International Telecommunication Union

ITU-T X.1212

(03/2017)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Design considerations for improved end-user perception of trustworthiness indicators

Recommendation ITU-T X.1212

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1212

Design considerations for improved end-user perception of trustworthiness indicators

Summary

Diverse kinds of attacks employ replicated content from trustworthy service providers, thereby deceiving end-users into believing its false trustworthiness.

Recommendation ITU-T X.1212 describes design consideration for improved end-user perception of trustworthiness indicators. The appendices describe representative techniques for measuring end-user perception of such indicators.

History

Edition	Recommendation	Approval	Study Group	
1.0	ITU-T X.1212	2017-03-30	17	11.1002/1000/13195

Keywords

End-user perception, phishing, trustworthiness indicators.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	5
2	References	5
3	Definitions	5
3.1	Terms defined elsewhere	5
3.2	Terms defined in this Recommendation	5
4	Abbreviations and acronyms	6
5	Conventions	6
6	End-user perception of trustworthiness indicators	6
7	Techniques for improved end-user perception of trustworthiness indicators	6
7.1	Visual elements	6
7.2	Narrative elements	7
7.3	Peripheral design transitions	8
7.4	Training mode	8
7.5	Accessibility	8
7.6	Children	9
Appendix I – Considerations for cognitive task analysis in cybersecurity		10
I.1	Considerations for cognitive task analysis in cybersecurity	10
I.2	Three enabling concepts of information security	10
I.3	Possible measurement methods	10
Appendix II – Consideration of end user protection with cognitive task analysis		11
II.1	Estimation of users' knowledge and skills	11
Bibliography		14

Recommendation ITU-T X.1212

Design considerations for improved end-user perception of trustworthiness indicators

1 Scope

A wide variety of attacks utilize replicated content from trustworthy service providers, thereby deceiving end-users into believing their false trustworthiness. This Recommendation describes design considerations for improved end-user perception of trustworthiness indicators. The appendices describe representative techniques for measuring the end-user perception of such indicators.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 disability [b-ITU-T F.790]: This is defined as a state when use of telecommunications equipment and services is restricted. Mainly, "disability" is viewed as a result of temporary or permanent functional limitation due to disease, accident, ageing and so on. More generally, "disability" includes a state when full use of telecommunications equipment and services is not possible due to the physical and/or social environment (e.g., voice telephony under noisy environment).

3.1.2 measurement [b-ENISA]: The act or the process of measuring, where the value of a quantitative variable in comparison to a (standard) unit of measurement is determined.

3.1.3 metric [b-ENISA]: A system of related measuring enabling quantification of some characteristic of a system, component or process. A metric is composed of two or more measures.

3.1.4 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.1.5 phishing [b-ITU X.1254]: A scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly.

3.1.6 telecommunications accessibility [b-ITU-T F.790]: For the telecommunications area, the usability of a product, service, environment or facility by the widest possible range of users and especially users with disabilities.

3.1.7 person with disabilities [b-ITU-T F.791]:The correct way to refer a person with a disability [b-UNCRPD].

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 trustworthiness indicators: Symbols presented by a web user agent that will be used to inform the trustworthiness of the website to end users.

4 Abbreviations and acronyms

DKIM DomainKeys Identified Mail

DOM Document Object Model

FNE Fear of Negative Evaluation

SSL Secure Socket Layer

URL Uniform Resource Locator

5 Conventions

None.

6 End-user perception of trustworthiness indicators

Protocols for cybersecurity information exchange, as identified in [b-ITU-T X.1500], may convey useful information for trustworthiness decisions of any interactions in cyberspace. Such information includes, but is not limited to, extended validation certificate information [b-CAB-Baseline], level of assurance of identities [b-ITU-T X.1254], domainkeys identified mail (DKIM) signatures of e-mail [b-IETF RFC 6376] and indication of phishing sites [b-IETF RFC 5901].

These trustworthiness indicators are however often ignored or least considered by end users, according to past studies based on diverse demographics (details are provided in Appendix II). Thus it is necessary to improve the end-user perception of trustworthiness indicators.

7 Techniques for improved end-user perception of trustworthiness indicators

In this clause, several techniques for improving end-user perception of trustworthiness indicators are presented. These techniques can be used individually or in combination, as desired or appropriate, to present trustworthiness indicators in a more recognizable manner.

7.1 Visual elements

Developers of trustworthiness indicators shall consider the use of standardized visual elements. Past studies have revealed that symbolic encoding of trustworthiness indicators, e.g., in uniform resource locators (URLs), are not friendly to novice users and they are often ignored [b-Miyamoto]. It is thus recommended to introduce visual elements, e.g., icons that represent trustworthiness indication. Implementers may consider employing a few standardized visual elements, as in road signs, to minimize cognitive overhead and training overhead.

According to product safety signs and labels [b-ANSI-Z535.4], the use of signal words (e.g., "Danger," "Warning,") with associated colours (red, orange, yellow) decreases levels of risks.

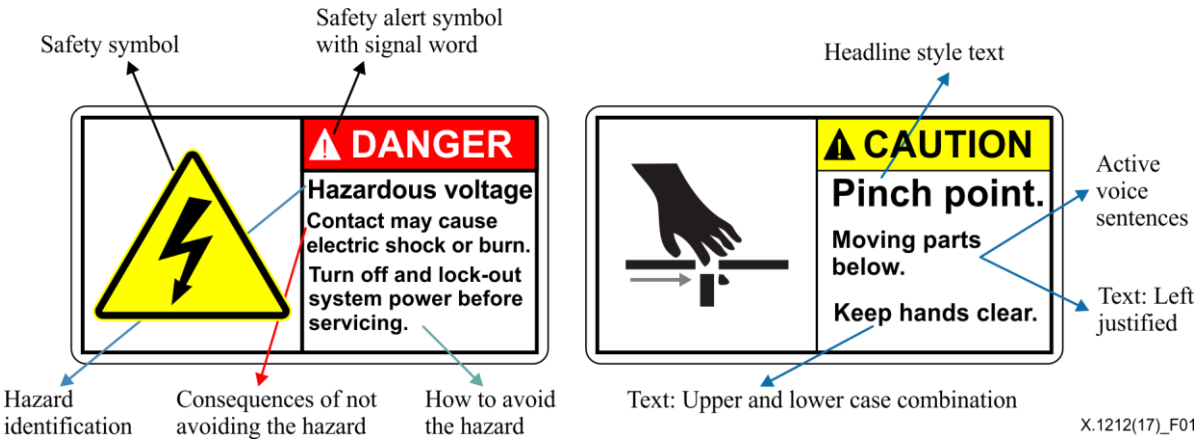


Figure 1 – Product safety signs and labels (ANSI Z535.4)

The message "DANGER" uses a white triangle, red exclamation mark and red background. The "WARNING" message employs a black triangle with an orange exclamation mark. The "CAUTION" message uses a black triangle with a yellow exclamation mark.

Additionally, developers of trustworthiness indicators should employ standard colouring schemes to represent the level of trustworthiness. In the context of colour psychology, red is used for attention. Red is the longest wavelength in the visible light spectrum, and has the property of appearing to be nearer than it is. Red therefore grasps users' attention and is used for traffic lights. The wavelength of yellow is relatively long and essentially stimulating, and it can grab users' attention. The centre of the spectrum is green; it is the intermediate wavelength of visible light. Green also tends to require no adjustment to be seen, so it is used as a restful and relaxed sign. Blue calms the mind and aids concentration.

Developers of trustworthiness indicators may use the concept of the "social brain," which encourages pro-social and cooperative behaviour. Past studies have found that people behave in a more socially conscious manner when they are near images of watching eyes [b-Rigdon], [b-Senju]. However, there is a sceptical view about it, which claims that the image of watching eyes had little to no effect on behaviour [b-Felt2014].

7.2 Narrative elements

Past studies have revealed that certain groups of users make their trustworthiness decision based on narrative writings, rather than domain names, protocol types or URLs [b-Felst2014], [b-Felt2015]. It is recommended to equip end-user software with the capability to convert symbolic information into narrative elements that do not employ acronyms. It can also be helpful to visually impaired users, when combined with text-to-speech systems.

In order to capture users' attention, i.e., warning messages, end-user software may need to consider several design criteria as follows:

1. Developers of trustworthiness indicators should avoid using technical terms. In the warning message, technical terms should be replaced with phrases or expressions that can be understood by users; they will ignore the message if they do not know how to properly respond to it.
2. Developers of trustworthiness indicators should consider the brevity of messages. Large quantities of text will give an indication that much effort will be required to read it, thus users may not read it. In the message, redundant text should be removed in order to be concise and accurate. It should be noted that there is a trade-off relationship between brevity and accuracy; it is not possible to explain all aspects of the threat model in a single short paragraph. Therefore warnings may utilize both visual and text elements. In order to calculate the level of the brevity, the developers may apply a readability index, which is the

measure of readability that estimates the years of education a person needs to understand a piece of writing.

3. Developers of trustworthiness indicators should describe the risk that had occurred or is about to occur. Warning messages should describe the underlying risk, since users are likely to comprehend and comply with the message if it describes the risks explicitly and unambiguously. The message should also include instructions on how to avoid risk, unless these instructions are obvious in the statement of the risk.

7.3 Peripheral design transitions

Developers of trustworthiness indicators may test their interface regarding the peripheral design transitions. Sudden transition in peripheral vision may be effective to signal potential risk. It is thus recommended to employ this technique through the transition of peripheral designs (typically called "themes" or "skins"), whenever end-users are faced with high-risk websites or e-mail messages.

7.4 Training mode

Developers of trustworthiness indicators may prepare training modes. The end-user perception of risk will be inaccurate at best if he or she is very rarely exposed to such risks. It is therefore recommended to equip end-user software with a training mode, where emulated risk events can be artificially generated and the end-user's perception accuracy can be trained. Such training can also be incentivized by gamifying the training.

7.5 Accessibility

Developers of trustworthiness indicators should design its interface considering accessibility. Vision refers to the ability to distinguish the form, size, shape and colour of visual stimuli. For individuals with vision impairment, there can be difficulties to find trustworthiness indicators. Due to the effects known as "protanopia" and "deuteranopia," some end-users have problems in distinguishing colours, e.g., red from green.

ISO/IEC developed the accessibility guideline document [b-ISO/IEC 40500] for persons with disabilities, although, it does not directly address trustworthiness indicators on the address bar. The CA Browser Forum's baseline requirements document [b-CAB-Baseline] defines the standard for certificates and certificate authorities, although it does not define how browsers present certificates to users.

The telecommunications accessibility checklist [b-ITU-T-FSTP-TACL] ensures that the specified services and features are accessible to diverse users, including persons with disabilities. In order to provide better accessibility for visual impairment or blindness, the interface should provide media presentation to the user, and have the ability to be controlled in various modes and types of control action. For persons with cognitive disabilities, important points should be highlighted to draw their attention as well as using supplemental media, such as icons, video and audio.

Screen reader applications may retrieve trustworthiness indicators from websites. They may present security information, e.g., the green address bar of an EV-SSL certificate, and read the information with text-to-speech services. They may also summarize information from a document object model (DOM) tree within the browser.

7.6 Children

With regard to children on line, a parent normally checks up by listening or seeing to the proceedings or activities of their children communicating online or has the information to restrict access in accessible format. That "protective" route may not be accessible to a parent with disabilities. That specific role, as identified, falls between two areas – child protection on line and accessibility for an adult/parent with disabilities with responsibilities for the upbringing of children without disabilities as well as children with disabilities.

Appendix I

Considerations for cognitive task analysis in cybersecurity

(This appendix does not form an integral part of this Recommendation.)

I.1 Considerations for cognitive task analysis in cybersecurity

Cognitive task analysis for cybersecurity purposes may involve the measurement of behavioural elements as well as the analysis of interactions, ultimately leading to the inference of internal mental processes. This Recommendation considers the three concepts of the information security, namely; confidentiality, integrity, and availability, as the requirements for cognitive task analysis in cybersecurity.

I.2 Three enabling concepts of information security

Confidentiality

Measured data may include personal information, which is essentially privacy sensitive. Thus, the use of such data needs to be handled carefully, accompanied by agreement with end users. The extent of sharing such information must be under strict control.

Integrity

The measurement methods might make use of the collected information regardless of the fear of negative evaluation (FNE). Observations are often affected by FNE, where some people will conceal their human errors, as disclosing mistakes often damage their own self-image and professional standing.

Availability

Observations should employ the method which is easily applicable to people. Within the context of phishing prevention, the methods should be available while users are browsing presented information. Non-contact devices will be preferred. Furthermore, users will not carry implants or other devices that may hurt them in any way.

I.3 Possible measurement methods

Research on experimental psychology has evidenced a strong link between eye movements and mental disorders [b-Crawford], [b-Noris]. Leigh et al. [b-Leigh] classified the eye movements into four categories, namely; saccades, fixations, smooth pursuit movements, and vestibulo-ocular reflexes. Generally, the saccadic eye movement changes with what a person is seeing. In the context of mental model, Irwin et al. showed that mental rotation is suppressed during the movements [b-Irwin], and Tokuda [b-Tokuda] showed that mental workload, the indicator of how mentally/cognitively busy a person is, can be estimated from saccadic intrusions.

Validation of facial skin temperature is also feasible to gather information as a physiological measure of mental status [b-Or], [b-Wang], [b-Volskamp]. According to Genno et al. [b-Genno], their experiments showed that there are temperature changes in the nose area when subjects experienced sensations like stress and fatigue. Furthermore, the thermography, when combined with other modes of measurement, provides a highly automated and flexible means to objectively evaluate workload [b-Or].

Aside from these solutions, brain activity, skin conductivity, heart measure, and blood pressure are often used to gather information, however, they tend to require obtrusiveness for users. Recognition of facial expression and gestures are helpful with regard to availability, however, they are easily affected by FNE.

Appendix II

Consideration of end user protection with cognitive task analysis

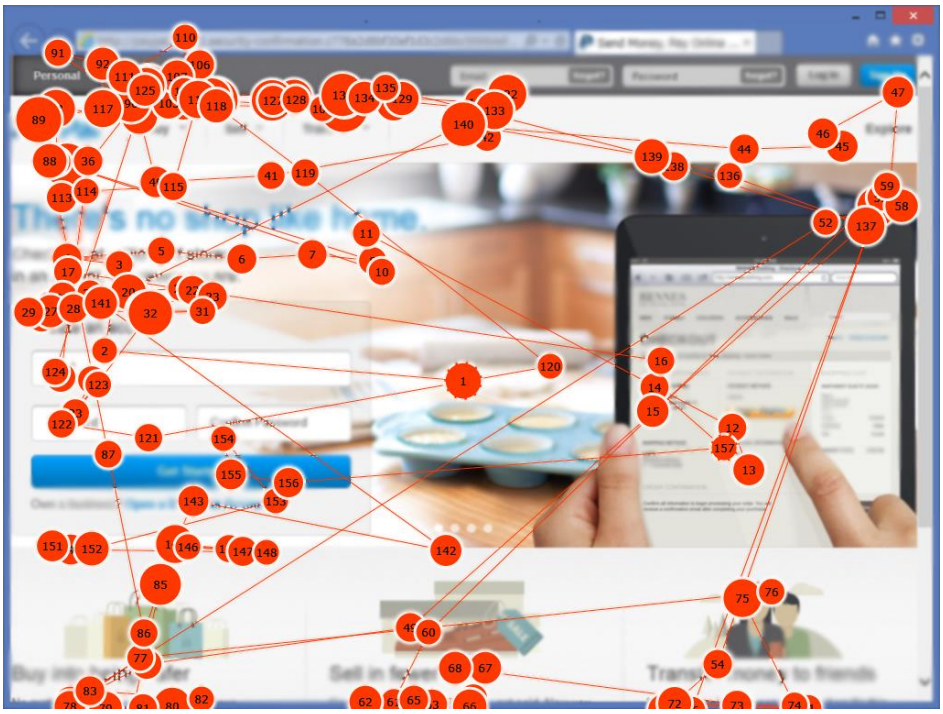
(This appendix does not form an integral part of this Recommendation.)

II.1 Estimation of users' knowledge and skills

A past study illustrates that end users can be categorized into two types, namely; experts and novices [b-Miyamoto]. The experts evaluate a site's URL and/or browser's secure socket layer (SSL) indicator rather than the contents of a web page to judge the credibility of sites. On the other hand, novices received strong signals from web contents. Due to the nature of phishing, the web contents are quite similar to that of legitimate site, leading novices to fall victims to the phishing trap.

These distinct characteristics of end users are useful to adjust phishing prevention for each of them. A possible solution is to provide phishing detection with lower false negative for novices, and lower false positive for experts. Generally, phishing prevention systems have a problem in detection accuracy as there is a trade-off relationship between false positive (labelling legitimate sites as phishing) and false negative (labelling phishing sites as legitimate). The false positive would increase if the systems focus on decreasing false negatives (labelling phishing sites as legitimate). Reduction of both errors is considered difficult. In spite of that, the system must protect novices, who often fail to make the correct decision.

Using an eye-tracking device facilitates the identification of novices among web users. Figure II.1 shows the eye movement of a novice in a phishing website and Figure II.2 shows that of an expert. Circles denote fixations, and the numbers in the circles denote the order of the fixation. In the phishing case, the novice looked at the web content but ignored the browser's address bar while assessing credibility, as shown in Figure II.1.

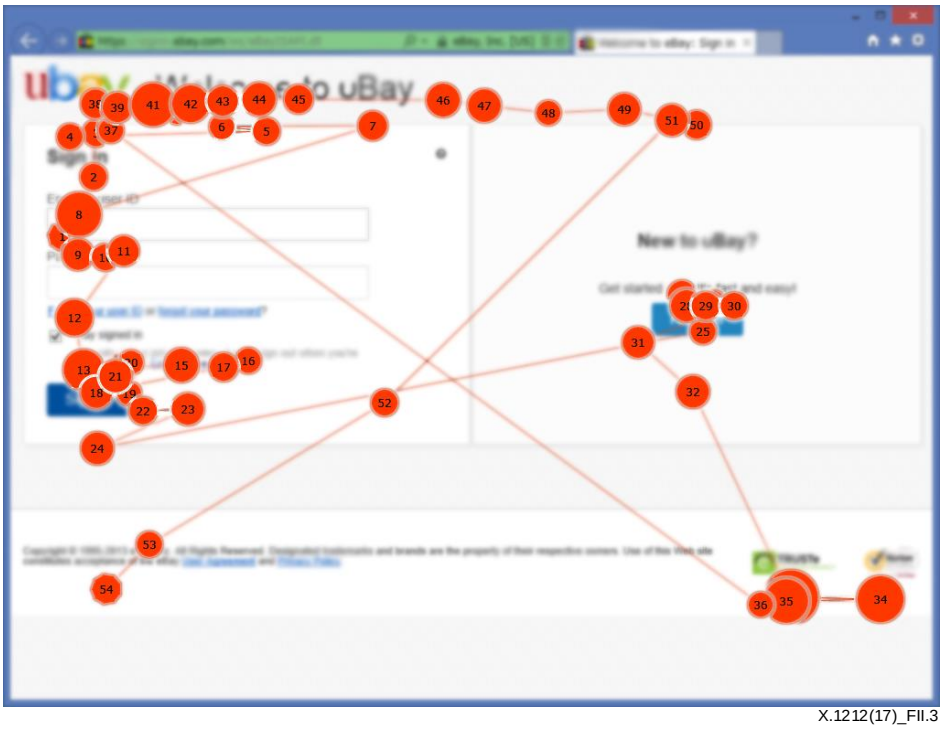


X.1212(17)_FII.1

Figure II.1 – A novice user on a phishing website

X.1212(17)_FII.2

Figure II.2 – An expert on a phishing website



X.1212(17)_FII.3

Figure II.3 – A novice on a legitimate website

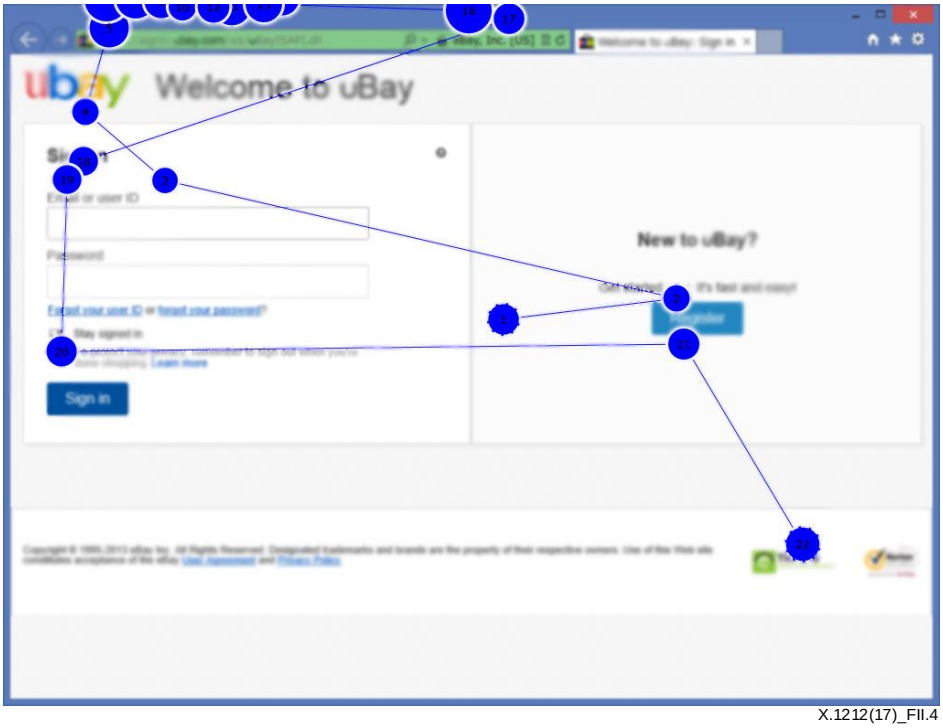


Figure II.4 – An expert on a legitimate website

In the legitimate case, the user also only paid attention to the web content as shown in Figure II.3. By contrast, an expert tends to evaluate the site's URL and/or the browser's SSL indicator rather than the contents of the web page in order to judge the credibility of the sites, as shown in Figure II.4. These behavioural observations indicate that experts tend to look at the address bar where the URL and browser's SSL indicator is displayed at the beginning of browsing. Novices are not aware of them due to the lack of knowledge on URL or SSL indicators.

Bibliography

[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.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017