国 际 电 信 联 盟

ITU-T X.1212

(03/2017)

国际电信联盟
电信标准化部门

X系列：数据网，开放系统通信和安全性

网络空间安全 – 网络安全

增强最终用户对可信指示符的感知的设计考虑

ITU-T X.1212建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
远程生物特征测定	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
网络安全	**X.1200–X.1229**
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1212建议书

增强最终用户对可信指示符的感知的设计考虑

摘要

各类攻击采用来自可信服务提供商的复制内容，从而使最终用户误信其虚假的可信性。

ITU-T X.1212建议书说明了增强最终用户对可信指示符的感知的设计考虑。附录介绍了测量最终用户对这些指示符的感知的代表性技术。

历史沿革

版本	建议书	批准日期	研究组	唯一ID*
1.0	ITU-T X.1212	2017-03-30	17	11.1002/1000/13195

关键词

最终用户感知、网络钓鱼、可信指示符。

---

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1212建议书

增强最终用户对可信指示符的感知的设计考虑

1 范围

各类攻击采用来自可信服务提供商的复制内容，从而使最终用户误信其虚假的可信性。本建议书说明了增强最终用户对可信指示符的感知的设计考虑。附录介绍了测量最终用户对这些指示符的感知的代表性技术。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书采用了下列其它资料定义的术语：

3.1.1 残疾：被定义为一种使电信设备和业务使用受到限制的状态。

大体而言，“残疾”被认为是由于疾病、事故、变老等引起的临时性或永久性的功能性限制的结果。更一般而言，“残疾”包含了一种状态，在这种状态下，由于物理环境和/或社会环境（例如嘈杂环境下的话音电话）的影响，不可能充分使用电信设备和业务。

3.1.2 测量[b-ENISA]：测定与（标准）衡量单位对比的量化变量值的测量行为或过程。

3.1.3 度量表[b-ENISA]：能够对方法、组件或程序的某些特性进行量化的相关测量体系。度量表由两种或更多测量标准构成。

3.1.4 个人可识别信息（PII）[b-ITU-T X.1252]：任何a) 可识别或可用于识别、联系或定位与其相关的个人；b) 从其中能够获得某个人的识别或联系信息；或c) 直接或间接与一个自然人相关联的信息。

3.1.5 钓鱼[b-ITU X.1254]：诱骗电子邮件或网页用户披露个人或保密信息供诈骗者非法使用的一种欺诈行为。

3.1.6 电信无障碍获取[b-ITU-T F.790]：在电信领域，产品、服务、环境或设施可被最广泛的用户范围（尤其是残疾人）使用的可用性。

3.1.7 残疾人[b-ITU-T F.791]：正确表述身患残疾人员的方法 [b-UNCRPD]。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 可信指示符（trustworthiness indicators）：由网络用户代理提供的用于向最终用户传达网站可信性的符号。

4 缩写词和首字母缩略语

DKIM 域名密钥识别邮件

DOM 文档对象模型

FNE 负面评价恐惧

SSL 安全套接层

URL 统一资源定位符

5 排印惯例

无。

6 最终用户对可信指示符的感知

[b-ITU-T X.1500]中确定的网络安全信息交换协议可传达对网络空间中任何交互的可靠性做出判断的有用信息。这类信息包括但不限于：扩展验证证书信息[b-CAB-Baseline]、身份保证水平[b-ITU-T X.1254]、电子邮件的域名密钥识别邮件（DKIM）签名[b-IETF RFC 6376]和钓鱼网站指征[b-IETF RFC 5901]。

但根据以往基于不同人口统计的研究，这些可信指示符往往被最终用户忽略或是得到最少考虑的因素（详见附录二）。因此有必要增强最终用户对可信指示符的感知。

7 增强最终用户对可信指示符的感知的技术

本节中介绍了若干增强最终用户对可信指示符的感知的技术。这些技术可随意或酌情单独使用或组合使用，以更易于识别的方式呈现可信指示符。

7.1 视觉元素

可信指示符的设计人员们须考虑采用标准化的视觉元素。以往的研究表明，可信指示符的符号编码（如统一资源定位符（URL）中所示）不便于新手用户使用，而且往往会被忽略[b-Miyamoto]。因此，建议引入视觉元素，如代表可信标志的图标。实施者可考虑使用一些标准化的视觉元素，如路标中使用的视觉元素，以尽可能降低认知负荷和培训开销。

根据产品安全标志和标签[b-ANSI-Z535.4]，使用信号词（如“危险”、“警告”）及相关颜色（红色、橙色、黄色）可降低风险等级。

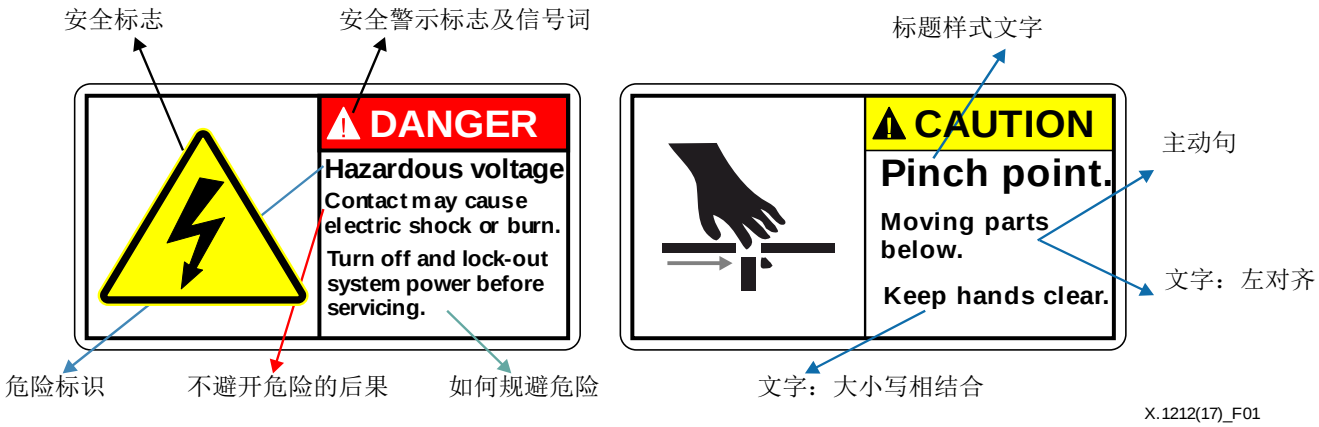


图1 – 产品安全标志和标签（ANSI Z535.4）

“DANGER（危险）”消息采用了白色三角形、红色感叹号和红色背景。“WARNING（警告）”消息采用了黑色三角形和橙色感叹号。“CAUTION（注意）”消息采用了黑色三角形和黄色感叹号。

此外，可信指示符的设计人员应使用标准配色方案来表示可信水平。在色彩心理学中，红色用于引起注意。红色在可见光谱中光波最长，在视觉上有一种迫近感。因此，红色易引起用户注意并且用于交通信号灯。黄色光波相对较长，光感强烈，可吸引用户的注意。绿色位于光谱中心；在可见光谱中波长居中。绿色通常亦不需要人眼做出调整，因此用作宁静、轻松的标志。蓝色使人平静，注意力集中。

可信指示符的设计人员可使用“社会脑”概念，此概念提倡亲社会行为和合作行为。以往研究发现，当人们接近注视的目光的图像时，会以更强社会意识的方式行事[b-Rigdon]、[b-Senju]。但有人对此提出了质疑，认为注视的目光的图像对行为的影响很小或没有影响[b-Felt2014]。

7.2 叙述性元素

以往的研究表明，某些用户群体根据叙述性文字（而非域名、协议类型或URL）判断可信度[b-Felst2014]、[b-Felt2015]。建议安装能够将符号信息转换为不使用首字母缩略语的叙述性元素的最终用户软件。当与文本转语音系统结合时，对视觉障碍用户也有帮助。

为了吸引用户注意，即警告消息，最终用户软件需要考虑如下几个设计标准：

1) 可信指示符的设计人员应避免使用技术术语。在警告消息中，技术术语应替换为用户可理解的短语或表述方式；如果用户不清楚如何恰当地做出响应，就会忽略该信息。

2) 可信指示符的设计人员应考虑消息的简洁性。大量的文本说明需要花很多精力去阅读，因此用户可能不会去读。应删除消息中的冗余内容，以确保简明以及准确。应注意，简洁性和准确性之间存在权衡关系；不可能在一个简短的段落中说明威胁模型的所有方面。因此，警告可同时利用视觉和文本元素。为了计算简洁性，开发人员可采用可读性指标，该指标是对估计某个人要理解一段文字所需教育年数的可读性的衡量。

3) 可信指示符的设计人员应描述已经发生或即将发生的风险。警告消息应描述潜在风险，因为如果清楚明确地描述风险，用户很可能会理解和遵从消息指示。该信息还应包括如何规避风险的说明，除非风险声明中已明确说明了如何规避风险。

7.3 外围设计转换

可信指示符的设计人员可针对外围设计转换测试其界面。外围视图的突然转换是表明存在潜在风险的有效手段。因此，建议在最终用户面临高风险网站或电子邮件消息时，通过外围设计（通常称为“主题”或“皮肤”）转换来应用这一技巧。

7.4 培训模式

可信指示符的设计人员可编制训练模式。如果最终用户很少接触到此类风险，那么最乐观地说最终用户对风险的认知也是不准确的。因此，建议安装具有培训模式的最终用户软件，该软件可人为地生成模拟风险事件，训练最终用户的感知精度。这种培训也可以通过游戏化来加以激励。

7.5 无障碍访问

可信指示符的设计人员在设计其界面时应考虑到无障碍访问问题。视觉是指区分视觉刺激的形式、大小、形状和颜色的能力。具有视觉障碍的人可能难以发现可信指示符。由于“红色盲”和“绿色盲”效应，一些最终用户在区分颜色（如红色和绿色）方面有困难。

国际标准化组织（ISO）/国际电工委员会（IEC）制定了针对残疾人的无障碍获取指南文件[b-ISO/IEC-40500]，但并未直接涉及地址栏上的可信指示符。认证机构（CA）浏览器论坛的基准要求文件[b-CAB-Baseline]定义了证书和认证机构的标准，但没有定义浏览器如何向用户提供证书。

电信无障碍获取清单[b-ITU-T-FSTP-TACL]确保指定的服务和功能可供包括残疾人在内的各类用户使用。为了改善针对视觉障碍或失明的无障碍获取性，应在界面向用户提供媒体演示，并能够通过各种模式和各类控制动作进行控制。对于认知方面患有残疾的人员，应强调重点，提醒他们注意并采用图标、视频和音频等辅助媒介。

读屏器应用可从网站检索可信指示符。这些应用可显示安全信息，如EV-SSL证书的绿色地址栏，并利用文本转语音服务读取信息，还可汇总来自浏览器中文档对象模型（DOM）树的信息。

7.6 儿童

关于上网儿童，父母通常借助倾听或观察其子女在线交流的过程或活动，或者掌握如何以可无障碍获取的方式限制信息获取方面信息的方式进行检查。对于残疾人父母而言，这种“保护”途径或许行不通。这种确定的特定角色属于两个领域：成人/残疾人父母保护上网儿童及无障碍获取，他们负有养育正常儿童和残疾儿童的职责。

附录一

网络安全中认知任务分析的考虑

（本附录不构成本建议书的组成部分）

I.1 网络安全中认知任务分析的考虑

用于网络安全目的的认知任务分析可包括行为元素的测量以及交互的分析，最终产生内部心理过程的推断。本建议书考虑了信息安全的三个概念，亦是对网络安全中认知任务分析的要求，即机密性、完整性和可用性。

I.2 信息安全的三个关键概念

机密性

测得的数据可能包含个人信息，这种信息属隐私信息。因此，此类数据需在得到最终用户同意的情况下谨慎使用。此类信息的共享范围必须受到严格控制。

完整性

测量方法可利用收集的信息，不考虑负面评价恐惧（FNE）。观察结果常受到FNE的影响，其中一些人会隐藏他们的人为错误，因为披露错误常会损害他们自己的形象和专业地位。

可用性

观察应采用人们易于应用的方法。在预防网络钓鱼的情况下，当用户浏览呈现的信息时，应可使用相关方法。非接触性设备是首选。此外，用户不会携带可能以任何方式对其造成伤害的植入物或其他设备。

I.3 可能的测量方法

实验心理学的研究证明眼球运动和精神障碍之间存在显著联系[b-Crawford]、[b-Noris]。Leigh等人[b-Leigh]将眼球运动分为四类，即扫视、注视、平稳追踪运动和前庭眼球反射。一般来说，扫视运动随着人们所看到的对象而发生改变。在心理模型中，Irwin等人说明了在运动期间心理旋转受到抑制[b-Irwin]，Tokuda[b-Tokuda]说明了可根据扫视性侵扰估计脑力负荷（一个人智力上/认知上忙碌程度的指标）。

面部皮肤温度的验证亦可收集信息作为对心理状态的生理测量[b-Or]、[b-Wang]、[b-Volskamp]。Genno等人[b-Genno]指出，他们的实验表明，当受试者经历压力和疲劳等感觉时，鼻部区域的温度会有所变化。此外，热成像与其他测量模式结合可提供一种高度自动化和灵活的方法来客观地评估负荷[b-Or]。

除了这些解决方案，大脑活动、皮肤导电性、心脏监测和血压常用来收集信息，但这些方法往往会对用户造成不便。对面部表情和手势的识别对于可用性是有帮助的，但却易受到FNE的影响。

附录二

从认知任务分析角度对保护最终用户的考虑

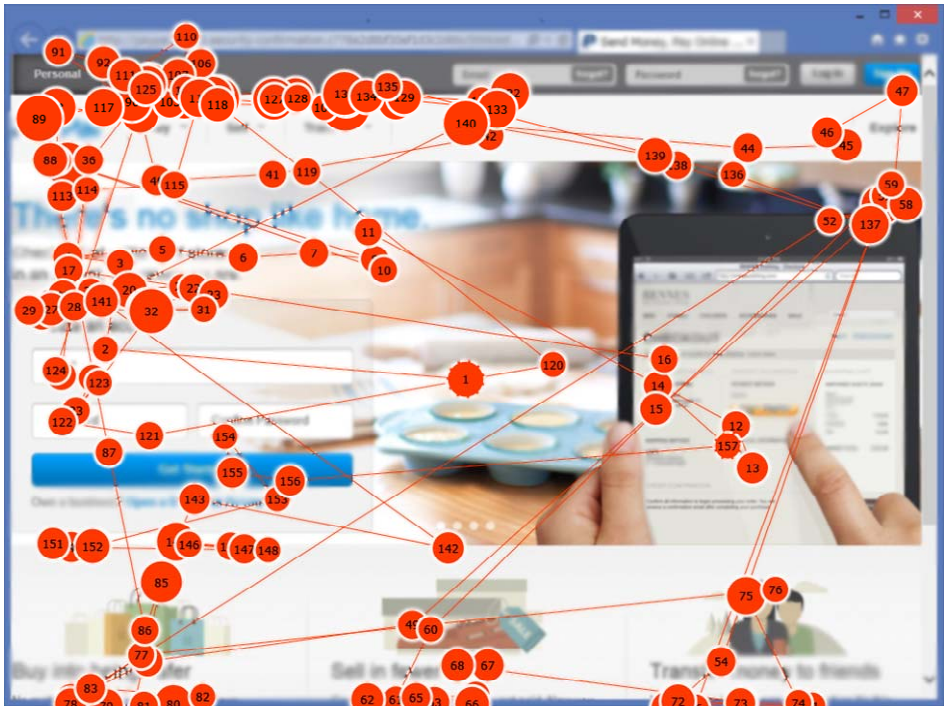
（本附录不构成本建议书的组成部分）

II.1 用户知识和技能的估计

以往的研究表明，最终用户可以分为两种类型，即专家和新手[b-Miyamoto]。专家用户通过评估网站的URL和/或浏览器的安全套接层（SSL）指示符（而非网页的内容）来判断网站的可信性；另一方面，新手用户对网络内容的感知较强，由于网络钓鱼的性质，网页内容与合法网站的内容非常相似，导致新手用户成为网络钓鱼陷阱的受害者。

最终用户的这些独特特性对于针对每个用户调整网络钓鱼预防措施非常有用。一种可能的解决方案是为新手用户提供漏报率较低的网络钓鱼检测工具，为专家用户提供误报率较低的网络钓鱼检测工具。一般来说，网络钓鱼预防系统在检测准确性方面存在问题，因为误报（将合法网站标记为钓鱼网站）和漏报（将钓鱼网站标记为合法网站）之间存在权衡关系。如果系统专注于降低漏报率（将钓鱼网站标记为合法网站），误报率就会上升。普遍认为，同时减少这两种错误非常困难。尽管如此，系统必须保护往往不能做出正确决定的新手用户。

使用眼球追踪装置便于确定网络用户中的新手用户。图II.1显示了新手用户在钓鱼网站上的眼球运动，图II.2显示了专家用户的眼球运动。圆圈表示注视，圆圈中的数字表示注视的顺序。在钓鱼网站的情况中，新手用户在评估可信性时关注的是网络内容，而忽略了浏览器的地址栏，如图II.1所示。

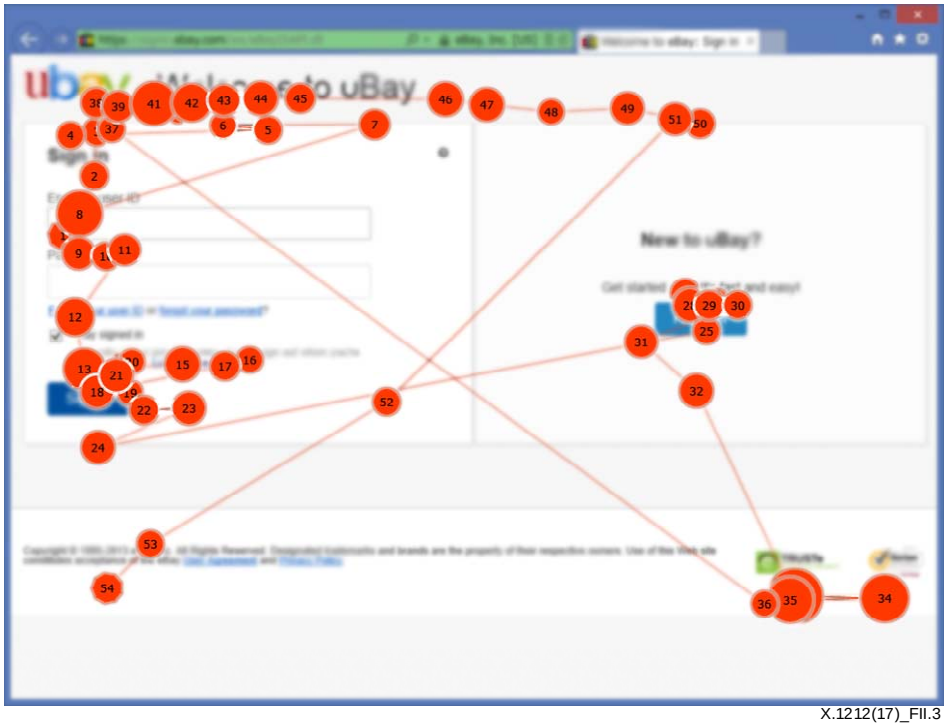


X.1212(17)_FII.1

图II.1 – 新手用户在钓鱼网站

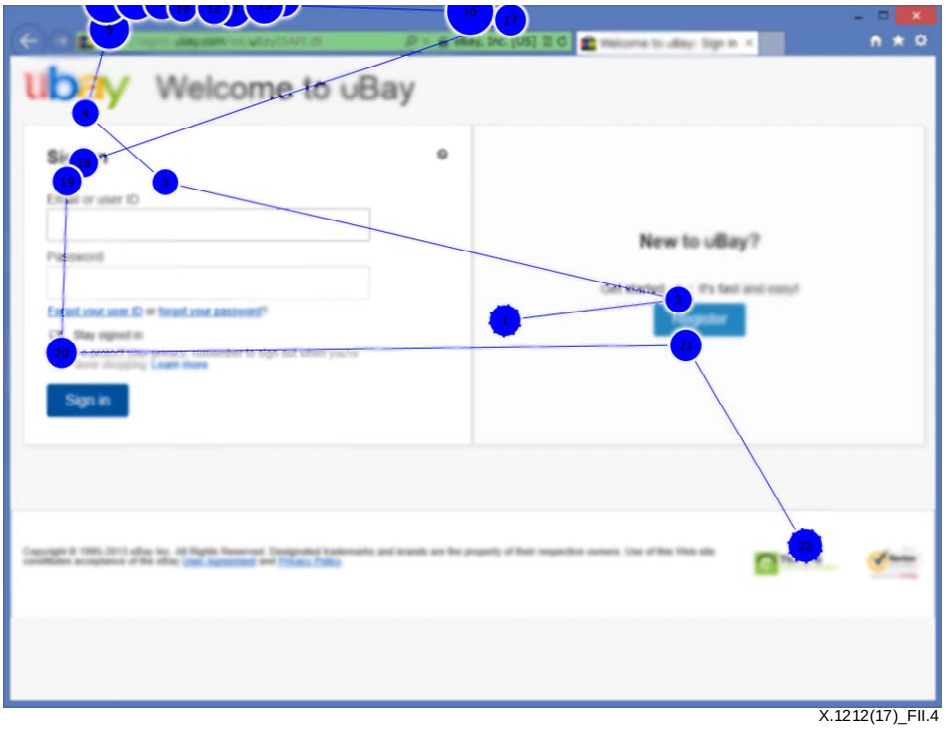
X.1212(17)_FII.2

图II.2 – 专家用户在钓鱼网站



X.1212(17)_FII.3

图II.3 – 新手用户在合法网站



S X.1212(17)_FII.4

图II.4 – 专家用户在合法网站

在合法网站的情况中，用户亦仅注意网页内容，如图II.3所示。相比之下，专家用户往往会评估网站的URL和/或浏览器的SSL指示符而非网页内容，以判断网站的可信性，如图II.4所示。这些行为观察结果表明，专家用户在浏览开始时倾向于查看显示URL和浏览器SSL指示符的地址栏。由于缺乏关于URL或SSL指示符的知识，新手用户不会考虑到这些问题。

参考文献

[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.

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	一般关税原则
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	终端和主观及客观的评价方法
系列 Q	交换和信令
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	电信系统的语言和通用软件方面

瑞士印刷
2017年，日内瓦