الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

إرشادات الأمن السيبراني
لمستهلكي التجارة الإلكترونية

Cybersecurity Guidelines for E-commerce Consumers

(CGEC – 1: 2019)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

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، والمملكة هي أحد أكبر أسواق التجارة الإلكترونية في منطقة الشرق الأوسط وشمال أفريقيا، ولمواكبة النمو المتسارع للتجارة الإلكترونية والمخاطر المصاحبة لها على المستهلكين، 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 طـورت الهيئة الوطنية للأمن الـسـيـبراني إرشـــادات الأمـن الـسـيـبراني لمستهلكي الـتـجـارة الإلكترونية (CGEC – 1: 2019) بهدف مساعدة المستهلكين في المملكة للأخذ بأفضل الـممارسـات لحماية أجهزتهم وأنظمتهم وحساباتهم وبياناتهم وعمليات الـدفـع عند تسوقهم عـبر قـنـوات الـتـجـارة الإلكترونية.

الإرشادات الرئيسية هي:

١. اعمل على حماية حساباتك وأجهزتك المستخدمة في التجارة الإلكترونية.
٢. اعمل على حماية عملياتك ذات العلاقة بالتجارة الإلكترونية.
٣. توخَ الحذر عند الاتصال بالإنترنت لغرض التجارة الإلكترونية.
٤. قلل مشاركة معلوماتك الشخصية.

هذه الوثيقة تعرض تفاصيل هذه الإرشادات الرئيسية.

المقدمة

طوّرت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ «الهيئة») إرشادات الأمن السيبراني لمستهلكي التجارة الإلكترونية (CGEC – 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.

وفقًا لدراسة حديثة[1] عن السوق في المملكة، فإن نحو ٥٨٪ من السكان قد قاموا بالتسوق عبر الإنترنت على الأقل مرة كل ثلاثة أشهر، وأنفقوا ما متوسطه أربعة آلاف ريال سعودي على التسوق عبر الإنترنت سنويًا. ومن المرجح أن هذه الأرقام في ارتفاع، بسبب الاستخدام المتزايد للحلول المتنقلة مثل تطبيقات الهواتف الذكية وزيادة سهولة التسوق عبر الإنترنت. ووفقًا للدراسة نفسها، فإن عددًا كبيرًا من سكان المملكة قد قاموا بالشراء من شركات واقعة في دول الخليج العربي ودول خارج المنطقة، في حين قام عدد بسيط من المستهلكين (٧٪) بالشراء بشكل حصري من موفّري خدمة تجارة إلكترونية مقرهم في المملكة العربية السعودية.

إن بعض الدوافع الرئيسية لهذا النمو المتسارع واعتماد استخدام التجارة الإلكترونية هو التوصيل المنزلي وتوفير الوقت والعروض المغرية والأسعار المناسبة على الإنترنت ومجموعة المنتجات الواسعة التي يمكن الاختيار منها، ولكن التجارة الإلكترونية قد تسببت أيضًا في أنواع جديدة من التهديدات، التي تشير إليها هذه الإرشادات.

نطاق التطبيق

تستهدف هذه الإرشادات جميع المستهلكين في المملكة والذين يقومون بالتسوق الإلكتروني عبر أي قناة كانت (مثل مواقع التواصل الاجتماعي والمواقع الإلكترونية والتطبيقات) باستخدام أي جهاز إلكتروني (مثل أجهزة الحاسب الآلي والهواتف والتلفزيونات الذكية والأجهزة اللوحية).

هذه الإرشادات توعوية والغرض منها مساعدة المستهلكين لخوض تجربة تجارة إلكترونية آمنة.

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

إرشادات الأمن السيبراني لمستهلكي التجارة الإلكترونية

١. اعمل على حماية حساباتك وأجهزتك المستخدمة في التجارة الإلكترونية

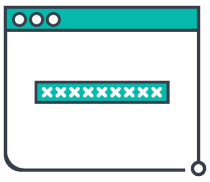
١-١ استخدم برامج الحماية من الفيروسات

- استخدم برامج الحماية من الفيروسات على كل أجهزتك، خاصةً الأجهزة التي تستخدمها عادةً للتجارة الإلكترونية. إذا كان جهازك لا يحتوي على أي برنامج مثبت مسبقًا للحماية من الفيروسات، فإنه يُنصح بتثبيت برنامج للحماية قبل القيام بأي عملية تجارية إلكترونية.
- تأكد من استخدامك لنسخ موثوقة ورسمية من برامج الحماية من الفيروسات.

١-٢ استخدم كلمات مرور مختلفة

- احرص على استخدام كلمات مرور مختلفة لكل واحد من المواقع والتطبيقات التي تتسوق منها عادةً. عليك أيضًا استخدام كلمات مرور مختلفة لأجهزتك وحساباتك في مواقع التواصل الاجتماعي.
- غيّر كلمات المـرور دوريًـا لحماية هويتك الرقمية ولا تشارك كلمات المـرور مع الآخرين.

١-٣ اختر كلمات مرور قوية



- اتبع أفضل الممارسات عند اختيار كلمة مرور لحساباتك المتعلقة بالتجارة الإلكترونية:
  - تجنب استخدام الكلمات الشائعة (مثل qwerty أو password) أو تسلسل بسيط للأرقام (مثل ١٢٣٤٥٦) أو المعلومات الشخصية (مثل تاريخ الميلاد أو سنة التخرج).
  - لا تكتبها على الورق.
  - اختر كلمة مرور طويلة ومعقدة قدر الإمكان، باستخدام مجموعة من الأحرف (الكبيرة والصغيرة) والرموز (!@#$%^&*) والأرقام العشوائية.

١-٤ خذ بعين الاعتبار استخدام خيارات تحقق إضافية

- استـخـدم آلـيـات الـتـحـقـق الإضـافـيـة (مـثـل رسـائـل الـبـريـد الإلـكـتـروني) في حـال تـوفـرهـا مـن قـبـل تطبيقات الـتـجـارة الإلـكـتـرونـيـة ومـواقـعـهـا (شاملةً حسابات التواصل الاجتماعي).
- اختر التسوق من موفري خدمة التجارة الإلكترونية الذين يقدمون خيار تحقق الأمان الإضافي.

١-٥ حدّث التطبيقات دوريًا

- احرص أن تكون جميع التطبيقات (بما في ذلك أنظمة التشغيل وبرامج الحماية من الفيروسات) المثبتة على أجهزتك محدّثة دائمًا. يمكنك القيام بهذه التحديثات آليًا (بالسماح بهذه الميزة على جهازك) أو يدويًا (بتحديد وقت معين من الأسبوع/الشهر للقيام بالتحديثات).

١-٦ قم بالنسخ الاحتياطي لبياناتك

- ضع نسخاً احتياطية لبياناتك على سبيل المثال عن طريق نسخها على حاسبك الآلي أو على قرص صلب خارجي وذلك لتلافي فقدان بياناتك في حال تعرض جهازك (الذي تستخدمه للتجارة الإلكترونية) للفيروسات.
- فعّل خاصية النسخ الاحتياطي التلقائي في حال توفرها على جهازك.

١-٧ غيّر الإعدادات الافتراضية على أجهزتك وحساباتك

- راجع وغير إعدادات الأمان والسرية الافتراضية في حساباتك ومتصفح الإنترنت كي تتجنب حفظ معلومات تسجيل الدخول أو بيانات الدفع أو الحسابات البنكية على سبيل المثال.

١-٨ انتبه للتحذيرات الأمنية

- لا تتجاهل التحذيرات الأمنية (مثل التنبيهات عن عدم موثوقية موفّري الخدمة أو المواقع الإلكترونية غير الآمنة) والتي قد تظهر على شاشتك.
- تأكد من قراءتك وفهمك للتحذيرات قبل اتخاذك لأي تصرف.

٢ . اعمل على حماية عملياتك ذات العلاقة بالتجارة الإلكترونية

٢-١ راجع عملياتك دوريًا

- راجع كشوفاتك البنكية (خاصةً بطاقتك الائتمانية) وعمليات محفظتك الإلكترونية (eWallet) دوريًا واتصل على البنك فورًا عند رؤيتك لأي عمليات شراء مشتبه بكونها احتيالية. كما يمكنك إيقاف بطاقتك الائتمانية في حال تم استخدامها بشكل غير مشروع، وذلك عن طريق تطبيق البنك على الأجهزة الذكية أو الموقع الالكتروني على سبيل المثال. كلما تم رصد الاحتيال عبر الإنترنت بشكل أسرع، كلما استطاع البنك تنبيه بقية المستهلكين بشكل أسرع.
- تأكد من تحديث معلومات الاتصال بك لدى الجهة المصدرة لبطاقتك الائتمانية (وسيلة الدفع).
- فعّل تنبيهات الرسائل النصية على بطاقتك الائتمانية ومحفظتك الإلكترونية لتبقى على علم بجميع العمليات التي تتم على حسابك.

٢-٢ استخدم بطاقة ائتمانية مخصصة

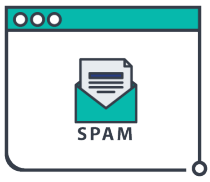
- حاول تخصيص بطاقة واحدة فقط لعمليات التسوق الإلكتروني في حال إذا كان لديك عدد من البطاقات الائتمانية.
- استخدم بطاقة ذات حد منخفض أو بطاقة مسبقة الدفع إذا كانت متوفرة لدى البنك الذي تتعامل معه.

٢-٣ اعمل على حماية محفظتك الإلكترونية

- تأكد من حماية الوصول لمحفظتك الإلكترونية باستخدام آلية تحقق قوية (مثل كلمة المرور) حيث أنه ازدادت الهجمات المتعلقة بالمحافظ الإلكترونية منذ أصبحت هذه المحافظ أكثر استخدامًا وشعبية للمتسوقين عبر الإنترنت.
- راجع حساب محفظتك الإلكترونية باستمرار للتأكد من عدم وجود أي نشاطات مشبوهة (مثل محاولة تسجيل دخول فاشلة).

٣. توخَ الحذر عند الاتصال بالإنترنت لغرض التجارة الإلكترونية

٣-١ اعمل على حماية حسابك من الرسائل غير المرغوب فيها (SPAM)

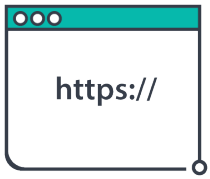


- فعّل نظام تصفية الرسائل غير المرغوب فيها (SPAM) على بريدك الإلكتروني حيث يوفر الكثير من مقدمي خدمات البريد الإلكتروني (وخاصة البريد الإلكتروني على الإنترنت) هذا النظام.
- بلّغ مقدم الخدمة أو منصة التواصل الاجتماعي فورًا عن الرسائل غير المرغوب فيها (على البريد الإلكتروني أو مواقع التواصل الاجتماعي).
- خصص بريداً إلكترونيًا لاستخدامه حصراً في التسوق الإلكتروني.

٣-٢ احذر من الاتصالات الاحتيالية

- احذر من الاتصالات الاحتيالية حيث أن أحد طرق الاحتيال الشائعة هي الاتصالات من موفري خدمة تجارة إلكترونية مزيفين يمتلكون عادةً مواقع مزيفة أو حسابات مزيفة في مواقع التواصل الاجتماعي.
- حاول قدر الإمكان أن تتسوق وتتعامل مع موفّري الخدمة الموثوقين فقط. أحد الطرق الجيدة للتأكد من سمعة موفري الخدمة وشرعيتهم هي منصات تقييم السمعة والموثوقية عبر الإنترنت (مثل منصة معروف[٢]).

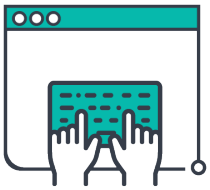
٣-٣ استخدم مواقع إلكترونية آمنة



- تأكد أن رابط الموقع يبدأ بـ (https://) بدلًا من (http://) قبل إدخال معلوماتك الشخصية أو المالية.
- تجنب التعامل مع موفّري الخدمة الذين لا يقدمون هذه الحماية المتقدمة حيث أن خاصية الحماية هذه تعني أن الموقع محمي ببروتوكولات تشفير موثوقة تساعد على حماية معلوماتك الشخصية والمالية.

[٢] https://maroof.sa

٣-٤ احذر الروابط في الإعلانات



- تجنّب النقر على الروابط التي تراها في الرسائل (على البريد الإلكتروني أو الرسائل النصية أو مواقع التواصل الاجتماعي) أو على الإنترنت (في الإعلانات عادةً) لأنها قد تقوم بتحويلك إلى مواقع مزيفة.
- احذر من المواقع المزيفة والتي تتسم غالباً بعلامات مثل عرض أسعار مثيرة للشك للمنتجات.

٣-٥ تسوّق باستخدام تطبيقات وأجهزة وشبكات آمنة

- احذر من التطبيقات والمواقع المزيفة، ويمكنك تجنبها على سبيل المثال عن طريق تحميل التطبيقات من متجر التطبيقات الرسمي.
- تجنب إجراء عمليات الدفع الإلكترونية أو إدخال بيانات تسجيل الدخول على مواقع التواصل الاجتماعي عند استخدام الأجهزة العامة (مثل أجهزة مراكز العمل في الفنادق) أو الاتصال بشبكة إنترنت لاسلكية عامة (مثل الشبكات اللاسلكية في المطارات).

٣-٦ بلّغ بسرعة عن الحوادث

- تصرّف بسرعة وأبلغ موفر خدمة التجارة الإلكترونية في حال اختراق أي من حساباتك المستخدمة للتجارة الإلكترونية.
- تـواصـل مـع البنك فـوراً في حـال سرقـة معلومات الـدفـع الخاصة بـك. تذكر أنه كلما أسرعت في التبليغ عن الحادث، كلما قمت بالحد من الأضرار.
- تواصل فوراً مع الجهات المختصة في حال اختراق هاتفك.

٤ . قلل مشاركة معلوماتك الشخصية

٤-١ اقرأ سياسة الخصوصية

- تسوّق فقط من موفّري الخدمة الذين يتميزون بسمعة جيدة ولديهم سياسة خصوصية منشورة. إقرأ السياسة وتأكد من أنها تشرح بوضوح كيف سيتم استخدام بياناتك وتخزينها من قبل موفر الخدمة.
- تجنب التعامل مع موفّري الخدمة الذين تشمل سياساتهم إساءة استخدام البيانات الشخصية (مثل إعطاء المعلومات الشخصية للمستهلكين (بدون موافقتهم) لوكالات الإعلانات).

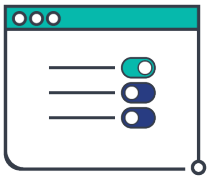
٤-٢ اعمل على حماية معلوماتك الشخصية

- لا تزوّد مواقع التجارة الإلكترونية بمعلومات أكثر من المطلوب عند تسجيل الحساب أو التسوق.
- شارك المعلومات المطلوبة لإتمام عمليات الدفع للمتجر الإلكتروني فقط ولا تقم بالموافقة على خيار حفظ أو تخزين معلوماتك الشخصية أو المالية على التطبيقات أو المواقع الإلكترونية.
- لا تقم بمشاركة معلومات البطاقة الائتمانية عبر القنوات غير الآمنة وغير المشفرة (مثل البريد الإلكتروني أو رسائل التواصل الاجتماعي).

٤-٣ تجاهل رسائل التصيد الإلكتروني

- تجنب رسائل التصيد الإلكتروني بالتأكد من هوية المرسل قبل فتح الرسالة. حيث أن رسائل التصيد الإلكتروني هي رسائل تظهر وكأنها من مرسل شرعي، والهدف منها هو خداع مستلم الرسالة للإفصاح عن معلومات شخصية مثل اسم المستخدم أو كلمة المرور أو تفاصيل البطاقة الائتمانية.

٤-٤ حدد صلاحيات التطبيقات



- فكّر جيدًا في منطقية طلب تطبيقات الهواتف الذكية أو الموقع الإلكتروني لبعض الصلاحيات للوصول لعدد من البيانات والمهام على جهازك (مثل الموقع الجغرافي والكاميرا والعناوين والميكروفون).

ملحق أ: مصطلحات وتعريفات

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.
الأمن السيبراني **Cybersecurity**	حسـب مـا نـص عليـه تنظيـم الهيئـة الصـادر بالأمـر الملـكي رقـم (٦٨٠١) و تاريـخ (١١ / ١٤٣٩/٢هـ)، 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 اخـتراق 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).
بروتوكول نقل النص التشعبي الآمن **Hyper Text Transfer Protocol Secure (HTTPS)**	بروتوكـول يسـتخدم التشـفير لتأمـين صفحـات الويـب وبياناتهـا عنـد انتقالهـا عبر الشـبكة وهـو نسـخة آمنـة مـن نظـام بروتوكول نقـل النـص التشـعبي (HTTP).
حادثة **Incident**	انتهـاك أمنـي يخالـف سياسـات الأمـن السـيبراني أو سياسـات الاسـتخدام المقبـول أو ممارسـات الأمـن السـيبراني أو ضوابطـه أو متطلباتـه.
التصيد الإلكتروني **Phishing**	محاولـة الحصـول عـلى معلومـات حساسـة مثـل أسـماء المسـتخدمين وكلـمات المـرور أو تفاصيـل بطاقـة الائتـمان، وتكـون في الغالـب لأسـباب ونوايـا ضـارة وخبيثـة، وذلـك بالتنكـر عـلى هيئـة جهـة جديـرة بالثقـة في رسـائل البريـد الإلكـتروني أو الرسـائل النصيـة أو الرسـائل عـلى مواقـع التواصـل الاجتماعـي.

المصطلح	التعريف
الخصوصية **Privacy**	الحمايـة مـن التدخـل غـير المـصرح بـه أو الكشـف عـن معلومـات شـخصية حـول فـرد معـين.
تهديد **Threat**	أي ظـرف أو حـدث يحتمـل منـه أن يؤثـر سـلباً عـلى أعـمال الجهـة أو الفـرد (بمـا في ذلـك مهمتهـا أو وظائفهـا أو مصداقيتهـا أو سـمعتها) أو أصولهـا أو منسـوبيها مسـتغلاً في ذلـك أحـد أنظمـة المعلومـات عـن طريـق الوصـول غـير المـصرح بـه إلى المعلومـات أو تدميرهـا أو كشـفها أو تغييرهـا أو حجـب الخدمـة. وأيضـاً قـدرة مصـدر التهديـد عـلى النجـاح في اسـتغلال إحـدى نقـاط الضعـف الخاصـة بنظـام معلومـات معـين. وهـذا التعريـف يشـمل التهديـدات السـيبرانية.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority