.
11. What is spear phishing? Definition and risks. Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/spear-phishing.
12. Vishing: The Growing Threat and How to Protect Yourself. TOPSEC. On site: https://www.topsec.com/vishing-voice-phishing-the-growing-threat-and-how-to-protect-yourself/.
13. 10 Most Common Signs of a Phishing Email. On site: https://www.titanhq.com/blog/10-tell-tale-signs-that-spam-email-is-a-phishing-scam/.
14. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://www.keyfactor.com/blog/https-phishing-attacks-how-hackers-use-ssl-certificates-to-feign-trust/.
15. What is an Evil Twin Attack? Evil Twin Wi-Fi Explained, Kaspersky. On site: https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks.
16. Whaling: how it works, and what your organization can do about it. On site: https://serviceteamit.co.uk/news/whaling-how-it-works-and-what-your-organisation-can-do-about-it/.
17. Clone Phishing: Here›s What You Need to Know to Protect Your Organization. On site: https://hoxhunt.com/blog/clone-phishing#:~:text=Clone%20phishing%20is%20when%20hackers,strategies%20to%20safeguard%20your%20organizatio.
18. Advanced persistent threat (APT), Imperva , on site: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

19. Ramonas, Lukas. What is a dumpster diving attack, Nordvpn, may 2023, on site: https://nordvpn.com/blog/dumpster-diving-attack/
20. Cieply, Michael and Brooks Barnes, Sony Cyberattack, first a Nuisance, Swiftly Grew Into a Firestorm, The New York Times, December 2014, on site: https://www.nytimes.com/201431/12//business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.
21. What-is-gdpr? Gdpr, on site: https://gdpr.eu/what-is-gdpr/.
22. .Microsoft, on site: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam.
23. What is a VPN? Microsoft, on site: https://linksshortcut.com/oFBiU.
24. What is mobile device management (MDM)? IBM, on site: https://www.ibm.com/topics/mobile-device-management.
25. What are the GDPR Fines? on site: https://gdpr.eu/fines/.
26. How the GDPR could change in 2020? on site: https://gdpr.eu/gdpr-in-2020/.
27. Italy fines Eni Gas e Luce €11.5 million for multiple GDPR violations, on site: https://gdpr.eu/italy-fines-energy-company-for-multiple-gdpr-violations/.

هذا الدليل

في ظل التطوُّر المتسارع للفضاء السيبراني، وما يُرافقه من تصاعُد في حدَّة التهديدات والمخاطر السيبرانية؛ لم تعد السلامة الرقمية ترفاً فكرياً أو قضيةً ثانويةً، بل أصبحت أولوية قصوى بالنسبة للدول والمؤسسات والمجتمعات والأفراد، وبات يُنظَر إليها على أنها قضية رئيسة. وانسجاماً مع هذا الطرح، كانت فكرة دليل السلامة الرقمية، والذي يُعدّ من الأدوات التوعوية المعتمَدة في سياق المبادرة الوطنية للسلامة الرقمية.

يُعدّ هذا الدليل بمثابة مُوجِّه عامّ وداعم معرفيّ رئيس لمختلف شرائح المجتمع؛ فهو يتضمَّن معارف حديثة تخصّ الأمن السيبراني والسلامة الرقمية، ويُقدّم معلومات تفصيلية حول أبرز المفاهيم السيبرانية، ويُحدّد المخاطر السيبرانية الحديثة، ويُوجِّه المجتمع لكيفية التعامل معها، بما ينعكس إيجاباً على أمن المجتمع وتحصينه سيبرانياً.

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency