وزارة الإتصالات و تكنولوجيا المعلومات

Ministry of Information and Communications Technology

هيئة تنظيم قطاع الاتصالات - الأردن

Telecommunications Regulatory Commission - Jordan

# إرشادات الاستخدام الآمن للإنترنت

# فهرس المحتويات

## أولا: مقدمة

تنفيذا لوثيقة السياسة العامة لقطاع الاتصالات وتكنولوجيا المعلومات 2012، وتحديداً للبند 140 منها والذي ينص على أنه: "ستقوم الحكومة، من خلال الهيئة، بالعمل مع مزودي خدمات الانترنت لتوفير المشورة للمستخدمين حول الاستخدام الآمن للإنترنت وحماية الأطفال، وكذلك بالعمل على منع وحجب المواقع الإباحية بالوسائل الممكنة ومن خلال تمكين المستفيدين من الحد من النفاذ الى أي محتوى غير مرغوب به، واتخاذ أي من الإجراءات التشريعية والتنظيمية لتحقيق ذلك"، عملت كلٌ من وزارة الاتصالات وتكنولوجيا المعلومات وهيئة تنظيم قطاع الاتصالات على إعداد هذه الإرشادات؛ وذلك بهدف توعية المستخدمين حول الاستخدام الآمن للإنترنت والطرق المقترح إتباعها، وتوفير ممكنات البيئة الآمنة لمستخدمي الانترنت على مختلف شرائحهم وطبيعة اهتماماتهم واستخداماتهم للإنترنت.

ويُعرَّف الاستخدام الآمن للإنترنت بشكل عام على أنه مجموعة من الإرشادات والممارسات الموصى باتباعها بهدف تحقيق الأمان عند استخدام الإنترنت، والمتمثلة بتمكين المستخدم من حماية ممتلكاته و/أو قيمه من المخاطر الإلكترونيّة المختلفة وما يترتب عليها من اعتداءات لفظية أو جسدية أو عاطفية سواءً كانت بشكل مباشر أو غير مباشر، وهي تشمل ولا تنحصر بالتعرض للاستغلال أو الانتهاك أو التنمر أو الاساءة أو الابتزاز أو انتحال الشخصيّة أو السرقة.

وقد تم إعداد هذه الإرشادات بحث تكون موجهة لفئات المستخدمين المختلفة، وذلك بهدف مخاطبة كل فئة حسب طبيعة استخدامها وتعاملها مع الإنترنت، بغرض تحقيق الهدف المنشود وراء إعداد هذه الإرشادات بكل فعالية. وقد تم التعامل مع الفئات التالية المستخدمة للإنترنت كفئات مستهدفة عند إعداد الإرشادات:

1- الشركاء في قطاع الاتصالات وتكنولوجيا المعلومات

- مزودو خدمات الانترنت
- مزودو خدمات المحتوى على الانترنت
- مقدمو خدمات التجارة الإلكترونية

2- مستخدمو الانترنت عبر مراكز ومقاهي الانترنت وعبر نقاط النفاذ اللاسلكية المجانية (الواي فاي)

3- أولياء الأمور والتربويين والأطفال.

4- المشتركون ومستخدمو مواقع التواصل الاجتماعي والمتعاملون بالتجارة الإلكترونية.

## ثانيا: إرشادات الاستخدام الآمن للإنترنت

### 1- إرشادات عامة للشركاء في قطاع الاتصالات وتكنولوجيا المعلومات:

هذه الإرشادات موجهة إلى الشركاء في قطاع الاتصالات وتكنولوجيا المعلومات المعنيين بتقديم خدمات النفاذ للإنترنت وتطبيقات الانترنت المختلفة ليصار الى تنفيذها من قبلهم، بهدف توفير ممكنات البيئة الآمنة لعملائهم المستفيدين من خدمات الإنترنت.

ويوصى بتعميم هذه الإرشادات على الشركاء المعنيون بالتنفيذ و يتمثلون الجهات التي تمارس أياً من الأعمال التالية:

- تزويد خدمات الانترنت
- تزويد خدمات المحتوى
- تقديم خدمات التجارة الإلكترونية
- تقديم خدمات الدخول إلى الانترنت عبر مراكز ومقاهي الانترنت المرخصة
- تقديم خدمة الدخول المجاني إلى الانترنت عبر نقاط النفاذ اللاسلكية (واي فاي)

أ. إرشادات موجهة لمزودي خدمات الانترنت تسهم في تحقيق الاستخدام الآمن للإنترنت لمشتركيهم:

1. توفير الخيار للمشتركين بالحصول على خدمات مدفوعة الثمن تعنى بحماية أجهزتهم من الفايروسات والبرامج الخبيثة والمواقع المشبوهة عند تصفح الإنترنت.
2. أهميّة قيام مزودي خدمة الإنترنت بتوثيق دخول مستخدمي نقاط نفاذ الإنترنت اللاسلكيّة المجانيّة ( Wi-Fi Hot Spot) التي يقومون بتوزيعها/تفعيلها في الشوارع والأماكن العامة والمواقع السياحية في مختلف محافظات المملكة لتتيح لجميع رواد هذه الاماكن التمتع باستخدام الإنترنت من خلال آلية إرسال كلمة السر الخاصة بالدخول لتصفح الإنترنت إلى رقم هاتف خلوي محلي(أردني) والتي يتطلب من المستخدم إدخالها بعد ذلك، لكي يتمكن من التفاعل مع الشبكة العنكبوتيّة وتصفح الإنترنت وبالتالي تسهيل تحديد هوية المستخدم من خلال رقم هاتفه المتنقل المدخل في حال تم إساءة إستخدام الخدمة من قبله.
3. اقتراح برامج مكافحة الفيروسات والجدران النارية ( PC firewalls ) المجانيّة ، بالإضافة إلى نشر أسماءها ورابط تنزيلها على مواقع الشركات الإلكترونيّة لتأمين أجهزة الحواسيب الخاصة بالمستفيدين، ويفضل أن تكون تلك البرامج من ضمن البرامج المعروفة والموصى بها عالميا.
4. إمكانية اقتراح برامج مجانيّة للكشف عن الملفات الخبيثة كملفات التجسس والملفات الدعائية والملفات التي تسيطر على متصفح الإنترنت.
5. شمول عروض الشركات لأجهزة الحاسوب أو الأجهزة الخلوية الذكية بحيث تكون مزودة ببرامج مرخصة لحماية هذه الأجهزة من الفايروسات والبرامج الخبيثة مع القابلية لتنزيل آخر التحديثات وبشكل أوتوماتيكي.
6. في حال تقديم خدمة البريد الإلكتروني، تقوم الشركة بتوفير آلية لفحص الملفات والمرفقات المرسلة مع الرسائل الإلكترونيّة، بحيث يتم عزل هذه الملفات في حال ثبوت بأنها مرسلة من عنوان وهمي أو احتيالي، أو تحتوي على توقيع لفايروسات متداولة. بالإضافة إلى توفير مرشحات رسائل البريد الالكتروني ( filters ) وخدمات مكافحة البريد غير المرغوب فيه ( anti-spam solutions )
7. توفير الخيار للمشتركين من قبل الشركات بالحصول على خدمات مدفوعة الثمن لفلترة المواقع الإلكترونيّة أو اقتراح برامج فلترة مجانيّة ليصار إلى تثبيتها على أجهزة الحاسوب التي يستخدمها الاطفال، على أن تقع مسؤولية متابعة الأخيرة على أولياء الأمور أنفسهم.
8. استخدم مواقع فحص المنافذ(ports) من جهات عالمية موثوقة، للتأكد من عدم وجود منافذ مفتوحة للمخترقين، وتعرف تلك المواقع باسم (online port scanners) .

ب. إرشادات موجهة لمزودي خدمات المحتوى على الانترنت:

1. الاحتفاظ بالسجلات الإلكترونية ( Log Files )، والتي تتيح التعرف على هوية صاحب المحتوى.
2. إطلاع صاحب المعلومة على سياسة الاستخدام الخاصة بالموقع الإلكتروني والاتفاق على تنفيذها بما يضمن صحة المحتوى المنشور ويحمّل الناشر مسؤولة المحتوى وبشكل لا يتعارض مع القوانين الناظمة حول هذا الموضوع.
3. عدم التعامل مع أي جهة تكررت مخالفتها لسياسة الاستخدام الخاصة بالموقع.
4. للمحتوى الذي يتضمن مادة لها تأثير سلبي نفسي أو مرضي على فئة معينة من المتصفحين كالأطفال أو المرضى أو غيرهم، يتم نشر رسالة تنويهيه تحذر من مضمون المحتوى قبل إتاحة تصفحه/مشاهدته.

جـ. إرشادات موجهة لمقدمي خدمات التجارة الإلكترونية:

1. تمكين المستخدم من إدخال بياناته الخاصة مثل رقم الحساب البنكي أو كلمة السر من خلال استخدام الفأرة للإدخال على لوحة المفاتيح الوهمية ( Virtual Keyboard ) .
2. يفضل تأكيد عملية الشراء من خلال إرسال رسالة نصية على الهاتف النقال الخاص بالمشتري تحمل رمز يدخله المشتري لإثبات هويته والاستمرار في عملية الدفع الإلكتروني.
3. توعية المتعاملين بالآليات المتبعة من قبل الموقع للحصول على المعلومات وخاصة تلك المتعلقة بالحسابات البنكية أو عملية الدفع الإلكتروني، تجنبا لاستخدام جهات خارجيّة لقنوات الاتصال المتبعة للحصول على معلومات لا يتوجب حصولهم عليها ويمكن أن يستغلوها بشكل يخالف التشريعات النافذة.
4. ضرورة قيام مقدمي خدمات التجارة الإلكترونيّة بعمل تحقق من نقاط الضعف، وذلك ( Vulnerabilities Check) للتحقق من عدم وجود أية ثغرات في مواقعهم الإلكترونيّة، والعمل على تحديثها دورياً لضمان عدم استغلال أية ثغرة إلكترونيّة.
5. ينصح بضرورة عدم تخزين البيانات الخاصة بالمستخدم وخاصة بيانات بطاقة الائتمان، وفي حال الحاجة إلى الاحتفاظ ببيانات ومعلومات المتعاملين، يجب أن تكون مخزنة بشكل مشفر لضمان عدم الاطلاع عليها من قبل الغير.
6. ضرورة بأن تكون خدمة الدفع الإلكتروني تعمل وفقاً لقناة مشفرة (https).
7. ضرورة بأن يقوم مقدمو خدمات التجارة الإلكترونيّة بحفظ بيانات وأماكن التسليم لزبائنهم للحيلولة دون استخدام بطاقات الائتمان الخاصة بالغير وعدم القدرة على معرفة المنتهك الأصلي، مما يمكّن من التحقق من هوية المستخدم الأصلي للبطاقة في حال تم استخدام البطاقة بشكل غير قانوني.
8. ضرورة توجيه المتعاملين بالتجارة الإلكترونيّة بعدم استخدام البريد الإلكتروني في عمليات تبادل المعلومات البنكيّة لغايات تنفيذ الحوالات الماليّة، بل الإعتماد على الطرق التقليديّة الأكثر أماناً لتلافي الوقوع تحت شرك العمليات الإحتياليّة من خلال هذه الحسابات الإلكترونيّة الوهميّة والتي يمكن أن لا تعود للأشخاص الذين سوف يتعاملوا معهم .

2- إرشادات موجهة لمستخدمي الانترنت عبر مراكز ومقاهي الانترنت وعبر نقاط النفاذ اللاسلكية المجانية (الواي فاي) معنونة بـ "لسلامة استخدامك للإنترنت في الاماكن العامة":

تعنى هذه الإرشادات بمخاطبة مستخدمي الإنترنت عبر مراكز ومقاهي الإنترنت وعبر نقاط النفاذ اللاسلكية المجانية، وكما يلي:

1. تجنب إرسال أو الافصاح عن أية معلومات شخصية غير ضرورية على شبكة الإنترنت، مثل بيانات الحساب البنكي ورقم الهاتف.
2. قم بتسجيل دخولك سواء من خلال السجلات اليدوية المعدة من قبل مقهى الانترنت أو من خلال البرنامج المعد من قبل الجهة المقدمة لخدمة الانترنت من خلال نقاط النفاذ، لحمايتك من أية مسائلات قانونية لاحقاً.
3. قم بعملية مسح المعلومات الخاصة بالمواقع التي قمت بزيارتها، بالإضافة إلى ملفات التعقب (cookies) بعد الانتهاء من الاستخدام.
4. ضرورة تنزيل الأدوات الإضافيّة (Add-on) الخاصة بالمتصفحات مثل موزيلا فايرفوكس أو جوجل كروم التي تعمل على ضمان الخصوصيّة وحماية معلومات المستخدم مثل ( Better Privacy ) أو( Privacy Badger ) الخ.
5. التحقق من تسجيل خروجك من حساباتك على الانترنت (البريد الإلكتروني، الخدمات البنكية الإلكترونية، مواقع التواصل الاجتماعي... الخ) لحمايتك من التعرض للسرقة أو الانتحال. وإغلاق المتصفح بعد ذلك.
6. تحقق من عدم قيامك بقبول خاصية الحفظ التلقائي لكلمات السر خلال دخولك لأي من حساباتك الشخصية على الانترنت (كبريدك الإلكتروني، مواقع التواصل الاجتماعي، الخ..).
7. تجنب فتح المواقع الإلكترونية ومواقع التواصل الاجتماعي من خلال الروابط المرسلة عبر البريد الإلكتروني إلا بعد التأكد من العنوان الحقيقي للرابط.

## 3- إرشادات توجيهية لأولياء الأمور والتربويين والأطفال:

تعنى هذه الإرشادات بتزويد المعلمين والمربين بمبادئ توجيهية وتوعوية تمكنهم من مساعدة الأطفال على المرور بتجارب آمنة وإيجابية خلال تصفح الإنترنت، وهي توجه أولياء الأمور إلى تهيئة أجهزة الحاسوب بطريقة تسمح باستخدام الإنترنت كمصدر للتعلم وليس كجهاز للتفاعل، كما تعنى بتوجيه الأطفال نحو الاستخدام الآمن للإنترنت.

ويوصى بتعميم هذه الإرشادات على المعنيين بالتنفيذ.

### أ. إرشادات توجيهية لأولياء الأمور والتربويين:

1. قم بتثبيت برمجيات الحماية من الفيروسات والبرامج الخبيثة والـ ( Firewalls ) على جهاز الحاسوب وحدثها بشكل دوري، إلى جانب برامج فلترة وحجب للمواقع الضارة والمسيئة.
2. قم بتثبيت عدد من البرامج والأدوات (التي يقترحها مزود خدمة الإنترنت) والتي من شأنها أن تسهل لك مراقبة الطلبة/ الأطفال أثناء استخدام الانترنت، وخاصة مواقع التواصل الاجتماعي والدردشة.
3. احرص على معرفة من يتواصل مع أبنائك عبر مواقع التواصل الاجتماعي.
4. احرص على حفظ بطاقات الائتمان الخاصة بك بعيداً عن أطفالك وأن تكون عملية الدفع بإشرافك الشخصي إن وجدت.

5. التأكيد على الأبناء بعدم القيام بأي عمليات شراء أو تحويل مالي على الانترنت أو عبر الهاتف النقال دون إشراف مباشر من الأهل، وعدم قبول أية عروض ترويجية من جهات غير معروفة المصدر لمنتجات على الإنترنت.
6. احرص على وضع الحاسوب في غرفة مشتركة لضمان تصفح الاطفال لمواقع الإنترنت بشكل سليم.
7. تحدث مع الطلبة/ الأطفال – وحسب فئاتهم العمريّة- عن مخاطر استخدام الإنترنت دون أخذ وسائل الحيطة والحذر، مع التأكيد على ضرورة الالتزام بالضوابط المفروضة، وعن كيفية التعامل الآمن مع الانترنت.
8. تحاور مع الطلبة/ الأطفال عن تجاربهم على شبكة الإنترنت لتعميم الفائدة ، وشجعهم على إخبارك في حال تعرضوا للخطر أو صادفوا أي موقف غريب أو مشبوه، أو شعروا بعدم الراحة أو الأمان حيال أي موضوع كان.
9. قم بإجراء مراجعة دورية للمواقع التي قام الطلبة/ الأطفال بزيارتها وبشكل مستمر.
10. احرص على إعداد بعض القواعد والإرشادات التي تحكم استخدام الطلبة/ الأطفال للإنترنت، وعلق هذه الإرشادات داخل غرفة الحاسوب ودرب الطلبة على هذه القواعد قبيل البدء بالاستخدام في حالة الاستخدام المدرسي، بحيث تتضمن إرشادات تضمن سلامة الطلبة/ الأطفال .
11. وجه الطلبة/ الأطفال لاستخدام الإنترنت باعتدال من خلال تحديد عدد ساعات الاستخدام المسموح بها.
12. قم بفصل/ إيقاف كاميرا الويب في حال عدم استخدامها أو في حال استخدام جهاز الحاسوب من قبل الأطفال.
13. أنشئ ملفات خاصة للإشارات المرجعية أو المواقع المفضلة لطفلك في متصفح الإنترنت في جهاز الحاسوب.
14. استخدم محركات بحث خاصة بالأطفال مثل ( Yahooligans ) وأن تكون هي الصفحة الرئيسية (Homepage)
15. في حال الولوج للإنترنت باستخدام الهاتف النقال، احرص على تثبيت برمجيات تتحكم بصلاحيات استخدام الانترنت عبر الهاتف لمنع استخدامه من قبل الأطفال.
16. ينصح بتطبيق الطرق التي تمنع ظهور النوافذ المنبثقة (Pop-up Windows) أثناء التصفح.
17. تجنب فتح المواقع الإلكترونية ومواقع التواصل الاجتماعي من خلال الروابط المرسلة عبر البريد الإلكتروني إلا بعد التأكد من العنوان الحقيقي للرابط.

ب. إرشادات توجيهية للأطفال:

1- لا تفصح عن معلوماتك الشخصية (مثل عنوانك، بريدك الالكتروني، اسم والديك، رقم هاتفك النقال، اسم مدرستك ...الخ ) للغرباء على الانترنت.
2- لا تفصح عن كلمة السر الخاصة بحساباتك (مثل حساب البريد الإلكتروني ومواقع التواصل الاجتماعي) على الانترنت.
3- اختر كلمة سر لا يمكن توقعها بسهولة ( يفضل استخدام الرموز والارقام والحروف الكبيرة في حال استخدام اللغة الإنجليزية).
4- لا تقبل طلبات الصداقة على مواقع التواصل الاجتماعي من شخص لا تعرفه.
5- لا تستعرض أي بريد الكتروني من أي شخص أو جهة مجهولة الهوية.
6- أخبر والديك أو أشقائك الأكبر منك سناً في حال أن تعرضت للتهديد من قبل أي شخص أو جهة مجهولة.
7- لا ترسل صورا لنفسك أو أي أحد من أفراد عائلتك على الإنترنت.
8- لا توافق أبدا على مقابلة أي شخص تحت أي ظرف ، وأخبر والديك حالا عن أي شخص يقترح عليك ذلك.

9- لا تكشف عنوان سكنك لاستلام منتج ما بالبريد دون علم الأهل.
10- لا تواصل حديثا يشعرك بعدم الارتياح مع أي شخص على الإنترنت وخاصة في الموضوعات التي تشعرك بالخجل.
11- لا تفتح أي رابط مرسل خلال الدردشة مع أي شخص لا تعرفه، وأنهي الدردشة التي لا تشعر بالراحة حيالها بشكل مباشر.
12- تجنب فتح المواقع الإلكترونية ومواقع التواصل الاجتماعي من خلال الروابط المرسلة عبر البريد الإلكتروني إلا بعد التأكد من العنوان الحقيقي للرابط.

## 4- إرشادات توجيهية للمشتركين:

ويوصى بتعميم هذه الإرشادات على المعنيين بالتنفيذ، فهي توجه استخدام المشتركين وتستهدفهم مباشرة من خلال مزودي خدمات الإنترنت.

إرشادات مزودي خدمة الانترنت لمشتركيهم في المنازل:

1. اعرف جيداً مع من تتعامل قبل الكشف عن أية معلومات خاصة تتعلق بك.
2. تجنب الافصاح عن أية معلومات شخصية في خدمات المحادثة المباشرة (Live Chat) كغرف المحادثة والمنتديات، واستخدم اسما مستعاراً.
3. احرص على عدم ارسال أية معلومات سرية ككلمات السر وأرقام بطاقات الإئتمان عبر البريد الالكتروني، واعلم أن المواقع المعروفة أو الموثوق بها لا تطلب تلك المعلومات عبر البريد الإلكتروني.
4. استخدم كلمات سر صعبة التخمين وتجنب المعلومات العامة كتواريخ الميلاد وأرقام السيارات أو الهواتف وأسماء الأبناء، وحاول المزج بين الأحرف الصغيرة والكبيرة والأرقام والرموز.
5. تجنب المنتديات المشبوهة والتي عادة ما يجتمع فيها مخترقو الأنظمة.
6. تجنب تفعيل خاصية الحفظ التلقائي لكلمات السر على الحواسيب العامة في حال استخدامها وخاصة المتعلقة بالبريد الإلكتروني و/أو مواقع التواصل الاجتماعي.
7. ضرورة تنزيل الأدوات الإضافيّة ( Add-on ) الخاصة بالمتصفحات مثل موزيلا فايرفوكس أو جوجل كروم التي تعمل على ضمان الخصوصيّة وحماية معلومات المستخدم مثل ( Better Privacy ) أو( Privacy Badger ) الخ.
8. تجنب الاحتفاظ بالصور والمعلومات الشخصية على جهاز الحاسوب، واستخدم عوضاً عن ذلك ذاكرة التخزين الخارجية ( External Hard disk Drive ).
9. قم بفصل/ إيقاف كاميرا الويب في حال عدم استخدامها.
10. استخدم كلمات سر للملفات الحساسة.
11. تجنب الرد على رسائل البريد الإلكتروني المشبوهة.
12. تجنب فتح المواقع الإلكترونية ومواقع التواصل الاجتماعي من خلال الروابط المرسلة عبر البريد الإلكتروني إلا بعد التأكد من العنوان الحقيقي للرابط.
13. استخدم برامج تشفير الملفات ( Files encryption ) .

14. في حال ولوجك للإنترنت باستخدام الهاتف النقال، احرص على تثبيت برمجيات تتحكم بصلاحيات استخدام الانترنت على الهاتف لمنع استخدامه من قبل أشخاص آخرين وخاصة الأطفال. واحرص على تعطيل أي خاصية تسمح بتخزين المعلومات بطريقة تلقائية على الحوسبة السحابية ( Cloud Computing ).
15. احرص على تثبيت برمجيات الحماية من الفيروسات والبرامج الخبيثة على جهاز الحاسوب وحدثها بشكل دوري، إلى جانب برامج فلترة للمواقع الضارة.
16. تجنب القيام بأي عمليات شراء أو تحويل مالي على الانترنت أو عبر الهاتف النقال، وعدم قبول أية عروض ترويجية من جهة غير معروفة المصدر لمنتجات على الإنترنت.
17. تجنب تثبيت أشرطة الأدوات (Tool Bars) أثناء تنزيل البرامج المجانية والتي تظهر بالعادة كخيار تلقائي إضافي، فبعض المواقع تثبت أشرطة مخصصة لها وتتسبب بنقل الفيروسات.

ب. إرشادات لمستخدمي مواقع التواصل الاجتماعي تحت عنوان " لسلامة خصوصيتك في برامج التواصل الاجتماعي"

1. عند تسجيل دخولك في مواقع التواصل الاجتماعي أو المدونات أو الحسابات الأخرى، تأكد من عدم قبول خيار حفظ كلمة السر من قبل متصفح الانترنت.
2. لا تفصح عن معلومات حساباتك للآخرين، مثل كلمة السر.
3. ينصح بربط بيانات تسجيلك مع رقم هاتفك للتمكن من استعادة حسابك في حال تم اختراقه.
4. قم بضبط اعدادات الخصوصية التي توفرها مواقع التواصل الاجتماعي بما يضمن توفير مستوى حماية أعلى، وقم بمتابعة تحديثات سياسات الخصوصية الخاصة بالمواقع.
5. اختر كلمة سر لا يمكن توقعها بسهولة ( يفضل استخدام كلمات السر الطويلة التي تحتوى على الرموز والارقام والحروف الكبيرة في حال استخدام اللغة الانجليزية )، ولا تكررها لجميع حساباتك على الإنترنت، ويفضل تغييرها بشكل دوري.
6. عند إنشاءك لمحتوى عام على موقع التواصل الاجتماعي، تأكد من صحة المعلومات وسلامتها، وتذكر بأن رأيك على الإنترنت يعبر عن رأيك الحقيقي، وأنت مسؤول عنه قانونياً.
7. قم بتسجيل خروجك من حساباتك على مواقع التواصل الاجتماعي بعد الانتهاء من الاستخدام.
8. ينصح بضبط إعدادات الخصوصية في حالة مشاركة الصور الشخصية للتحكم بالأشخاص المسموح لهم بالاطلاع عليها.
9. ضبط إعدادات جهاز الهاتف النقال لتحديد الموقع الجغرافي، وإبطالها في حال عدم الحاجة اليها، حيث أن تلك الخاصية تسمح لكثير من التطبيقات تتبع وتحديد الموقع الجغرافي للمستخدم.
10. تجنب فتح المواقع الإلكترونية ومواقع التواصل الاجتماعي من خلال الروابط المرسلة عبر البريد الإلكتروني إلا بعد التأكد من العنوان الحقيقي للرابط.

جـ. إرشادات للمتعاملين بالتجارة الإلكترونية:

عند القيام بعملية الشراء الإلكتروني عبر مواقع التجارة الإلكترونية، تأكد من الآتي:

1. تسوق عبر المواقع الإلكترونيّة والتجارية المتداولة والمعروفة بمصداقيتها محلياً و/أوعالمياً.
2. تأكد من أن الموقع الذي يقدم خدمات التجارة الإلكترونية يمتلك عنواناً فعلياً وأرقام اتصال حقيقيين قبل التعامل معه.
3. اطلع على سياسة الموقع الإلكتروني وشروط تقديم الخدمة قبل إدخال رقم بطاقة الائتمان/ الدفع أو إجراء عمليّة الدفع الإلكتروني، فهي توضح المعلومات الشخصية التي يجمعها الموقع وكيفية استخدامها، وما إذا كان يتم مشاركتها مع جهات أخرى.
4. لا تقم بإعطاء معلومات أكثر من المطلوب عند ملئ النماذج الالكترونية. واحرص على عدم تخزين معلومات بطاقات الائتمان على جهاز الحاسوب أو المواقع التي تتعامل معها للدفع الإلكتروني.
5. قم بطباعة كشف يتضمن المواد التي قمت بشرائها وأعدادها ورقمها وتاريخها لغايات متابعة استلامها.
6. عند الشروع في علمية الدفع بواسطة بطاقة الإئتمان، تأكد بأن يكون الموقع الإلكتروني مسبوقاً ب ( https ) وليس ( http ) لضمان حماية أخذ معلومات البطاقة من قبل المخترقين واستخدامها لاحقاً بطريقة غير مشروعة، وتأكد من ظهور صورة القفل ( padlock ) في أسفل الصفحة أو نافذة العنوان.
7. اضغط على القفل لتظهر لك معلومات شهادة التوثيق الإلكتروني، وتأكد من أن الشهادة منحت لنفس عنوان الموقع.
8. تجنب الشراء عن طريق المواقع الإلكترونيّة غير المعروفة و التي ترسل العروض الترويجية من جهات غير معروفة المصدر عن طريق البريد الإلكتروني.
9. يمكنك الاستعانة بميزة الدفع عن طريق طرف ثالث مثل ( PayPal ).
10. استخدم بطاقات الدفع الإلكترونيّة التي يمكنك التحكم بسقف شحنها والتي تشحن فقط عند الحاجة.