الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1212

(2017/03)

السلسلة X: شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

اعتبارات التصميم لتحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة

التوصية ITU-T X.1212

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية	X.1349-X.1340
أمن إنترنت الأشياء	X.1369-X.1360
أمن نظام النقل الذكي	X.1379-X.1370
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1212

اعتبارات التصميم لتحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة

ملخص

تُستخدم في شتى أنواع الهجمات نسخ لمحتوى متأتٍ من موفِّري خدمات يستحقون الثقة، ما يخدع المستعملين النهائيين بجعلهم يعتقدون أنه يستحق الثقة على الرغم من أنه لا يستحقها.

وتبيِّن التوصية ITU-T X.1212 اعتبارات التصميم لتحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة. وتُعرض في التذييلين التقنيات الرئيسية المستخدَمة لقياس تصوُّر المستعملين النهائيين لهذه المؤشرات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1212	2017-03-30	17	11.1002/1000/13195

مصطلحات أساسية

تصوُّر المستعملين النهائيين، التصيُّد الإلكتروني الاحتيالي، مؤشرات استحقاق الثقة.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2018

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 المصطلحات المعرَّفة في وثائق أخرى 1
2.3 المصطلحات المعرَّفة في هذه التوصية 2
4 المختصرات والأسماء المختصرة 2
5 الاصطلاحات 2
6 تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة 2
7 تقنيات تحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة 2
1.7 العناصر المرئية 2
2.7 عناصر النصوص السردية 3
3.7 عمليات الانتقال من تصميم إلى آخر من تصاميم التجهيزات المحيطية 4
4.7 أسلوب التدريب 4
5.7 إمكانية النفاذ 4
6.7 الأطفال 5
التذييل I – الاعتبارات المتعلقة بتحليل المهام المعرفية في مجال الأمن السيبراني 6
1.I الاعتبارات المتعلقة بتحليل المهام المعرفية في مجال الأمن السيبراني 6
2.I المفاهيم الثلاثة التي تتيح تحقيق أمن المعلومات 6
3.I الطرائق الممكن اتباعها في القياس 6
التذييل II – اعتبارات حماية المستعملين النهائيين في تحليل المهام المعرفية 7
1.II تقدير معارف ومهارات المستعملين 7
بيبليوغرافيا 11

اعتبارات التصميم لتحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة

1 مجال التطبيق

تُستخدم في طائفة واسعة من الهجمات نسخ لمحتوى متأتٍ من موفِّري خدمات يستحقون الثقة، ما يخدع المستعملين النهائيين بجعلهم يعتقدون أنه يستحق الثقة على الرغم من أنه لا يستحقها. وتبيِّن هذه التوصية اعتبارات التصميم لتحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة. وتُعرض في التذييلين التقنيات الرئيسية المستخدَمة لقياس تصوُّر المستعملين النهائيين لهذه المؤشرات.

2 المراجع

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تُستخدم في هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الإعاقة (disability) [b-ITU-T F.790]: تُعرّف "الإعاقة" بأنها حالة يكون فيها استعمال تجهيزات وخدمات الاتصالات مقيَّداً. ويُنظر أساساً إلى "الإعاقة" على أنها ناجمة عن عجز وظيفي مؤقت أو دائم بسبب مرض أو حادث أو شيخوخة وما إلى ذلك. وبوجه أعم، تنطوي "الإعاقة" على حالة يتعذر فيها الاستعمال الكامل لتجهيزات وخدمات الاتصالات بسبب البيئة المادية و/أو الاجتماعية (كالمهاتفة في بيئة تتسم بالضوضاء).

2.1.3 القياس (measurement) [b-ENISA]: فعل أو عملية القياس، حيث تحدَّد قيمة متغير كمي بالمقارنة مع وحدة قياس (معيارية).

3.1.3 المبيِّن (metric) [b-ENISA]: نظام قياسات متصلة يمكِّن من التحديد الكمي لخاصيةٍ ما لنظام أو مكوّن أو عملية. ويتكوَّن المبيِّن من مقياسين أو أكثر.

4.1.3 المعلومات المحدِّدة لهوية شخص (personally identifiable information) (PII) [b-ITU-T X.1252]: أي معلومات أ) تعرِّف الشخص الذي تخصه أو يمكن استعمالها في التعرف عليه أو الاتصال به أو تحديد موقعه؛ ب) أو يمكن من خلالها الحصول على معلومات التعرف على شخص أو بيانات اتصاله؛ أو ج) تكون مرتبطة أو يمكن ربطها بشخص طبيعي بطريقة مباشرة أو غير مباشرة.

5.1.3 التصيّد الإلكتروني الاحتيالي (phishing) [b-ITU X.1254]: احتيال ينخدع به مستعمل البريد الإلكتروني أو الموقع الشبكي للكشف عن معلومات شخصية أو سرية بحيث يستطيع المحتال استخدامها بصورة غير شرعية.

6.1.3 إمكانية النفاذ إلى الاتصالات (telecommunications accessibility) [b-ITU-T F.790]: يُقصد بالمصطلح في مجال الاتصالات إمكانية استعمال منتج أو خدمة أو بيئة أو مرفق من جانب أوسع طائفة ممكنة من المستعملين، وخصوصاً المستعملون ذوو الإعاقة.

7.1.3 الشخص ذو الإعاقة (person with disabilities) [b-ITU-T F.791]: الطريقة اللائقة للإشارة إلى شخص يعاني من إعاقة [b-UNCRPD].

2.3 المصطلحات المعرَّفة في هذه التوصية

يعرَّف في هذه التوصية المصطلح التالي:

1.2.3 مؤشرات استحقاق الثقة (trustworthiness indicators): هي الرموز التي يعرضها وكيل للمستعملين على شبكة الويب فيستعان بها لتنوير المستعملين النهائيين بشأن استحقاق الموقع الشبكي المعني للثقة.

4 المختصرات والأسماء المختصرة

DKIM البريد المعرَّف بمفاتيح الميادين *(DomainKeys Identified Mail)*

DOM نموذج موضوع الوثيقة *(Document Object Model)*

FNE خشية التقييم السلبي *(Fear of Negative Evaluation)*

SSL طبقة التوصيل الآمنة *(Secure Socket Layer)*

URL محدِّد موقع الموارد الموحَّد *(Uniform Resource Locator)*

5 الاصطلاحات

لا توجد.

6 تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة

إن بروتوكولات تبادل المعلومات بشأن الأمن السيبراني، كما تعرَّف في التوصية [b-ITU-T X.1500]، يمكن أن تأتي بمعلومات مفيدة فيما يخص القرارات المتعلقة باستحقاق الثقة في إطار كل ما قد يحدث من تفاعلات في الفضاء السيبراني. ومن هذه المعلومات، على سبيل الذكر لا الحصر، معلومات عن شهادات الصلاحية الممتدة [b-CAB-Baseline] ودرجة التيقن من الهويات [b-ITU-T X.1254]، وتواقيع البريد الإلكتروني للبريد المعرَّف بمفاتيح الميادين (DKIM) [b-IETF RFC 6376]، والإشارة إلى مواقع التصيد الإلكتروني الاحتيالي [b-IETF RFC 5901].

بيد أن المستعملين النهائيين غالباً ما يتجاهلون هذه المؤشرات المتعلقة باستحقاق الثقة أو لا يعيرونها الاهتمام الكافي، بحسب ما تبيِّنه دراسات سابقة أجريت استناداً إلى إحصاءات ديمغرافية شتى (ترد التفاصيل ذات الصلة في التذييل II). ولذا يتعين تحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة.

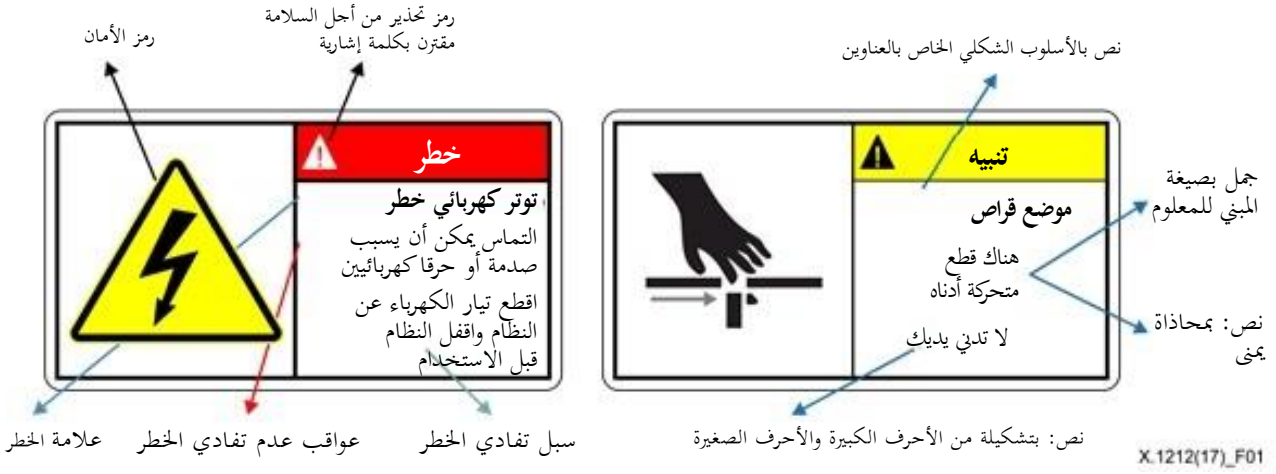
7 تقنيات تحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة

تُقدَّم في إطار هذا القسم عدة تقنيات لتحسين تصوُّر المستعملين النهائيين لمؤشرات استحقاق الثقة. ويمكن استعمال هذه التقنيات منفردةً أو مجتمعةً، كما يراد أو كما تقتضيه الحال، لعرض مؤشرات استحقاق الثقة على نحو يزيد من إمكان التعرف عليها.

1.7 العناصر المرئية

يجب أن ينظر واضعو مؤشرات استحقاق الثقة في الاستعانة بعناصر مرئية مقيَّسة. فقد بيَّنت دراسات سابقة أن مؤشرات استحقاق الثقة القائمة على التشفير الرمزي، كما في محدِّدات مواقع الموارد الموحَّدة (URL)، يصعب على المستجدين من المستعملين النهائيين استخدامها وغالباً ما تُتجاهل [b-Miyamoto]. ولذا يوصى بالأخذ بعناصر مرئية، مثل الأيقونات التي تدل على استحقاق الثقة. ويمكن للقائمين على التنفيذ النظرُ في الاستعانة ببضعة عناصر مرئية مقيَّسة، كما في حالة إشارات السير على الطرقات، لتقليل ما يلزم من جهد وتركيز إضافيين ومن تدريب إضافي.

وبحسب إشارات وعلامات أمان المنتجات [b-ANSI-Z535.4]، تُقلَّص درجات المخاطر باستخدام كلمات إشارية (مثل "خطر" و"إنذار") مقترنة بألوان (الأحمر، والبرتقالي، والأصفر).



الشكل 1 – إشارات وعلامات أمان المنتجات (ANSI Z535.4)

يقترن بلاغ "الخطر" (DANGER) بمثلثٍ أبيضَ وعلامةِ تعجُّبٍ حمراءَ وخلفيةٍ حمراء. ويقترن بلاغ "الإنذار" (WARNING) بمثلثٍ أسودَ وعلامةِ تعجُّب برتقالية. ويقترن بلاغ "التحذير" (CAUTION) بمثلثٍ أسود وعلامةِ تعجُّبٍ صفراء.

ويضاف إلى ذلك أن واضعي مؤشرات استحقاق الثقة ينبغي أن يستعملوا أنساق ألوان قياسية لتمثيل درجات استحقاق الثقة. وفي سياق أثر الألوان من الناحية النفسية يستعان باللون الأحمر لاسترعاء الانتباه. فاللون الأحمر يقابل طول الموجة الأكبر في طيف الضوء المرئي، ويتميَّز بخاصةِ الظهور وكأنه أقرب مما هو بالفعل. ولذا فإن الأحمر يخطف انتباه المستعملين ويُستعان به في إشارات المرور. أما الأصفر فإن طول الموجة المقابل له كبير نسبياً وهو حفَّاز في الأساس، ويمكن أن يسترعي انتباه المستعملين. ويتوسط اللون الأخضر طيف الألوان؛ فهو يقابل طول الموجة المتوسط للضوء المرئي. وينزع اللون الأخضر أيضاً إلى كونه يُرى رؤيةً لا تستلزم أي تضبيط، ما يجعله يُستعمل بمثابة إشارةٍ مريحةٍ أو باعثةٍ على الاسترخاء. أما اللون الأزرق فإنه يهدئ البال ويساعد على التركيز.

ويمكن لواضعي مؤشرات استحقاق الثقة أن يستعينوا بمفهوم "الدماغ الاجتماعي" الذي يشجِّع على التصرف التعاوني الرامي إلى خدمة المجتمع. فقد خُلص في دراسات سابقة إلى أن الناس يتصرفون على نحو يتسم بمزيد من الوعي الاجتماعي عندما يكونون على مقربة من صور لعيون ناظرة [b-Rigdon] و[b-Senju]. بيد أنه يُنظر إلى ذلك نظرةَ تشكُّكٍ، يقول أصحابها بأنه ليس لصورة العيون الناظرة أثر يذكر على السلوك [b-Felt2014].

2.7 عناصر النصوص السردية

بيَّنت دراسات سابقة أن بعض مجموعات المستعملين يتخذون قراراتهم بشأن استحقاق الثقة استناداً إلى النصوص السردية، لا إلى أسماء الميادين، ولا إلى أنواع البروتوكولات، ولا إلى محدِّدات مواقع الموارد الموحَّدة (URL) [b-Felst2014] و[b-Felt2015]. فيوصى بتجهيز برمجيات المستعملين النهائيين بما يمكِّن من تحويل المعلومات الرمزية إلى عناصر نصوص سردية لا تُستعمل فيها المختصرات. كما يمكن أن يكون ذلك مفيداً للمستعملين المعوقين بصرياً، إذا اقترن بنظم تحوِّل النص إلى كلام.

فلجذب انتباه المستعملين قد يتعين عند إعداد بلاغات الإنذار في البرمجيات الخاصة بالمستعملين النهائيين النظر في عدة معايير للتصميم على النحو التالي:

1 ينبغي لواضعي مؤشرات استحقاق الثقة أن يتفادوا استخدام المصطلحات التقنية. فينبغي أن يستعاض في بلاغ الإنذار عن المصطلحات التقنية بجمل أو عبارات يستطيع المستعملون فهمها؛ إذ إنهم سيتجاهلون البلاغ إذا لم يعلموا كيفية التحرك السليم بناءً عليه.

2 ينبغي لواضعي مؤشرات استحقاق الثقة النظر في صوغ بلاغات مقتضبة. فطول النصوص سيعطي مؤشراً عن لزوم جهود كثيرة لقراءتها، ما قد يثني المستعملين عن قراءتها. كما ينبغي أن يُستبعد من البلاغ كل نص زائد لكي يغدو البلاغ وجيزاً ودقيقاً في آن واحد. وينبغي التنويه إلى أن ثمة علاقة توازن بين الإيجاز والدقة قائمة على اعتماد حل وسط؛ فلا يمكن شرح جميع جوانب نموذج التهديد في فقرة قصيرة وحيدة. ولذا يمكن أن تُستخدم في بلاغات الإنذار العناصر المرئية والعناصر النصية معاً. ولحساب مدى الإيجاز الممكن الأخذ به يمكن لواضعي المؤشرات أن يطبقوا دليلاً للقدرة على القراءة، يقيس القدرة على القراءة بتقدير عدد سنوات التعليم التي يتعين أن يكون الشخص المعني قد تابعها لكي يفهم نصاً مكتوباً.

3 ينبغي لواضعي مؤشرات استحقاق الثقة أن يبيّنوا الخطر الذي وقع أو الوشيك الوقوع. فينبغي أن يُبيَّن في بلاغات الإنذار الخطر المتَّخَذ أساساً لإصدارها، لأن المستعملين يُحتمل أن يحيطوا بالبلاغ ويمتثلوا له إذا كان يصف المخاطر وصفاً صريحاً لا لبس فيه. كما ينبغي أن يتضمن البلاغ تعليمات عن سبل تفادي الخطر، إذا لم تكن التعليمات المعنية واضحة في وصف الخطر.

3.7 عمليات الانتقال من تصميم إلى آخر من تصاميم التجهيزات المحيطية

يمكن لواضعي مؤشرات استحقاق الثقة أن يختبروا واجهتها البينية فيما يخص عمليات الانتقال من تصميم إلى آخر من تصاميم التجهيزات المحيطية. فيمكن أن يكون للانتقال الفجائي في مرأى التجهيزات المحيطية مفعول يشير إلى خطر محتمل. ولذا يوصى بالاستعانة بهذه التقنية بالانتقال من تصميم إلى آخر من تصاميم هذه التجهيزات (التي دُرج على تسميتها "شارات" (themes) أو "هيئات" (skins))، كلما واجه المستعملون النهائيون مواقع شبكية أو بلاغات بريد إلكتروني تنطوي على خطر عال.

4.7 أسلوب التدريب

يمكن لواضعي مؤشرات استحقاق الثقة أن يعدّوا أساليب تدريبية. فتصور المستعمل النهائي للأخطار سيكون غير دقيق في أحسن الأحوال إذا كان لا يتعرض إلى الأخطار المعنية إلا نادراً جداً. ولذا يوصى بتجهيز برمجيات المستعملين النهائيين بأسلوب تدريبي، يمكن به محاكاة أحداث تنطوي على أخطار على نحو مصطنع يُدرَّب به المستعملون النهائيون على تصوُّر الأخطار بدقة. كما يمكن إضفاء طابع تحفيزي على هذا التدريب بجعله يشتمل على التباري.

5.7 إمكانية النفاذ

ينبغي لواضعي مؤشرات استحقاق الثقة أن يصمِّموا واجهتها البينية واضعين باعتبارهم إمكانية النفاذ. إن الإبصار يشير إلى القدرة على تمييز شكل الحافزات البصرية، وقدّها، وهيئتها، ولونها. فيمكن أن يواجه الأشخاص المعوقو البصر مصاعب في تبيُّن مؤشرات استحقاق الثقة. فبسبب آثار عمى الألون الناجم عن عدم تمييز اللون الأحمر (protanopia) وعمى الألوان الناجم عن عدم تمييز اللون الأخضر (deuteranopia) يمكن أن يواجه بعض المستعملين النهائيين مشكلات في تمييز الألوان، مثل تمييز اللون الأحمر عن اللون الأخضر.

لقد وضعت المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية وثيقة المبادئ التوجيهية الخاصة بإمكانية النفاذ [b-ISO/IEC-40500] للأشخاص ذوي الإعاقة، لكن هذه الوثيقة لا تتناول مباشرة مؤشرات استحقاق الثقة التي تظهر في شريط العنوان. ويُعرَّف في وثيقة المتطلبات الأساسية لمنتدى هيئات تصديق برمجيات التصفح [b-CAB-Baseline] المعيار الخاص بالشهادات وسلطات إصدارها، لكن لا تحدَّد فيها الكيفية التي تقدِّم بها برمجيات التصفح الشهادات للمستعملين.

وتضمن القائمة المرجعية لإمكانية النفاذ إلى الاتصالات [b-ITU-T-FSTP-TACL] أن يتاح لشتى المستعملين، بمن فيهم الأشخاص ذوو الإعاقات، أن يستخدموا الخدمات والوظائف المحدَّدة. فإذا أُريد تحقيق إمكانية أفضل لنفاذ المعوقين بصرياً أو المكفوفين، فينبغي للواجهة المعنية أن توفِّر للمستعمل عرضاً للوسائط، وأن تتسنى مراقبتها في شتى أساليب وأنواع التدابير التحكمية. وبالنسبة للأشخاص ذوي الإعاقات الإدراكية، ينبغي إبراز نقاط مهمة للفت انتباههم فضلاً عن استعمال وسائط متممة، كالأيقونات والوسائط الفيديوية والسمعية.

إن تطبيقات قراءة ما يظهر على الشاشة يمكن أن تجد مؤشرات استحقاق الثقة التي تظهر في المواقع الشبكية. ويمكن أن تتيح هذه التطبيقات معلومات تتعلق بالأمن، مثل شريط العنوان الأخضر لشهادة الصلاحية الممتدة (EV-SSL)، وقراءة المعلومات

بخدمات تحويل النصوص إلى كلام. كما يمكن أن تلخِّص هذه التطبيقات المعلومات المتأتية عن شجرة "نموذج موضوع الوثيقة" (DOM) ضمن برنامج التصفح.

6.7 الأطفال

فيما يخص الأطفال على شبكة الإنترنت، يقوم أحد الوالدين عادة بالتحقق من خلال الاستماع إلى مجريات أو أنشطة اتصالات أطفالهم عبر الإنترنت أو يمتلك المعلومات اللازمة لتقييد النفاذ بنسق قريب المنال. وقد لا يكون هذا السبيل "الواقي" متاحاً لأحد الوالدين ذي الإعاقة. ويندرج هذا الدور بعينه، كما هو محدد، بين مجالين – حماية الطفل على شبكة الإنترنت وإمكانية نفاذ شخص بالغ/أحد الوالدين ذي الإعاقة الذي يتولى مسؤولية تنشئة أطفال أصحاء وكذلك أطفال معوقين.

التذييل I

الاعتبارات المتعلقة بتحليل المهام المعرفية في مجال الأمن السيبراني

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I الاعتبارات المتعلقة بتحليل المهام المعرفية في مجال الأمن السيبراني

إن تحليل المهام المعرفية لأغراض الأمن السيبراني يمكن أن يشتمل على قياس العناصر السلوكية وعلى تحليل التفاعلات مما يؤدي في نهاية المطاف إلى تداخل العمليات الذهنية الباطنية. وتُدرس في إطار هذه التوصية ثلاثة مفاهيم لأمن المعلومات، هي السرّية والنزاهة والتيسُّر، باعتبارها متطلبات تحليل المهام المعرفية في مجال الأمن السيبراني.

2.I المفاهيم الثلاثة التي تتيح تحقيق أمن المعلومات

السرّية

يمكن أن تتضمن البيانات المَقِيسة معلومات شخصية، تكون من حيث الأساس حساسة فيما يتعلق بالخصوصية. وعليه فإن استعمال هذه البيانات يتعين أن يجري بعناية، مشفوعاً باتفاق مع المستعملين النهائيين. ويجب أن يخضع تبادل هذه المعلومات لمراقبة صارمة.

النزاهة

يمكن أن يستعان في طرائق القياس بالمعلومات المجمعة بصرف النظر عن خشية التقييم السلبي (FNE). والحال أن الملاحظات غالباً ما تتأثر بخشية التقييم السلبي، حيث يعمد بعض الناس إلى التستر على أخطائهم البشرية، لأن كشف الأخطاء غالباً ما يضر بالصورة المتكوّنة لديهم عن ذاتهم وبسمعتهم المهنية.

التيسُّر

ينبغي أن تُتَّبَع في المعاينات الطريقةُ التي يسهُل على الناس تطبيقها. ففي سياق اتّقاء التصيد الإلكتروني الاحتيالي ينبغي أن تكون الطرائق المعنية متاحة عندما يتصفح المستعملون المعلومات المقدَّمة. وتفضَّل في ذلك الأجهزة التي تعمل دون حاجة إلى تماس. كما يجب أن لا يحمل المستعملون مغروسات أو أجهزة أخرى يمكن أن تؤذيهم بأي شكل من الأشكال.

3.I الطرائق الممكن اتباعها في القياس

أثبتت البحوث في مجال علم النفس التجريبي وجود ارتباط وثيق بين حركات العينين والاضطرابات الذهنية [b-Crawford] و[b-Noris]. وقد صنَّف ليغ وآخرون [b-Leigh] حركات العينين فأدرجوها في أربع فئات، هي اللمحات والتحديقات وحركات التتبع المتواصل بالبصر والمنعكسات الدهليزية–البصرية. وعلى العموم تتغير حركة العين اللمحية بتغير ما يراه الشخص المعني. وقد بيَّن إروين وآخرون في سياق النموذج الذهني أن الدوران الذهني يلتغي خلال الحركات المعنية [b-Irwin]، وبيَّن توكودا [b-Tokuda] أن عبء العمل الذهني الذي يمثِّل مؤشراً إلى مدى انشغال الشخص ذهنياً/معرفياً، يمكن أن يقدَّر انطلاقاً من الحركات اللمحية الطارئة.

ويمكن أيضاً الاستعانة بتأكيد درجة حرارة الجسم السطحية المَقِيسة على البشرة لجمع معلومات بمثابة مقياس فسيولوجي للحالة الذهنية [b-Or] و[b-Wang] و[b-Volskamp]. ويذهب جينو وآخرون [b-Genno] إلى أن تجاربهم أثبتت وجود تغيرات في درجة الحرارة في منطقة الأنف عندما يشعر الأشخاص المعنيون بأحاسيس من قبيل الإجهاد والإرهاق. ثم إن البيانات المتعلقة بدرجة الحرارة، إذ تقترن بغير ذلك من طرائق القياس، تهيئ وسيلة مرنة ذات درجة عالية من الأتمتة لتقييم عبء العمل تقييماً موضوعياً [b-Or].

وإلى جانب هذه الحلول غالباً ما تُجمع المعلومات بالاستناد إلى نشاط الدماغ وناقلية البشرة وقياس نبض القلب وضغط الدم، لكن الاستعانة بهذه البيانات تنزع إلى تطلُّب تدخل تطفلي لدى المستعملين. ولئن كان من المفيد فيما يخص التيسُّرَ التعرفُ على تعابير الوجه وحركاته فإنه يسهُل تأثُّر هذه التعابير والحركات بخشية التقييم السلبي.

التذييل II

اعتبارات حماية المستعملين النهائيين في تحليل المهام المعرفية

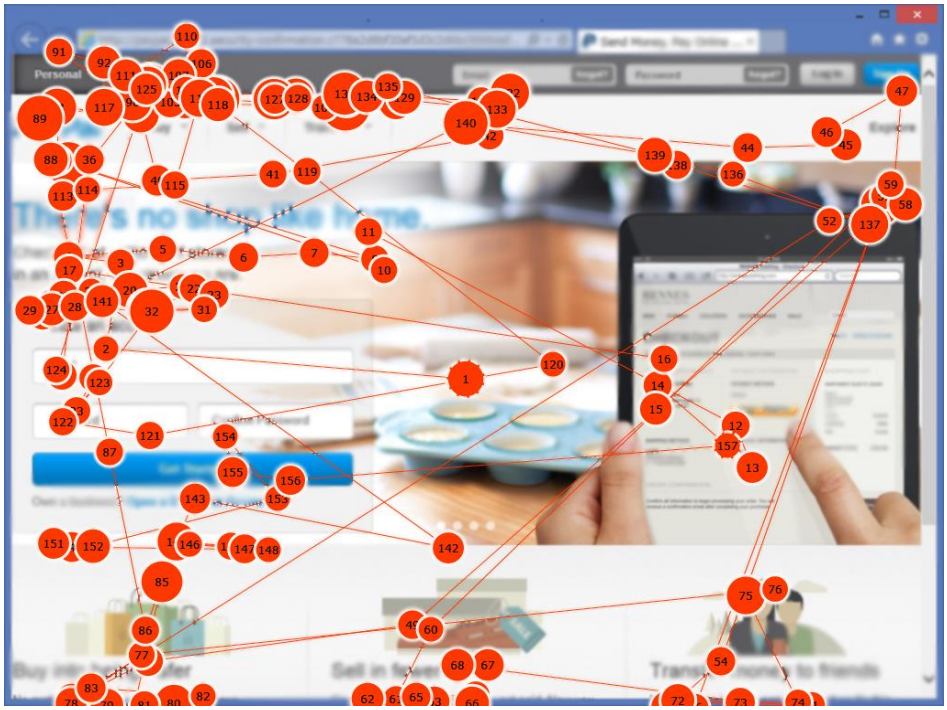
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II تقدير معارف ومهارات المستعملين

توضح دراسة سابقة أنه يمكن تصنيف المستعملين النهائيين في فئتين هما فئة الخبراء وفئة المستجدين [b-Miyamoto]. فالخبراء يقيِّمون مؤشِّر محدِّد موقع الموارد الموحد (URL) و/أو طبقة التوصيل الآمنة (SSL) لبرنامج التصفح بدلاً من تقييم محتويات صفحات المواقع الشبكية للبت في شأن مصداقية المواقع المعنية. أما المستجدون فهم شديدو التأثر بالإشارات التي يتلقونها من محتويات المواقع الشبكية. والحال أن طبيعة التصيد الإلكتروني الاحتيالي تجعل محتويات المواقع الشبكية الاحتيالية مماثلة لمحتويات الموقع المشروع، ما يفضي بالمستجدين إلى الوقوع في شَرَك التصيد الإلكتروني الاحتيالي.

إن هذه الخصائص المميِّزة للمستعملين النهائيين تفيد في تضبيط نظام الوقاية من التصيد الإلكتروني الاحتيالي فيما يخص كلاً منهم. وثمة حل يمكن الأخذ به يتمثل في تهيئة نسق كشف التصيد الإلكتروني الاحتيالي بحيث تكون الحالات السلبية الزائفة أقل فيما يخص المستجدين والحالات الإيجابية الزائفة أقل فيما يخص الخبراء. وبوجه عام تعترض نُظُمَ الوقاية من التصيد الإلكتروني الاحتيالي مشكلةٌ في دقة الكشف، لأن ثمة علاقة توازن قائمة على حل وسط بين عدد الحالات الإيجابية الزائفة (أي حالات اعتبار مواقع مشروعة مواقع للتصيد الإلكتروني الاحتيالي) وعدد الحالات السلبية الزائفة (أي حالات اعتبار مواقع للتصيد الإلكتروني الاحتيالي مواقع مشروعة). ومن شأن عدد الحالات الإيجابية الزائفة أن يزداد إذا رُكِّز في النظم على تقليص عدد الحالات السلبية الزائفة (اعتبار مواقع للتصيد الإلكتروني الاحتيالي مواقع مشروعة). أما تقليص الخطأين كليهما فيُعَدّ أمراً صعباً. وعلى الرغم من ذلك يجب أن يحمي النظام المستجدين، الذين غالباً ما يفشلون في اتخاذ القرار الصحيح.

وييسِّر استعمال جهاز لتتبع حركة العينين تمييز المستجدين من بين مستعملي المواقع الشبكية. فالشكل 1.II يبيِّن حركة عينَي مستعمل مستجد بينما يبيِّن الشكل 2.II حركة عينَي مستعمل خبير، في موقع شبكي احتيالي. وتشير الدوائر إلى حالات التحديق، بينما تشير الأرقام ضمن الدوائر إلى ترتيب هذه الحالات. ففي حالة موقع التصيد الإلكتروني الاحتيالي، نظر المستجد إلى محتوى الموقع الشبكي المعني لكنه تجاهل شريط عنوان برنامج التصفح عندما قيَّم المصداقية، كما يبيَّن في الشكل 1.II.

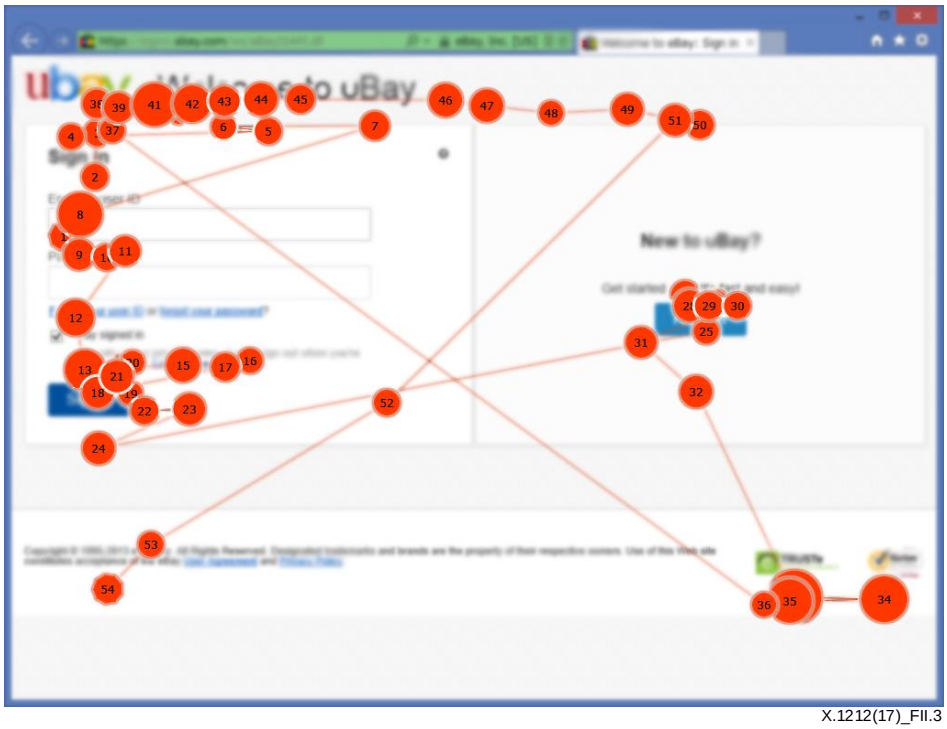


X.1212(17)_FII.1

الشكل 1.II – مستعمل مستجد على موقع شبكي احتيالي

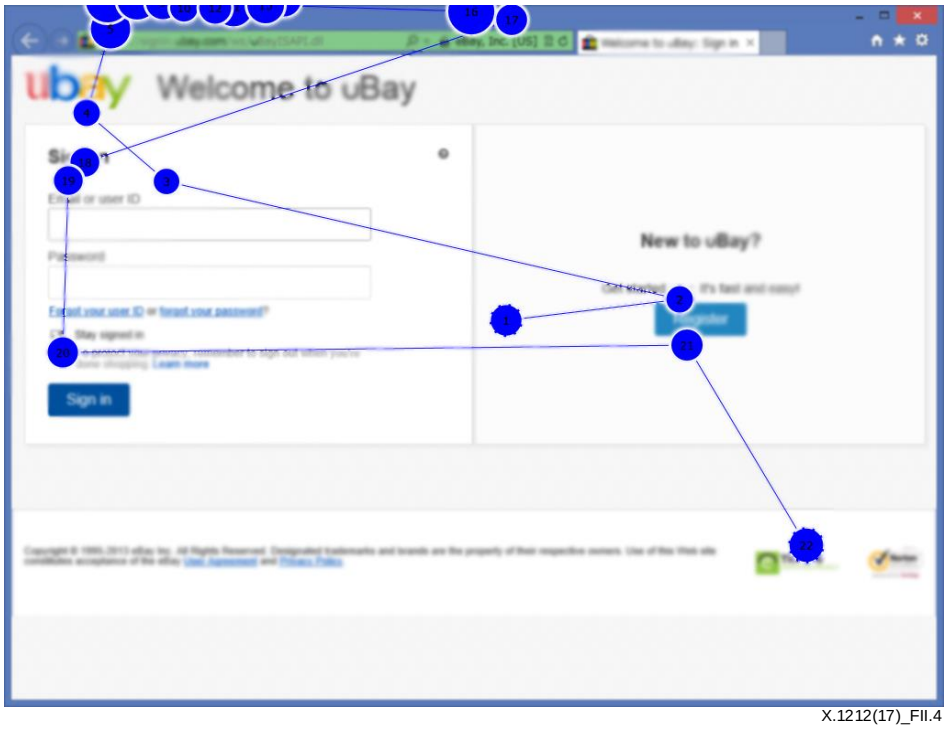
X.1212(17)_FII.2

الشكل 2.II – مستعمل خبير على موقع شبكي احتيالي



X.1212(17)_FII.3

الشكل 3.II – مستعمل مستجد على موقع شبكي مشروع



X.1212(17)_FII.4

الشكل 4.II – مستعمل خبير على موقع شبكي مشروع

في حالة الموقع الشبكي المشروع أيضاً لم يُعِر المستعمل المستجد الانتباه إلا لمحتوى الموقع كما يظهر في الشكل 3.II. أما المستعمل الخبير فينزع خلافاً لذلك إلى تقييم مؤشر محدِّد موقع الموارد الموحد (URL) و/أو طبقة التوصيل الآمنة (SSL) لبرنامج التصفح لا إلى محتويات صفحته لكي يحكم على مصداقية الموقع المعني كما يظهر في الشكل 4.II. وتشير معايَنات السلوك هذه إلى أن المستعملين الخبراء ينزعون إلى النظر إلى شريط العنوان حيث يُعْرَض مؤشر محدِّد موقع الموارد الموحد (URL) و/أو طبقة التوصيل الآمنة (SSL) لبرنامج التصفح عند بدء عملية التصفح. أما المستجدون فليسوا على علم بذلك لافتقارهم إلى المعرفة فيما يتعلق بمؤشر محدد موقع الموارد الموحد (URL) وطبقة التوصيل الآمنة (SSL).

بيبليوغرافيا

[b-ITU-T F.790] Recommendation ITU-T F.790 (2007), *Telecommunications accessibility guidelines for older persons and persons with disabilities.* <https://www.itu.int/rec/T-REC-F.790>

[b-ITU-T F.791] Recommendation ITU-T F.791 (2015), *Accessibility terms and definitions*. <https://www.itu.int/rec/T-REC-F.791>

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.* <https://www.itu.int/rec/T-REC-X.1252>

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.* <https://www.itu.int/rec/T-REC-X.1254>

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange.* <https://www.itu.int/rec/T-REC-X.1500>

[b-ITU-T-FSTP-TACL] ITU-T FSTP-TACL (2006), *Telecommunications Accessibility Checklist.* <https://www.itu.int/publ/T-TUT-FSTP-2006-TACL>

[b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*. <http://datatracker.ietf.org/doc/rfc5901/>

[b-IETF RFC 6376] IETF RFC 6376 (2011), *DomainKeys Identified Mail (DKIM) Signatures.* <http://datatracker.ietf.org/doc/rfc6376/>

[b-ISO/IEC 40500] ISO/IEC 40500:2012, *Information Technology – W3C Web Content Accessibility Guidelines (WCAG) 2.0.*

[b-ANSI-Z535.4] ANSI (2011), Product Safety Signs and Labels.

[b-CAB-Baseline] CA/Browser Forum (2011), *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* Version 1.0. <http://www.cabforum.org/Baseline_Requirements_V1.pdf>

[b-Crawford] Crawford, T.J., Higham, S., Renvoize, T., Patel, J., Dale, M., Suriya, A., Tetley S. (2005), *Inhibitory control of saccadic eye movements and cognitive impairment in Alzheimer's disease*, Biological Psychiatry, vol. 9, No. 57.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report.*

[b-Felt2014] Felt, A.P., Reeder, R.W., Almuhimedi. H., Consolvo, S. (2014), *Experimenting At Scale With Google Chrome's SSL Warnings*, in Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems.

[b-Felt2015] Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., Grimes, J. (2015), *Improving SSL Warnings: Comprehension and Adherence*, in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.

[b-Genno] Genno, H., Ishikawa, K., Kanbara, O., Kikumoto, M., Fujiwara, Y., Suzuki, R., Osumi, M. (1997), *Using facial skin temperature to objectively evaluate sensations*, International Journal of Industrial Ergonomics, vol. 19.

[b-Irwin] Irwin, D.E., Brockmole, J.R. (2000), *Mental rotation is suppressed during saccadic eye movements*, Psychonomic Bulletin and Review, vol. 7, no. 4.

[b-Leigh] Leigh, R.J., Zee, D.S. (1991), *The Neurology of Eye Movements*, 4th ed. Oxford University Press.

[b-Miyamoto] Miyamoto, D., Iimura, T., Tazaki, H., Blanc, G., Kadobayashi, Y. (2014), *EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits*, in Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security.

[b-Noris] Noris, B. Benmachiche, K., Meynet, J., Thiran, J.P., Billard, A. (2007), *Analysis of Head-Mounted Wireless Camera Videos for Early Diagnosis of Autism*, Advances in Soft Computing, vol. 45.

[b-Or] Or, C.K.L., Duffy, V.G. (2007), *Development of a facial skin temperature-based methodology for nonintrusive mental workload measurement*, Occupational Ergonomics, vol. 7.

[b-Rigdon] Rigdon, M., Ishii, K., Watabe, M., and Kitayama, S. (2009), *Minimal social cues in the dictator game*, Journal of Economic Psychology vol. 30, iss. 3.

[b-Senju] Senju, A., Johnson, M.H. (2009), *The eye contact effect: mechanisms and development*, Trend in Cognitive Science.

[b-Tokuda] Tokuda, S., Obinata G., Palmer, E., Chaparro, A. (2011), *Estimation of mental workload using saccadic eye movements in a free-viewing task*, in Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society.

[b-UNCRPD] United Nations, Conventions on the Rights of Persons with Disabilities (2006).

[b-Volskamp] Voskamp, J., Urban, B. (2009), *Measuring Cognitive Workload in Non-military Scenarios Criteria for Sensor Technologies*, in Proceedings of the 5th International Conference on Foundations of Augmented Cognition.

[b-Wang] Wang, L., Duffy V.G., Du, Y. (2007), *A composite measure for the evaluation of mental workload*, in Proceedings of the 1st International Conference on Digital Human Modelling.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2018