Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1212

(03/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Cybersécurité

Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité

Recommandation UIT-T X.1212

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	**X.1200–X.1229**
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1379
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1212

Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité

Résumé

Différents types d'attaque ont lieu au moyen de contenus reproduits à partir de ceux de fournisseurs de services de confiance, ce qui conduit des utilisateurs finals à croire à tort à la fiabilité de ces contenus.

La Recommandation UIT-T X.1212 expose des considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité. Ses appendices décrivent des techniques de représentation servant à mesurer la perception par l'utilisateur final de ces indicateurs.

Historique

Edition	Recommandation	Approbation	Commission d'études	Unique ID*
1.0	UIT-T X.1212	30-03-2017	17	11.1002/1000/13195

Mots clés

Perception par l'utilisateur final, hameçonnage, indicateurs de fiabilité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1212

Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité

1 Domaine d'application

Des attaques très diverses ont lieu au moyen de contenus reproduits à partir de ceux de fournisseurs de services de confiance, ce qui conduit des utilisateurs finals à croire à tort à la fiabilité de ces contenus. La présente Recommandation expose des considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité. Ses appendices décrivent des techniques de représentation servant à mesurer la perception par l'utilisateur final de ces indicateurs.

2 Références

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 handicap [b-UIT-T F.790]: Est défini comme un état pour lequel l'utilisation d'équipements et de services de télécommunications est restreinte. Le "handicap" est principalement considéré comme le résultat d'une limitation fonctionnelle temporaire ou permanente due à une maladie, à un accident, au vieillissement, etc. Plus généralement, le "handicap" inclut un état pour lequel il est impossible d'utiliser complètement des équipements et des services de télécommunication en raison de l'environnement physique et/ou social (par exemple, la téléphonie dans un environnement bruyant).

3.1.2 mesure [b-ENISA]: Action ou processus consistant à déterminer la valeur d'une variable quantitative par rapport à une unité de mesure (normalisée).

3.1.3 métrique [b-ENISA]: système de mesures connexes permettant de quantifier une certaine caractéristique d'un système, d'une composante ou d'un processus. Une métrique est composée de deux mesures ou plus.

3.1.4 information d'identification personnelle (PII, *personally identifiable information*) [b-UIT-T X.1252]: Toute information: a) identifiant ou permettant d'identifier, de contacter ou de localiser la personne à laquelle elle se rapporte; b) permettant d'obtenir les informations d'identification ou les coordonnées d'une personne; ou c) étant ou pouvant être directement ou indirectement liée à une personne physique.

3.1.5 hameçonnage [b-UIT-T X.1254]: Escroquerie au moyen de laquelle le destinataire d'un courriel est frauduleusement amené à révéler des informations personnelles ou confidentielles que l'escroc peut ensuite utiliser à des fins illicites.

3.1.6 accessibilité des télécommunications [b-UIT-T F.790]: Dans le domaine des télécommunications, utilisabilité d'un produit, d'un service, d'un environnement ou d'une fonctionnalité par l'ensemble le plus large possible d'utilisateurs, et notamment par les utilisateurs qui présentent un handicap.

3.1.7 personne handicapée [b-UIT-T F.791]: manière correcte de désigner une personne ayant un handicap [b-UNCRPD].

3.2 Terme défini dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 indicateurs de fiabilité: Symboles présentés par un agent utilisateur web qui serviront à informer les utilisateurs finals de la fiabilité d'un site web.

4 Abréviations et acronymes

La présente Recommandation utilise les abbréviations et acronymes suivants:

DKIM Courrier identifié par clé de domaine (*domainkeys identified mail*)

DOM Modèle d'objet de document (*document object model*)

FNE Peur de l'évaluation négative (*fear of negative evaluation*)

SSL Couche de connexion sécurisée (*secure socket layer*)

URL Localisateur uniforme de ressources (*uniform resource locator*)

5 Conventions

Néant.

6 Perception par l'utilisateur final des indicateurs de fiabilité

Les protocoles d'échange d'informations sur la cybersécurité, tels qu'ils sont définis dans [b-UIT-T X.1500], peuvent transmettre des informations utiles à la prise de décisions concernant la fiabilité, lors d'interactions qui ont lieu dans le cyberespace. Ces informations comprennent, sans toutefois s'y limiter, les informations relatives aux certificats de validation étendue [b-CAB-Baseline], le niveau de garantie des identités [b-UIT-T X.1254], les signatures DKIM des courriels [b-IETF RFC 6376], et des indications concernant les sites de hameçonnage [b-IETF RFC 5901].

Toutefois, ces indicateurs de fiabilité sont souvent ignorés ou très peu pris en compte par les utilisateurs finals, selon des études basées sur différents groupes d'utilisateurs (des informations détaillées sont données dans l'Appendice II). Il est donc nécessaire d'améliorer la perception par l'utilisateur final des indicateurs de fiabilité.

7 Techniques visant à améliorer la perception par l'utilisateur final des indicateurs de fiabilité

La présente section décrit plusieurs techniques visant à améliorer la perception par l'utilisateur final des indicateurs de fiabilité. Ces techniques peuvent être utilisées séparément ou associées, selon les souhaits ou les besoins, afin de rendre les indicateurs de fiabilité plus facilement reconnaissables.

7.1 Eléments visuels

Les concepteurs d'indicateurs de fiabilité doivent envisager l'utilisation d'éléments visuels normalisés. Des études ont montré que le codage symbolique des indicateurs de fiabilité, par exemple dans les localisateurs uniformes de ressources (URL), n'est pas adapté aux utilisateurs débutants, et que les indicateurs présentés de cette façon sont souvent ignorés [b-Miyamoto]. Il est donc recommandé d'introduire des éléments visuels, par exemple des icônes correspondant à une indication de fiabilité. Les personnes chargées de la mise en application peuvent envisager l'utilisation de quelques éléments

visuels normalisés, comme sur les panneaux de signalisation routière, afin de réduire au minimum la surcharge cognitive et la surcharge d'apprentissage.

D'après [b-ANSI-Z535.4] (*Product safety signs and labels*), l'utilisation de mots-indicateurs (par exemple "danger" et "attention") en association avec des couleurs (rouge, orange, jaune), réduit le niveau de risque.

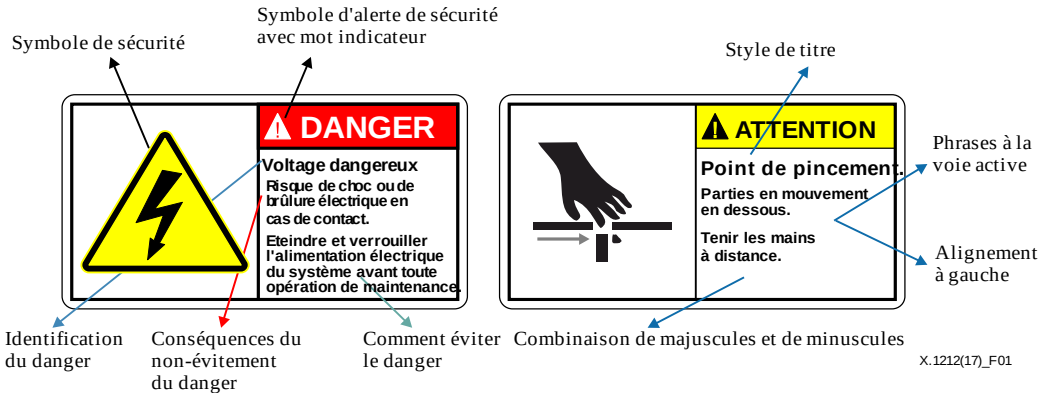


Figure 1 – Signes et étiquettes de sécurité des produits (ANSI Z535.4)

Les éléments utilisés pour le message "DANGER" sont un triangle blanc, un point d'exclamation rouge et un fond rouge. Pour le message "AVERTISSEMENT", un triangle noir et un point d'exclamation orange sont utilisés. Un triangle noir et un point d'exclamation jaune sont utilisés pour le message "ATTENTION".

De plus, les concepteurs d'indicateurs de fiabilité devraient utiliser des systèmes de couleur normalisés pour représenter le niveau de fiabilité. En psychologie des couleurs, le rouge sert à attirer l'attention. Il correspond à la longueur d'onde la plus longue dans le spectre de la lumière visible et a la propriété de sembler plus proche qu'il ne l'est. Par conséquent, le rouge capte l'attention des utilisateurs et est utilisé pour les feux de circulation. Le jaune, dont la longueur d'onde est relativement longue, est une couleur essentiellement stimulante, qui peut capter l'attention des utilisateurs. Le centre du spectre est le vert, qui correspond à la longueur d'onde intermédiaire de la lumière visible. En outre, le vert à tendance à ne pas nécessiter d'ajustement visuel, ce qui permet de l'utiliser comme un signe apaisant et relaxant. Le bleu calme l'esprit et favorise la concentration.

Les concepteurs d'indicateurs de fiabilité peuvent utiliser le concept de "cerveau social", qui encourage les comportements sociables et coopératifs. Des études ont montré que des sujets étaient davantage attentifs aux conventions sociales lorsqu'ils se trouvaient à proximité d'images d'oeil regardant [b-Rigdon], [b-Senju]. Toutefois, certains sont sceptiques quant aux conclusions de ces études, et affirment que l'image d'un oeil regardant est sans effet sur le comportement [b-Felt2014].

7.2 Eléments rédactionnels

Des études ont montré que certains groupes d'utilisateurs prenaient leurs décisions concernant la fiabilité sur la base de contenus rédigés, plutôt qu'en fonction de noms de domaine, de types de protocole ou d'URL [b-Felst2014], [b-Felt2015]. Il est recommandé de munir les logiciels pour utilisateurs finals d'une fonctionnalité qui permette de convertir des informations symboliques en contenus rédigés n'utilisant pas d'acronymes. Ce type de fonctionnalité peut aussi être utile pour les utilisateurs atteints de déficience visuelle, lorsqu'il est utilisé en association avec des systèmes de synthèse vocale.

Pour capter l'attention des utilisateurs, afin de leur envoyer des messages d'avertissement, les concepteurs de logiciels pour utilisateurs finals doivent peut-être envisager l'utilisation des critères de conception énoncés ci-après:

1) Les concepteurs d'indicateurs de fiabilité devraient éviter d'employer des termes techniques. Dans les messages d'avertissement, il convient de remplacer les termes techniques par des tournures ou expressions qui peuvent être comprises par les utilisateurs; en effet, ces derniers ignoreront le message s'ils ne savent pas comment y réagir de manière appropriée.

2) Les concepteurs d'indicateurs de fiabilité devraient s'efforcer d'utiliser des messages courts. Une grande quantité de texte indiquera qu'il faudra un effort de lecture important de la part des utilisateurs, qui risquent de ne pas lire le message. Dans un souci de concision et de précision, les éléments de texte redondants devraient être supprimés du message. Il convient de noter qu'il existe un compromis entre brièveté et précision: il n'est pas possible d'expliquer tous les aspects du modèle de menace en un court paragraphe. Par conséquent, pour les avertissements, les concepteurs peuvent utiliser à la fois des éléments visuels et des éléments de texte. Afin de déterminer le niveau de concision approprié, ils peuvent appliquer un indice de lisibilité, qui permet de mesurer la lisibilité d'un message écrit en estimant le nombre d'années d'éducation nécessaires à sa compréhension.

3) Les concepteurs d'indicateurs de fiabilité devraient décrire le risque qui est survenu ou est sur le point de survenir. Les messages d'avertissement devraient décrire le risque sous-jacent, étant donné qu'il est probable que les utilisateurs comprennent le message et s'y conforment si les risques y sont décrits d'une manière explicite et non ambiguë. Le message devrait aussi comporter des instructions concernant la manière d'éviter le risque, à moins que ces instructions ne soient évidentes dans la formulation du risque.

7.3 Variations des motifs périphériques

Les concepteurs d'indicateurs de fiabilité peuvent tester leur interface en ce qui concerne les variations des motifs périphériques. Une variation soudaine dans la vision périphérique peut être un moyen efficace de signaler un risque potentiel. Il est donc recommandé d'utiliser cette technique en procédant en faisant varier les motifs périphériques (typiquement appelés "thèmes" ou "habillage"), dès que les utilisateurs finals se trouvent devant des sites web ou des courriels qui présentent un risque élevé.

7.4 Mode d'apprentissage

Les concepteurs d'indicateurs de fiabilité peuvent mettre au point des modes d'apprentissage. La perception des risques par l'utilisateur final sera, dans le meilleur des cas, inexacte, s'il n'y est que très rarement exposé. Il est donc recommandé de doter les logiciels pour utilisateurs finals d'un mode d'apprentissage, qui permette de générer artificiellement des événements à risque basés sur des cas réels et de développer la qualité de perception de l'utilisateur final. La ludification de cet apprentissage peut être un moyen d'inciter l'utilisateur final à s'y soumettre.

7.5 Accessibilité

Les concepteurs d'indicateurs de fiabilité devraient concevoir leur interface en tenant compte de l'accessibilité. La vision désigne l'aptitude à distinguer l'aspect, la taille, la forme et la couleur de stimuli visuels. Il peut être difficile de mettre au point des indicateurs de fiabilité pour les personnes qui souffrent de déficience visuelle. En raison de troubles connus sous les noms de "protanopie" et "deutéranopie", certains utilisateurs finals ont du mal à distinguer des couleurs, par exemple le rouge du vert.

L'ISO/CEI a établi un document sur les règles d'accessibilité pour les personnes handicapées [b-ISO/IEC-40500], même si ce document ne traite pas directement des indicateurs de fiabilité dans la barre d'adresse. Le document du CA Browser Forum relatif aux exigences de base [b-CAB-Baseline] définit la norme en ce qui concerne les certificats et les autorités de certification,

bien qu'il ne définisse pas les modalités selon lesquelles les navigateurs présentent les certificats aux utilisateurs.

La liste de contrôle sur l'accessibilité des télécommunications [b-UIT-T-FSTP-TACL] permet de faire en sorte que les services et caractéristiques spécifiés soient accessibles aux différentes catégories d'utilisateurs, y compris aux personnes handicapées. Afin d'améliorer l'accessibilité pour les déficients visuels et les aveugles, l'interface devrait fournir une présentation média à l'utilisateur et pouvoir être commandée dans différents modes et selon différents types d'action de commande. Pour les personnes ayant un handicap cognitif, les points importants devraient être mis en avant afin d'attirer leur attention et des présentations médias supplémentaires, comme des icônes, des vidéos et éléments audio, devraient être utilisées.

Les applications de lecteur d'écran peuvent récupérer des indicateurs de fiabilité à partir des sites web. Elles peuvent présenter des informations de sécurité, par exemple la barre d'adresse verte d'un certificat SSL à validation étendue (SSL EV), et lire les informations à l'aide de services de synthèse vocale. Elles peuvent aussi résumer les informations provenant d'une arborescence de modèle d'objet de document (DOM) à l'intérieur du navigateur.

7.6 Enfants

En ce qui concerne les enfants en ligne, un parent exerce normalement une surveillance en écoutant ou en observant le comportement ou les activités de ses enfants lorsqu'ils communiquent en ligne, ou dispose des informations pour limiter l'accès au format accessible. Cette manière de procéder pour assurer la protection ne sera peut-être pas accessible pour un parent handicapé. Ce rôle particulier, tel qu'il est défini, concerne deux domaines – la protection en ligne des enfants et l'accessibilité pour un adulte/parent handicapé qui élève des enfants n'ayant pas de handicap ainsi que des enfants handicapés.

Appendice I

Considérations relatives à l'analyse cognitive des tâches dans le domaine de la cybersécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Considérations relatives à l'analyse des tâches dans le domaine de la cybersécurité

L'analyse cognitive des tâches aux fins de la cybersécurité peut consister à mesurer les éléments comportementaux ainsi qu'à analyser les interactions, pour finalement afin d'en déduire les processus mentaux internes. Dans la présente Recommandation, les trois concepts de la sécurité de l'information, qui sont le respect de la vie privée, l'intégrité et la disponibilité, sont considérés comme les exigences à satisfaire pour l'analyse cognitive des tâches dans le domaine de la cybersécurité.

I.2 Les trois concepts fondamentaux de la sécurité de l'information

Respect de la vie privée

Les données mesurées peuvent comporter des informations personnelles, qui sont par définition sensibles en termes de respect de la vie privée. Par conséquent, le traitement de ce type de données doit se faire avec précaution, avec l'accord des utilisateurs finals. Le degré de partage de ces informations doit être soumis à un contrôle strict.

Intégrité

Les méthodes de mesure pourraient faire usage des informations collectées sans tenir compte de la peur de l'évaluation négative. Or cette peur a souvent des incidences sur les observations, car les erreurs humaines sont souvent dissimulées par les personnes qui les commettent, leur divulgation conduisant souvent à une dégradation de l'image de soi et de la réputation professionnelle.

Disponibilité

Les observations devraient se faire à l'aide d'une méthode facilement applicable aux personnes. Dans le contexte de la prévention du hameçonnage, les méthodes devraient être disponibles pendant que les utilisateurs parcourent les informations présentées. Les dispositifs sans contact seront à privilégier. En outre, les utilisateurs ne porteront pas d'implants ou d'autres dispositifs susceptibles de les blesser d'une quelconque façon.

I.3 Méthodes de mesure envisageables

La recherche en psychologie expérimentale a mis en évidence un lien étroit entre mouvements oculaires et troubles mentaux [b-Crawford], [b-Noris]. Leigh et al. [b-Leigh] ont classé les mouvements oculaires dans quatre catégories, à savoir: saccades, fixations, mouvements de poursuite fluides, et réflexes vestibulo-oculaires. En général, le mouvement oculaire saccadique varie en fonction de ce que le sujet visualise. Dans le contexte du modèle mental, Irwin et al. ont montré que la rotation mentale est inhibée au cours des mouvements [b-Irwin], et Tokuda [b-Tokuda] a établi que la charge cognitive, c'est-à-dire l'indicateur du degré d'activité mentale/cognitive d'une personne, peut être estimée à partir des intrusions saccadiques.

La validation de la température cutanée au niveau du visage est une autre solution envisageable pour collecter des informations afin d'obtenir une mesure psychologique de l'état mental [b-Or], [b-Wang], [b-Volskamp]. Dans [b-Genno], Genno et al. affirment que, d'après leurs expériences, des variations de température interviennent au niveau de la zone du nez lorsque des sujets éprouvent des sensations comme le stress ou la fatigue. En outre, la thermographie, lorsqu'elle est associée à d'autres méthodes de mesure, offre un moyen hautement automatisé et souple d'évaluer d'une manière objective la charge de travail [b-Or].

Hormis ces solutions, l'activité cérébrale, la conductance cutanée, le rythme cardiaque et la pression artérielle sont souvent utilisés pour collecter des informations, mais la mesure de ces paramètres peut causer des désagréments aux utilisateurs. La reconnaissance des expressions faciales et des gestes est utile en ce qui concerne la disponibilité, mais ses résultats sont facilement faussés par la peur de l'évaluation négative.

Appendice II

Considérations relatives à la protection des utilisateurs finals à l'aide de l'analyse cognitive des tâches

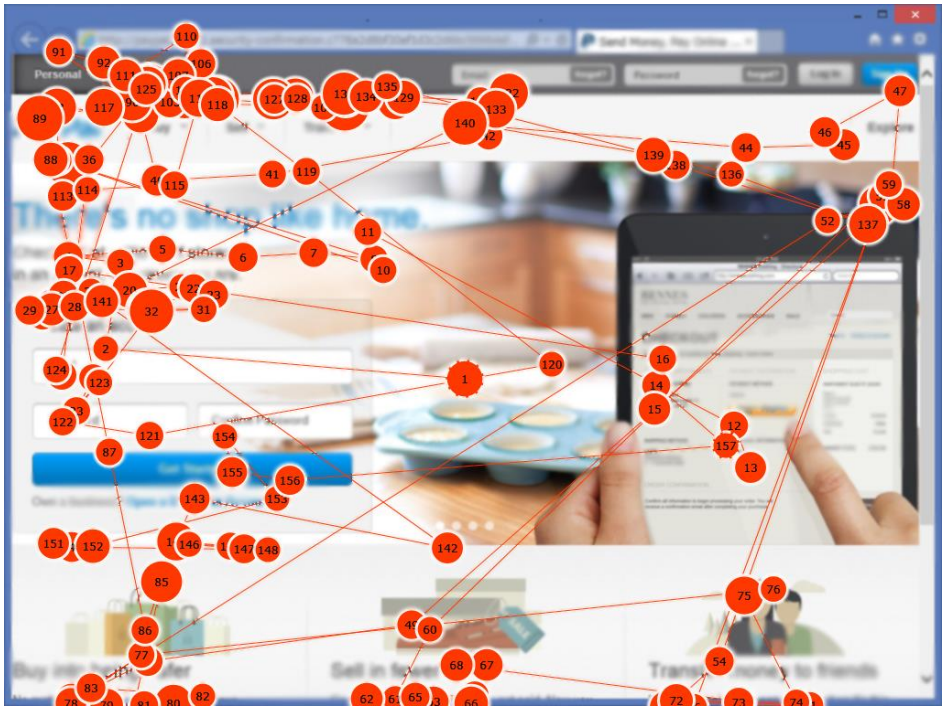
(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

II.1 Evaluation des connaissances et des compétences des utilisateurs

Une étude a montré que les utilisateurs finals peuvent être classés dans deux catégories, à savoir les experts et les débutants [b-Miyamoto]. Les experts jugent de la crédibilité d'un site à partir de son URL et/ou de l'indicateur de la couche de connexion sécurisée (SSL) du navigateur, plutôt qu'en se basant sur les contenus des pages web. En revanche, les débutants reçoivent de puissants signaux en provenance des contenus web. De par leur nature, les sites web de hameçonnage présentent des contenus très similaires à ceux de sites légitimes, ce qui conduit les débutants à se faire piéger.

Ces caractéristiques distinctes des utilisateurs finals sont utiles pour adapter la prévention en matière de hameçonnage à chacune des deux catégories. Une solution envisageable est de fournir un système de détection du hameçonnage qui retourne peu de faux négatifs pour les débutants et peu de faux positifs pour les experts. En général, les systèmes de prévention du hameçonnage ont un problème en ce qui concerne la prévision de la détection, en raison de l'existence d'un compromis entre les faux positifs (signaler des sites légitimes comme des sites de hameçonnage) et les faux négatifs (signaler des sites de hameçonnage comme légitimes). Le système a tendance à retourner davantage de faux positifs lorsqu'on cherche à lui faire retourner moins de faux négatifs (signaler des sites de hameçonnage comme légitimes). La réduction simultanée des deux types d'erreur est jugée difficile à réaliser. Néanmoins, le système doit protéger les débutants, qui souvent ne prennent pas la bonne décision.

L'utilisation d'un dispositif de suivi oculaire permet de repérer plus facilement les débutants parmi les utilisateurs du web. La Figure II.1 représente les mouvements oculaires d'un débutant sur un site web de hameçonnage, tandis que la Figure II.2 montre ceux d'un expert. Les cercles indiquent les points de fixation, et les nombres à l'intérieur des cercles indiquent l'ordre de fixation de ces points. Comme le montre la Figure II.1, dans le cas du site de hameçonnage, le débutant a regardé les contenus web mais a ignoré la barre d'adresse du navigateur lorsqu'il a évalué la crédibilité du site.

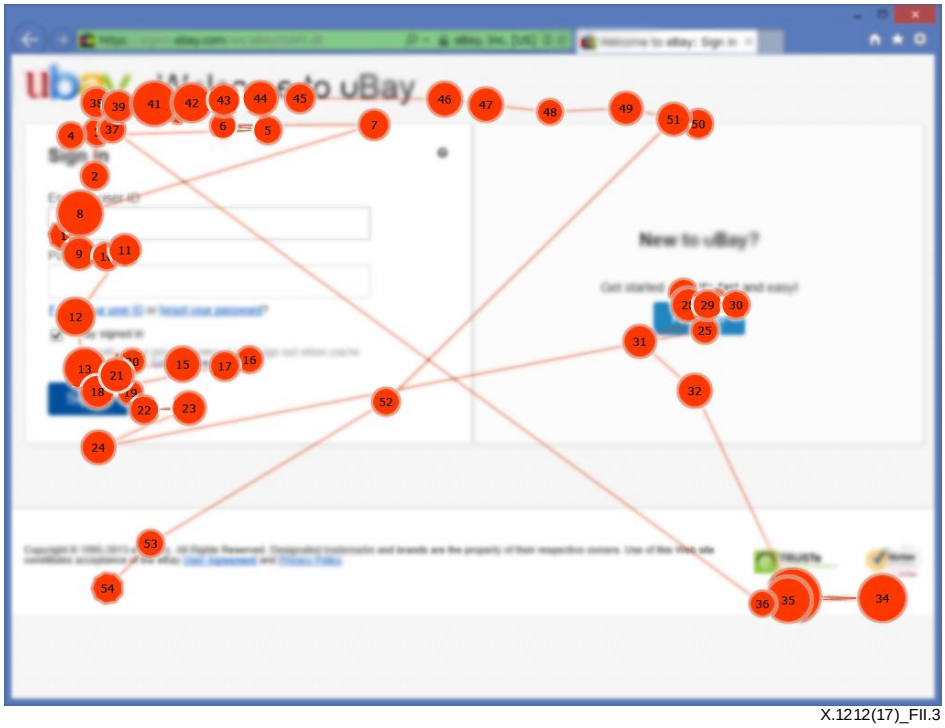


X.1212(17)_FII.1

Figure II.1 – Débutant sur un site web de hameçonnage

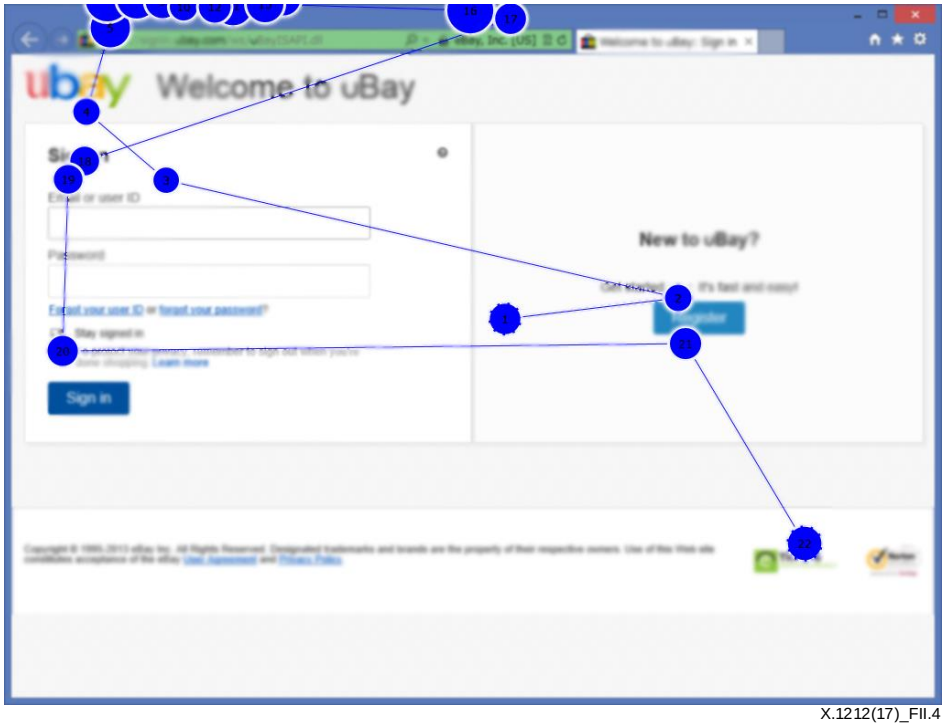
X.1212(17)_FII.2

Figure II.2 – Expert sur un site web de hameçonnage



X.1212(17)_FII.3

Figure II.3 – Débutant sur un site web légitime



X.1212(17)_FII.4

Figure II.4 – Expert sur un site web légitime

Comme le montre la Figure II.3, dans le cas du site web légitime, l'utilisateur débutant a encore prêté uniquement attention aux contenus web. En revanche, un expert a tendance à examiner l'URL du site et/ou l'indicateur SSL du navigateur, plutôt que les contenus de la page web pour juger de la crédibilité du site, comme le montre la Figure II.4. Ces observations du comportement des utilisateurs montrent que les experts ont tendance à regarder la barre d'adresse où l'URL et l'indicateur SSL du navigateur s'affichent au début de la navigation. Les débutants n'y prêtent pas attention en raison de leur méconnaissance des URL ou des indicateurs SSL.

Bibliographie

[b-UIT-T F.790] Recommandation UIT-T F.790 (2007), *Lignes directrices relatives à l'accessibilité des télécommunications pour les personnes âgées et les handicapés*.
<https://www.itu.int/rec/T-REC-F.790>

[b-UIT-T F.791] Recommandation UIT-T F.791 (2015), *Termes et définitions dans le domaine de l'accessibilité*.
<https://www.itu.int/rec/T-REC-F.791>

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*
<https://www.itu.int/rec/T-REC-X.1252>

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités.*
<https://www.itu.int/rec/T-REC-X.1254>

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité.*
<https://www.itu.int/rec/T-REC-X.1500>

[b-UIT-T-FSTP-TACL] UIT-T FSTP-TACL (2006), *Liste de contrôle sur l'accessibilité des télécommunications.*
<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/CEI 40500] ISO/CEI 40500: 2012 (W3C), *Technologies de l'information – Règles pour l'accessibilité des contenus Web (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*, 4ème éd. 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, no. 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] Nations Unies, Convention relative aux droits des personnes handicapées (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.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017