الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

إرشادات الأمن السيبراني
لموفري خدمة التجارة الإلكترونية

Cybersecurity Guidelines for E-commerce Service Providers

(CGESP – 1: 2019)

إشـــارة الـمـشـاركـة: أبـيـض
تـصـنـيـف الـوثـيـقـة: مـتـــاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP)

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد (سواء من داخل المنشأة أو خارجها) خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في المنشأة نفسها مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

الملخص التنفيذي

تعتبر التجارة الإلكترونية أحد أهداف برنامج التحول الوطني الداعمة لتحقيق رؤية المملكة ٢٠٣٠، حيث يُقدّر إنفاق المملكة على التجارة الإلكترونية بنحو ٢٦,٨ مليار ريال سعودي في عام ٢٠١٩ [١]، مما يجعلها أحد أكبر أسواق التجارة الإلكترونية في منطقة الشرق الأوسط وشمال أفريقيا، ولمواكبة النمو المتسارع للتجارة الإلكترونية والمخاطر المصاحبة لها، فقد صدرت موافقة مجلس الوزراء على نظام التجارة الالكترونية الذي يهدف إلى تعزيز موثوقية التجارة الإلكترونية ولزيادة مساهمتها في الاقتصاد الوطني، وتحفيز وتطوير أنشطة التجارة الالكترونية في المملكة.

لـذا طـوّرت الهيئة الوطنية للأمن السيبراني إرشـادات الأمـن السيبراني لموفري خدمة التجارة الإلكترونية (CGESP – 1: 2019) بهدف تثقيف ومساعدة موفري خدمة التجارة الإلكترونية من فئات المنشآت الصغيرة والمتوسطة والمكاتب الصغيرة والمنزلية في المملكة لتطبيق أفضل الممارسات لحماية تجارتهم وأجهزتهم وبياناتهم وحسابات عملائهم وعمليات الدفع مع الأخذ بعين الاعتبار تحقيق تجربة تسوق إلكترونية سلسة للمستهلكين.

الإرشادات الرئيسية هي:

١. استخدم وسائل مصادقة قوية.
٢. اعمل على حماية أنظمتك الخاصة بالتجارة الإلكترونية.
٣. قلل من تأثير انتهاكات البيانات.
٤. اعمل على حماية حساباتك على مواقع التواصل الاجتماعي الخاصة بتجارتك الإلكترونية.
٥. اعمل على حماية شبكتك الإلكترونية.
٦. ثقّف موظفيك ودرّبهم باستمرار.
٧. اعمل على حماية البنية التحتية الداخلية لتجارتك الإلكترونية.

[١] تقرير التجارة الإلكترونية من منظمة ستاتيستا للإحصائيات ٢٠١٩

المقدمة

طوّرت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ «الهيئة») إرشادات الأمن السيبراني لموفري خدمة التجارة الإلكترونية (CGESP – 1: 2019) بعد إجراء دارسة شاملة لعدة إرشادات وطنية ودولية تتعلق بالأمن السيبراني للتجارة الإلكترونية ودراسة المبادرات الوطنية والإحصاءات والمتطلبات التنظيمية ذات العلاقة بهدف المراجعة والاستفادة من أفضل ممارسات الأمن السيبراني وتحليل الحوادث والهجمات السيبرانية السابقة التي تعرض لها موفّرو خدمة التجارة الإلكترونية.

تستخدم ٢٦٪ من المنشآت الصغيرة والمتوسطة في المملكة منصات التواصل الاجتماعي[٢] للترويج لمنتجاتها، ويفيد نحو ٨٦٪ من المنشآت التي تبيع إلكترونيًا أنها كانت نشيطة بوصفها موفّر خدمة إلكتروني خلال السنوات الثلاث أو الخمس الماضية. ويركز أغلب موفري الخدمة هؤلاء على سوق المملكة في حين يستهدف عدد قليل منهم أسواق الخليج والشرق الأوسط. من جهة أخرى، فإن أغلبية تجار المكاتب الصغيرة والمنزلية (والمشار إليها أحيانًا بـ C2C أو التجارة بين المستهلكين أو المنشآت الصغرى أو الملكيات الفردية) يزيدون مبيعاتهم عن طريق الاستفادة من منصات التواصل الاجتماعي للوصول إلى الزبائن ورفع الحركة التجارية.

لقد أدّى الإقبال المتزايد على التجارة الإلكترونية إلى نشوء جيل جديد من التهديدات السيبرانية المصاحبة والتي تكون أحيانًا مجرد حوادث عرضية وأحيانًا أخرى تكون متعمدة من المخترقين أو المجرمين (والذين سيتم الإشارة إليهم بـ «المهاجمين» في هذه الوثيقة). تشمل الأخطار السيبرانية الشائعة في التجارة الإلكترونية الانتهاكات الأمنية لأنظمة التجارة الإلكترونية وبياناتها وهجمات تعطيل الخدمات والنقر الاحتيالي. هذه التهديدات قد تؤدي إلى نقص في العوائد وخسائر في المخزون وعدم توفر أنظمة المعلومات أو الموقع الإلكتروني ويؤدي ذلك إلى التأثير السلبي على السمعة بالإضافة إلى عواقب أخرى قانونية.

صُمِمت هذه الإرشادات لمساعدة موفّري خدمة التجارة الإلكترونية من أصحاب الشركات الصغيرة والمتوسطة والمكاتب الصغيرة والمنزلية في المملكة لفهم مخاطر الأمن السيبراني التي يواجهونها في التجارة الإلكترونية بصورة أفضل وتقديم نصائح عملية لحماية أعمالهم وأنظمتهم وبياناتهم من التهديدات السيبرانية.

[٢] التجارة الإلكترونية في المملكة العربية السعودية، هيئة الاتصالات وتقنية المعلومات، ٢٠١٧

نطاق التطبيق

تنطبق هذه الإرشادات على موفري خدمة التجارة الإلكترونية في المملكة العربية السعودية الذين يندرجون تحت القسمين[٣] الآتيين:

- المنشآت الصغيرة والمتوسطة.
- المكاتب الصغيرة والمنزلية.

تغطي هذه الإرشادات استخدام التجارة الإلكترونية عبر أي قناة كانت (مثل مواقع التواصل الاجتماعي والمواقع الإلكترونية والتطبيقات) باستخدام أي جهاز إلكتروني (مثل أجهزة الحاسب الآلي والهواتف والتلفزيونات الذكية والأجهزة اللوحية).

إن هذه الإرشادات توعوية، وتحث الهيئة كل موفّر خدمة تجارة إلكترونية في المملكة على اتباعها لتطبيق أفضل الممارسات التي تقلل من مخاطر الأمن السيبراني على أعمالهم وأنظمتهم وبياناتهم. ولأن طبيعة الأخطار السيبرانية دائمة التغير، فإن الهيئة تحث موفّري الخدمة على القيام ببحوثهم الخاصة من أجل معرفة أي إجراءات سيبرانية إضافية لازمة.

[٣] الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت)

العلاقة مع إصدارات الأمن السيبراني الوطنية الأخرى

بالإضافة لإرشادات الأمن السيبراني لموفري خدمة التجارة الإلكترونية، فقد طورت الهيئة أيضًا إرشادات الأمن السيبراني لمستهلكي التجارة الإلكترونية (CGEC – 1: 2019)، والهدف منها توعية مستهلكي التجارة الإلكترونية في المملكة. يجب على المنشآت الكبيرة (وهي فئة أخرى من موفّري خدمة التجارة الإلكترونية) الرجوع إلى الضوابط الأساسية للأمن السيبراني (ECC - 1 : 2018) للحصول على الإرشادات والالتزام الإجباري في بعض الحالات.

تدعم إرشادات الأمن السيبراني لموفري خدمة التجارة الإلكترونية الأنظمة، اللوائح، الأطر والمعايير الوطنية التي يتم الإشراف عليها من الجهات الآتية:

- وزارة التجارة والاستثمار (مثل نظام التجارة الإلكترونية)
- الهيئة الوطنية للأمن السيبراني (مثل نظام حماية البيانات – تحت التطوير)
- مؤسسة النقد العربي السعودي «ساما» (مثل الدليل التنظيمي لأمن المعلومات، مبادئ حماية عملاء المصارف، وغيرها من التعليمات ذات العلاقة التي تصدرها المؤسسة)

إرشادات الأمن السيبراني لموفري خدمة التجارة الإلكترونية

تتمحور الإرشادات الموضّحة في هذه الوثيقة حول سبع إرشادات رئيسية، ينطبق بعضها على موفري خدمة التجارة الإلكترونية من المنشآت الصغيرة والمتوسطة أو المكاتب الصغيرة والمنزلية، أو كليهما حسب هذا التوضيح:


تنطبق على موفري الخدمة من فئة المنشآت الصغيرة والمتوسطة


تنطبق على كلٍ من موفري الخدمة من فئات المكاتب الصغيرة والمنزلية و المنشآت الصغيرة والمتوسطة

	١. استخدم وسائل مصادقة قوية	نطاق التطبيق
١-١	**تجنب استخدام كلمات المرور القديمة أو كلمات المرور التي يمكن التنبؤ بها**	
	استخدم كلمات مرور قوية لحماية حساباتك التي تستخدمها للبيع في التجارة الإلكترونية، بحيث تكون: • مكوّنة من تسلسل عشوائي من الأحرف (الكبيرة والصغيرة) والأرقام والرموز (!@#$%^&*). • كلمات غير شائعة مع تجنب التسلسل البسيط للأرقام (مثل 123456) أو أي معلومات شخصية كتاريخ ميلادك أو اسم طفلك فهذه الكلمات يسهل توقعها. • طويلة (لا يقلّ طولها عن ثمانية أحرف) مما يصّعب على المهاجمين اختراقها. تأكد من تغيير كلمة المرور كل ثلاثة أشهر على الأقل ولا تشاركها مع الآخرين.	
١-٢	**غيّر جميع كلمات المرور الافتراضية**	
	• يجب تغيير كلمات المرور الافتراضية لمسؤول النظام (admin) على الفور عند التثبيت وقبل الاستخدام؛ حيث أن الكلمات الافتراضية معروفة للمهاجمين، ويمكن استخدامها لاختراق أنظمتك التجارية الإلكترونية والوصول إليها. • احرص على استخدام كلمات مرور مختلفة لكل واحد من أنظمتك وحساباتك والتطبيقات ذات العلاقة بالتجارة الإلكترونية.	
١-٣	**خذ بعين الاعتبار استخدام خيارات تحقق إضافية**	
	فعّل خاصية التحقق المتعدد العناصر للهوية عند توفر ذلك في الأنظمة أو التطبيقات ذات العلاقة بتسجيل دخول عملائك وذلك لحماية المستهلكين الذين تتعامل معهم في التجارة الإلكترونية. على سبيل المثال، عندما يقوم المستهلك بتسجيل الدخول باستخدام كلمة المرور، قد يتم إرسال رمز إليه (عبر رسالة نصية على رقم الهاتف الذي تم استخدامه في عملية التسجيل) ويجب عليه بعدها إدخال هذا الرمز لإكمال عملية تسجيل الدخول. ولحماية حساباتك التي تستخدمها للبيع في التجارة الإلكترونية، اشترك في خيارات التحقق الإضافية (مثل رسائل البريد الإلكتروني) التي تقدمها تطبيقات التجارة الإلكترونية ومواقعها (ويشمل هذا حسابات مواقع التواصل الاجتماعي).	

	٢. اعمل على حماية أنظمتك الخاصة بالتجارة الإلكترونية	نطاق التطبيق
٢-١	**اعرف الأصول التقنية لتجارتك الإلكترونية**	
	ضَع قائمة مُحدّثة لكل أدوات تقنية المعلومات والبرمجيات والبيانات وأي أصول تقنية تستخدمها لتجارتك الإلكترونية حيث أن أول خطوة لحماية أنظمتك هي معرفة الأجهزة والبيانات الحرجة والمهمة لتجارتك، وعادةً ما تكون هي الأصول التي لا يمكن لتجارتك العمل بدونها.	

٢-٢	**تحكّم بعدد حسابات مسؤولي الأنظمة**	
	امنح موظفي تجارتك الإلكترونية أقل مستوى من صلاحيات المستخدم المطلوبة للقيام بمهامهم الوظيفية وامنح صلاحيات مسؤول النظام بحذر شديد، حيث يتمتع حساب مسؤول النظام بصلاحيات خاصة للقيام بتغييرات في النظام لا يمكن لحسابات المستخدمين الآخرين القيام بها. كما يجب أن يكون كل دخول على الحساب المسؤول تحت رقابة صارمة من خلال كلمة مرور شديدة القوة/التحقق من الهوية متعدد العناصر وتقليص مهلة الانتظار، ويجب عليك أيضًا مراجعة دخول المستخدمين دوريًا، وتقليل عدد الأشخاص المخولين للوصول للأنظمة عن بعد والسماح لهم بالوصول لأنظمة محدودة وغير حساسة.	
٣-٢	**استخدم برامج الحماية من البرمجيات الضارة**	
	استخدم برامج الحماية وحدثها باستمرار على كل جهاز مستخدم في بيئة الأعمال الخاصة بتجارتك الإلكترونية (بما في ذلك أجهزة الحاسب الآلي والهواتف الذكية والأجهزة اللوحية) لحماية أنظمة تجارتك الإلكترونية من البرمجيات الضارة (كالفيروسات على سبيل المثال). اضبط برنامج الحماية ليقوم بالتحقق اليومي من وجود التحديثات، والقيام بعمل مسح كامل بشكل منتظم.	
٤-٢	**حدّث تطبيقاتك بانتظام على جميع الأجهزة**	
	حدث تطبيقاتك دورياً حيث أن إحدى أكثر الطرق كفاءة في الحماية ضد البرمجيات الضارة والفيروسات هي إبقاء جميع أجهزة وتطبيقات تجارتك الإلكترونية (خاصةً أنظمة التشغيل) مُحدّثَة بآخر التصحيحات الأمنية وتحسينات المُوّردِين.	
٥-٢	**اطلع على التهديدات السيبرانية أولاً بأول**	
	اشترك بتنبيهات الموردين والإنذارات السيبرانية لتبقى على اطلاع بمستجدات الأمن السيبراني والتهديدات النشطة. يمكنك أيضًا متابعة آخر التحديثات من منظمات موثوقة (مثل المركز الوطني الإرشادي السعودي للأمن السيبراني Saudi CERT) لمعرفة المزيد عن إصدارات الأمن السيبراني ومستجداته.	
٦-٢	**تجنب الارتباط بشبكات لاسلكية غير محمية**	
	تجنب استخدام الشبكات اللاسلكية غير المحمية (مثل الشبكات اللاسلكية العامة) لأي معاملة تجارية إلكترونية حيث أن تلك الشبكات تعتبر مكاناً مثالياً للمهاجمين لاعتراض نقل البيانات والحصول على بياناتك مثل معلومات تسجيل الدخول والمعلومات المالية.	
٧-٢	**استخدم بروتوكولات تشفير موثوقة لحماية موقعك**	
	خذ في الحسبان استخدام بروتوكلات التشفير الآمنة لموقعك الإلكتروني، حيث أن بروتوكولات التشفير تضمن أمان العمليات التجارية في موقعك التجاري، ويتم ذلك عن طريق تشفير أي بيانات يتم إدخالها في موقعك الإلكتروني.	
٨-٢	**استعن بمواقع موثوقة لعرض إعلاناتك**	
	اعمل على حماية إعلاناتك من النقرات الاحتيالية وذلك عن طريق عرض إعلاناتك على مواقع موثوقة والتي تعرف أنها مصدر لعملاء حقيقيين.	

	٣. قلل من تأثير انتهاكات البيانات	نطاق التطبيق
٣-١	**قم بالنسخ الاحتياطي لبياناتك**	
	خذ بعين الاعتبار النسخ الاحتياطي لبياناتك المهمة، والتي قد تحتوي على بيانات تجارتك وحساباتك في مواقع التواصل الاجتماعي ومعلومات العملاء. يمكنك استخدام خدمات النسخ الاحتياطي عبر الإنترنت (مثل النسخ الاحتياطي السحابي) أو وسائل التخزين الخارجية (مثل الأقراص الصلبة الخارجية). إذا قررت استخدام الخدمات السحابية للنسخ الاحتياطي، امتنع عن تخزين بيانات المواطنين في السحابة عندما تكون الخدمة مستضافة خارج المملكة وذلك امتثالاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. قم بالنسخ الاحتياطي بشكل دوري على الأقل مرة أسبوعيًا، وتأكد من كفاءة أدوات التخزين عن طريق التأكد فعلياً من وجود البيانات على تلك النسخ الاحتياطية لتفادي حالات العطب أو ضياع البيانات.	
٣-٢	**اعمل على حماية بياناتك بالتشفير**	
	شفّر كل البيانات الحرجة المخزنة على جهازك أو السحابة أو القرص الخارجي وكذلك البيانات التي يتم إرسالها عبر البريد الإلكتروني حيث أن التشفير هو عملية تتمثل في جعل بياناتك غير قابلة للقراءة لأي أحد لا يمتلك كلمة المرور أو المفتاح الصحيح. شفّر الملفات الحساسة المخزنة على وسائل التخزين المتنقلة (مثل محرك أقراص فلاش USB) حتى تمنع الآخرين من الوصول للبيانات في حال فقدان وسائل التخزين المتنقلة.	
٣-٣	**اعمل على حماية المعلومات المالية للعملاء**	
	اتبع مبدأ تقليل البيانات وهو ما يعني تقليل كمية البيانات الشخصية وأنواعها المختلفة التي يتم جمعها وتخزينها. وعندما تقرر تخزين بيانات الدفع الخاصة بالعملاء على منصة تجارتك الإلكترونية (مثل تفاصيل البطاقات الائتمانية) تأكد من تطبيقك لضوابط أمن سيبراني صارمة (مثل الوصول المحدود والتشفير) لهذه البيانات من أجل حماية تجارتك ضد انتهاكات سرية بيانات الدفع. كما يجب عليك التأكد من امتثالك لأي متطلبات محلية أو دولية ذات علاقة بحماية البيانات. على سبيل المثال، إذا كان لديك عملاء خارج المملكة، تأكد من التعرف على أي متطلبات ذات علاقة يجب على تجارتك الالتزام بها (مثل تنظيم حماية البيانات العامة لعملاء الاتحاد الأوروبي GDPR). تأكد من إبلاغ مؤسسة النقد العربي السعودي والعملاء فور حدوث أي تسريب لبيانات الدفع.	
٣-٤	**غيّر إعداداتك الأمنية الافتراضية**	
	راجع التفضيلات الافتراضية وتغييرها في متصفحك لتجنب حفظ بيانات تسجيل الدخول لمواقع التواصل الاجتماعي ومعلومات العملاء والتعبئة التلقائية للبيانات. إن كنت تقوم بمعاملات تجارتك المصرفية إلكترونيًا، خذ في الحسبان استخدام جهاز مخصص فقط لهذا الغرض وتأكد من قطع اتصاله بالشبكة عند عدم استخدامه.	

٣-٥	**فعّل الحذف الآمن عن بعد على أجهزتك المحمولة**	
	فعّل خاصية الحذف الآمن عن بعد حيث أن بعض الأجهزة المحمولة تأتي عادةً بميزة الحذف الآمن لجميع محتوياتها عن بعد عند فقدان المستخدم لها. اطلب من موظفيك التبليغ السريع عن فقدان أي جهاز عمل محمول في أسرع وقت ممكن حتى يمكن استعادة الجهاز أو قفله أو حذف محتوياته عن بعد. سوف يمنع هذا الإجراء المهاجمين من الوصول إلى أنظمة تجارتك الإلكترونية وحساباتها.	

	٤. اعمل على حماية حساباتك على مواقع التواصل الاجتماعي الخاصة بتجارتك الإلكترونية	نطاق التطبيق
١-٤	**مارس السلوكيات الآمنة على مواقع التواصل الاجتماعي**	
	خذ المزيد من الحيطة عند استخدام تطبيقات ومواقع التواصل الاجتماعي. كن حذرًا عند التواصل عبر هذه المواقع والتطبيقات خاصةً عند تلقيك لرسائل تطلب منك معلومات تجارية حساسة، فقد أصبحت مواقع التواصل الاجتماعي طريقة شائعة يستخدمها المهاجمون للحصول على معلوماتك التجارية. حدد شخصاً أساسياً ليكون مسؤولاً عن حسابات التواصل الاجتماعي لتجارتك الإلكترونية.	
٢-٤	**وثّق حساباتك على مواقع التواصل الاجتماعي**	
	وثّق حساباتك حيث أن أغلب منصات التواصل الاجتماعي توفر مؤشرًا مرئيًا (مثل أيقونة بجانب اسم المستخدم) لتوّضح بأن هذا الحساب موثق. إحدى الطرق الجيدة للتوثيق هي منصات تقييم السمعة والموثوقية عبر الإنترنت (مثل منصة معروف). يعد توثيق حسابك خطوة إيجابية لزيادة ثقة عملائك بهذا الحساب. كما أن عليك الحذر من طلبات التواصل من تجار آخرين لا تعرفهم، لهذا قم ببحث سريع للتأكد من مشروعيتهم وتجنب ربط حساباتك على مواقع التواصل الاجتماعي مع خدمات أو تطبيقات غير معروفة، وعليك القيام بإلغاء أي تصريح دخول غير ضروري.	

	٥. اعمل على حماية شبكتك الإلكترونية	نطاق التطبيق
١-٥	**عطّل الخدمات غير اللازمة على الأنظمة**	
	عطّل الخدمات والمميزات الإضافية والتي لا يتم استخدامها في الغالب حيث تحتوي الكثير من الأجهزة مثل الحواسيب والموجهات اللاسلكية على مثل تلك الخدمات والمميزات ، مثلما يحتوي عدد من أنظمة التشغيل على برمجيات غير لازمة مثبتة مسبقًا.	
٢-٥	**اعزل وقسم الشبكات**	
	قسّم شبكتك إلى شبكات فرعية لحماية المعلومات الحساسة من التدفق إلى الأجزاء غير الآمنة من شبكة تجارتك الإلكترونية.	

٥-٣	**اعمل على حماية محيط الشبكة**	
	استخدم أنظمة منع التسلل (IPS) لحماية محيط شبكتك، فهذه الأنظمة لديها القدرة على رصد أنماط حركة مرور البيانات الغريبة والشاذة في نشاطات الشبكة، مما قد يشير إلى احتمالية وجود محاولات هجوم على أنظمتك. يُنصح أيضًا باستخدام جدار حماية في شبكتك والتأكد من مراجعة قائمة الوصول دوريًا.	
٥-٤	**افحص أنظمتك باستمرار**	
	اختبر أنظمة تجارتك الإلكترونية ضد الاختراق دوريًا وعند تغيير أي شفرة رئيسية أو تحديث للنظام. اختبارات الاختراق تحاكي الهجمات السيبرانية مثل تعطيل الخدمات الموزعة DDoS وذلك للتعرف على مناطق الضعف في النظام الذي يتم فحصه.	

	٦. ثقّف موظفيك ودرّبهم باستمرار	نطاق التطبيق
٦-١	**طوّر ونفذ سياستي الأمن السيبراني وخصوصية المعلومات**	
	طور ونفّذ سياسة الأمن السيبراني والتي ستحدد ما يستطيع موظفوك فعله وما لا يستطيعون فعله عند استخدامهم لأنظمة العمل، ويجب أن توضح السياسة العواقب التي سيواجهها الموظف في حال انتهاكه لها. ويجب الأخذ بالحسبان ضرورة تدريب موظفيك دوريًا على متطلبات الأمن السيبراني الموضحة في سياسة الأمن السيبراني. أيضاً طوّر سياسة خصوصية المعلومات على أن تكون مبنيةً على أفضل الممارسات العالمية المقبولة في الخصوصية. تأكد من نشر إشعار الخصوصية على متجرك الإلكتروني لتوضح للمستهلكين مدى التزامك بحماية وخصوصية بياناتهم.	
٦-٢	**اعمل على الحماية من رسائل التصيد الإلكتروني والهندسة الاجتماعية**	
	احرص على رفع مستوى الوعي لدى موظفيك للحماية من رسائل التصيد الإلكتروني والهندسة الاجتماعية. حيث تعني الهندسة الاجتماعية التلاعب النفسي بالأشخاص لجعلهم يفصحون عن معلومات سرية شخصية ومالية. ويستخدم المهاجمون رسائل التصيد الإلكتروني لإجراء هجمات الهندسة الاجتماعية وجمع المعلومات التي يحتاجونها لارتكاب عمليات الاحتيال أو الوصول لأنظمة الحواسب الآلية الخاصة بالعمل أو حسابات التواصل الاجتماعي. يجب عليك تثقيف موظفيك حول علامات رسائل التصيد الإلكتروني، والتي قد تتسم بشيء من السمات الآتية: • ضعف في الإملاء والقواعد اللغوية وعلامات الترقيم. • استخدام كلمات مثل «صديق» أو «زميل عزيز» بدلًا من مخاطبة شخص محدد. • تتميز هذه الرسائل بطابع من الإلحاح، من حيث الوقت أو طلب من شخص أعلى رتبة في الشركة. • قد تقدم خصمًا كبيرًا على سلعة مطلوبة.	

٦-٣	**امنع طاقم العمل من تحميل تطبيقات غير معروفة**	
	درّب موظفيك على استخدام البرمجيات الضرورية للعمل فقط وتحميلها من مصادر موثوقة مثل متاجر التطبيقات (App Store).	
٦-٤	**درب موظفيك على التعامل مع بلاغات الحوادث وعلامات الاختراق**	
	درّب موظفيك على التعامل مع بلاغات حوادث الأمن السيبراني و التعرف على علامات الاختراق، ودرّبهم أيضًا على التبليغ عن حوادث الأمن السيبراني فورًا، بعض العلامات المتعارف عليها قد تبدو في: •البطء الشديد في استجابة الحاسب الآلي أو التطبيقات أو الشبكة للأوامر والطلبات. • عدم القدرة على دخول الحسابات الحساسة وتلقي رسائل تفيد بتغيير كلمة المرور على الرغم من عدم تغييرك لها. • عدم القدرة على الوصول لملفاتك أو التطبيقات أو الخدمات.	

	٧. اعمل على حماية البنية التحتية الداخلية لتجارتك الإلكترونية	نطاق التطبيق
٧-١	**احفظ نسخك الاحتياطية في مكان آمن**	
	ضع الأقراص الخارجية الصلبة التي تستخدمها لتخزين نسخك الاحتياطية في مكان آمن، وذلك في خزنة مقاومة للحرائق أو من الأفضل وضعها في مبنى آخر.	
٧-٢	**ثبّت أنظمة تصفية الرسائل غير المرغوب فيها**	
	ثبّت أنظمة تصفية الرسائل غير المرغوب فيها على مقسم البريد الإلكتروني. ستحجب أنظمة تصفية الرسائل غير المرغوب فيها أغلبية الرسائل الاقتحامية والمزعجة وستسمح فقط للرسائل المقبولة والشرعية بالوصول إلى البريد الإلكتروني الخاص بتجارتك الإلكترونية. وابقِ عناوين البريد الإلكتروني لموظفيك سرية، واستخدم عناوين بريد إلكترونية عامة (مثل help@companyname.com) للمعلومات التي ترغب في نشرها للعموم. تجنب فتح الروابط التي يتم إرسالها من قبل المستهلكين حيث أن بعضهم يرسل روابط إلى مواقع وبرامج ضارة على أنظمتك.	
٧-٣	**راجع سجلات التدقيق والفحص والسجلات الأمنية**	
	راجع سجلات التدقيق والفحص وسجلات الأحداث الأمنية (مثل السجلات التي تحتوي على معلومات أنشطة تسجيل الدخول والخروج) والتي تساعد في الرصد والتحقيق في الهجمات السيبرانية. عليك متابعة سجلات التدقيق والفحص والسجلات الأمنية باستمرار، إذ سوف تكشف هوية الأشخاص الذين قاموا بالوصول لأنظمة تقنية المعلومات والعمليات التي قاموا بإجرائها. سيساعد الحفاظ على سجلات التدقيق والفحص بطريقة سليمة أيضًا على استرداد العمليات التجارية المفقودة وسيوّضح مناطق الضعف الأمنية ونقاط الاختراق غير المشروع المحتملة على تجارتك الإلكترونية.	

٤-٧	**استخدم تفعيل البريد الإلكتروني و حروف التحقق (CAPTCHA) لتسجيل المستخدمين**	
	اطلب من المستخدمين تأكيد تسجيلهم عبر النقر على رابط التفعيل المُرسل لبريدهم الإلكتروني أو باستخدام حقل حروف التحقق « CAPTCHA » (فحص إلكتروني يُستخدم للتأكد من أن المستخدم بشري) وذلك لتجنب التسجيل الضخم الذي تتسبب به الحملات الاقتحامية. من المهم جعل عملية استخدام رابط التفعيل سهلة (كإرسال البريد الإلكتروني فورًا أو وضع مهلة انتهاء) وجعل تحدي حروف التحقق بسيطًا بما يكفي حتى لا يؤدي إلى إزعاج المستخدمين الشرعيين.	
٥-٧	**استعمل برمجيات منع الاحتيال**	
	استخدم برنامج لمنع الاحتيال في التجارة الإلكترونية وهو أحد الطرق الجيدة لمنع الهجمات مثل النقر الاحتيالي والتسجيل الضخم وإساءة الاستخدام التي تؤثر على المخزون (inventory abuse) يقدم الكثير من الموردين حلولاً تحتوي على خوارزميات لرصد النقر الاحتيالي أو التسجيل الضخم بالإضافة إلى قائمة سوداء لعناوين الشبكات المخادعة المعروفة.	
٦-٧	**اختر منصة تجارية إلكترونية آمنة**	
	اختر الشركات الموثوقة والمعروفة والتي لديها تقييم جيد وتتحلى بشفافية حول سياسة الخصوصية وذلك عند البحث عن أنسب موقع تجارة الكترونية أو منصة دفع تجارية. أيضاً ابحث عن الموردين الدوليين الممتثلين للمعايير الدولية مثل ISO و PCI أو الموردين المحليين المطبقين للمعايير المتعلقة بالأمن السيبراني والصادرة من الجهات ذات العلاقة مثل (الهيئة الوطنية للأمن السيبراني، مؤسسة النقد العربي السعودي، وغيرها). وغالباً فإن بوابات الدفع الآمنة تكون مزودة بخصائص أمنية كنظام الحماية الآمن (مثل Verified by Visa) و خدمات التعرف على الاحتيال والتي تتضمن عناوين الشبكة والأسماء والمشتريات السابقة لتحديد مدى صحة عملية الشراء من عدمها. كما يجب مراجعة التزامات الحماية المقدمة من بوابات الدفع بشكل فعال واستباقي في حال حدوث هجوم سيبراني ويشمل ذلك أهمية الإفصاح عن الاختراقات.	
٧-٧	**صمّم صفحة لتسجيل المستخدمين**	
	صمّم نموذج ورابط للتسجيل خاص بالموقع في حال إذا كنت ترغب بالسماح للمستخدمين بالتسجيل في موقعك الإلكتروني. تكون التطبيقات الروبوتية الخبيثة (malicious bots) (تطبيقات تقوم بتشغيل مهام تلقائيًا عبر الإنترنت) وهي في الغالب مبرمجة للبحث عن روابط افتراضية أو عوامل الإدخال لتسجيل مستخدمين مزيفين. الكثير من منصات التجارة الإلكترونية مزودة بخصائص التعديل لتجنب تهديدات التطبيقات الخبيثة.	
٨-٧	**اعمل على حماية بضاعتك من تهديدات تعطيل المخزون**	
	قلل من تهديد هجمات تعطيل المخزون عن طريق استخدام سياسة سلة المشتريات وهي عبارة عن تعيين مدة معينة لحجز بضاعة من المتجر قبل إتمام عملية الشراء، وذلك عن طريق تحديد عدد المرات التي يمكن السماح بها لإعادة البضاعة إلى سلة المشتريات بعد حذفها. إن تعطيل المخزون هي مشكلة حقيقية إذ تقوم التطبيقات الخبيثة بحجز بضائع من مخزون المتجر بدون إتمام عملية الشراء بصورة كاملة مما يؤدي إلى نفاذ كمية هذه البضائع عن المشترين الشرعيين.	

ملحق أ: مصطلحات وتعاريف

يبين الجدول الآتي بعض المصطلحات المذكورة في هذه الوثيقة ومعانيها.

المصطلح	التعريف
هجوم **Attack**	أي نـوع مـن الأنشـطة الخبيثـة التـي تحـاول الوصـول بشـكل غـير مـشروع أو جمـع مـوارد النظـم المعلوماتيـة أو المعلومـات نفسـها أو تعطيلهـا أو منعهـا أو تحطيمهـا أو تدميرهـا.
النسخ الاحتياطية **Backup**	الملفـات والأجهـزة والبيانـات والإجـراءات المتاحـة للاسـتخدام في حـال الأعطـال أو الفقـدان، أو إذا حـذف الأصـل منهـا أو توقـف عـن الخدمـة.
رمز التحقق **CAPTCHA**	كلمـة CAPTHCA باللغـة الإنجليزيـة هـي اختصـار لاختبـار تورينـج العـام الآلي كليًـا للتفريـق بـين البشر والحواسـيب الآليـة Completely Automated Public Turing test to tell Computers and Humans Apart – وهـو برنامـج أو نظـام يسـتطيع التفريـق بـين إدخـال البـشر وبـين إدخـال الآلات، ويُسـتخدم عـادةً لتفـادي الإقحـام واسـتخراج البيانـات الآلي مـن المواقـع الإلكترونيـة.
الأمن السيبراني **Cybersecurity**	حسـب مـا نـص عليـه تنظيـم الهيئـة الصـادر بالأمـر الملـكي رقـم (٦٨٠١) و تاريـخ (١٤٣٩/٢/١١هـ)، فـإن الأمـن السـيبراني هـو حمايـة الشـبكات وأنظمـة تقنيـة المعلومات وأنظمـة التقنيـات التشـغيلية، ومكوناتهـا مـن أجهـزة وبرمجيـات، ومـا تقدمـه مـن خدمـات، ومـا تحتويـه مـن بيانـات، مـن أي اختـراق أو تعطيـل أو تعديـل أو دخـول أو اسـتخدام أو اسـتغلال غـير مـشروع. ويشـمل مفهـوم الأمـن السـيبراني أمـن المعلومـات والأمـن الإلكـتروني والأمـن الرقمـي ونحـو ذلـك.
موفر خدمة التجارة الإلكترونية **E-commerce Service Provider**	التاجـر (الشـخص المقيـد بالسـجل التجـاري الـذي يـزاول التجـارة الإلكترونيـة) أو المـمارس (الشـخص غـير المقيـد بالسـجل التجـاري الـذي يـزاول التجـارة الإلكترونيـة).
حادثة **Incident**	انتهـاك أمنـي يخالـف سياسـات الأمـن السـيبراني أو سياسـات الاسـتخدام المقبـول أو ممارسـات الأمـن السـيبراني أو ضوابطـه أو متطلباتـه.
البرمجيات الضارة **Malware**	برنامـج يصيـب الأنظمـة بطريقـة خفيـة (في الغالـب) لانتهـاك سريـة أو سـلامة ودقـة أو توافـر البيانـات أو التطبيقـات أو نظـم التشـغيل.

المصطلح	التعريف
التحقق من الهوية متعدد العناصر Multifactor Authentication (MFA)	نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: • المعرفة (شيء يعرفه المستخدم فقط «مثل كلمة المرور»). • الحيازة (شيء يملكه المستخدم فقط «مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول» ويطلق عليها «One Time Passwords»). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط «مثل بصمة الإصبع»).
النسخ الاحتياطي المتصل Online Backup	طريقة للتخزين يتم فيها النسخ الاحتياطي بانتظام عبر شبكة على خادم بعيد، (إما داخل شبكة الجهة أو بالاستضافة لدى مزود خدمة).
حزم التحديثات والإصلاحات Patch	حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسب الآلي أو لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات أو إصلاح الأخطاء وتحسين إمكانية الاستخدام أو الأداء.
الخصوصية Privacy	الحماية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد معين.
المنشآت الصغيرة والمتوسطة SME	موفري الخدمة الذين لديهم من ٦ إلى ٢٤٩ موظفاً وأرباحهم من ٣ إلى ٢٠٠ مليون ريال سعودي.
المكاتب الصغيرة والمنزلية SoHo	موفري الخدمة من الأفراد أو الذين لديهم موظف واحد إلى خمسة موظفين وأرباحهم أقل من ثلاثة ملايين ريال سعودي.
تهديد Threat	أي ظرف أو حدث يحتمل منه أن يؤثر سلباً على أعمال الجهة أو الفرد (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها ويُستغل في ذلك أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال إحدى نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority