ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 2
Geneva, Switzerland
1 July 2016

Introduction to X.cogent (Q4/SG17), a design consideration for trustworthiness indicators

Daisuke Miyamoto,
Assistant Professor, The University of Tokyo,
daisu-mi@nc.u-Tokyo.ac.jp

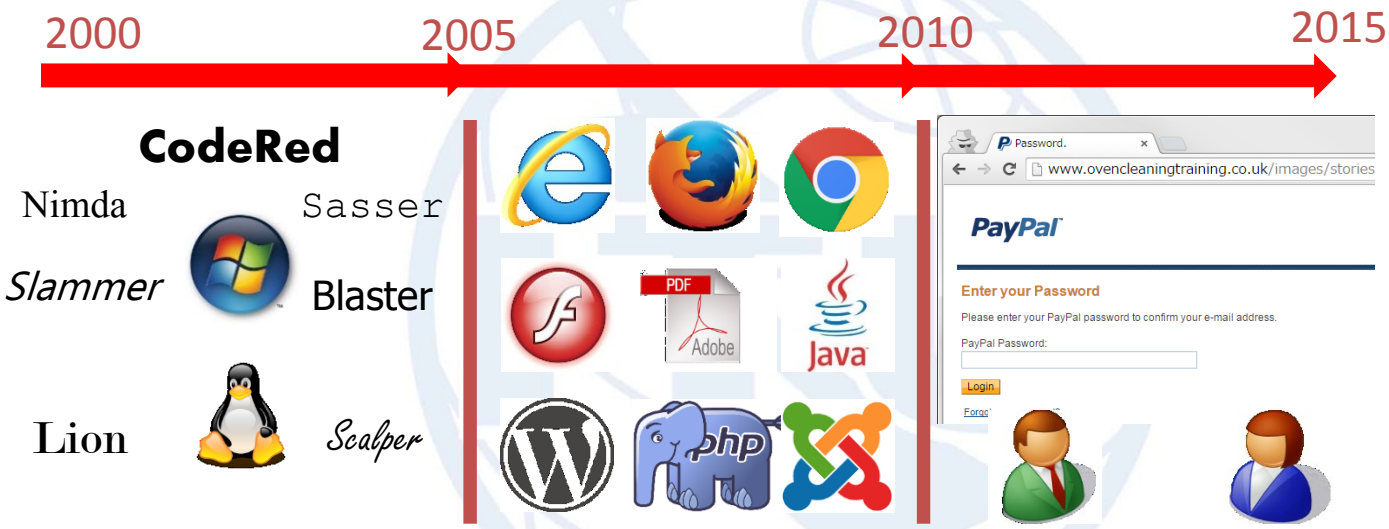
1956 2016
CCITT / ITU-T

ITU

Overview

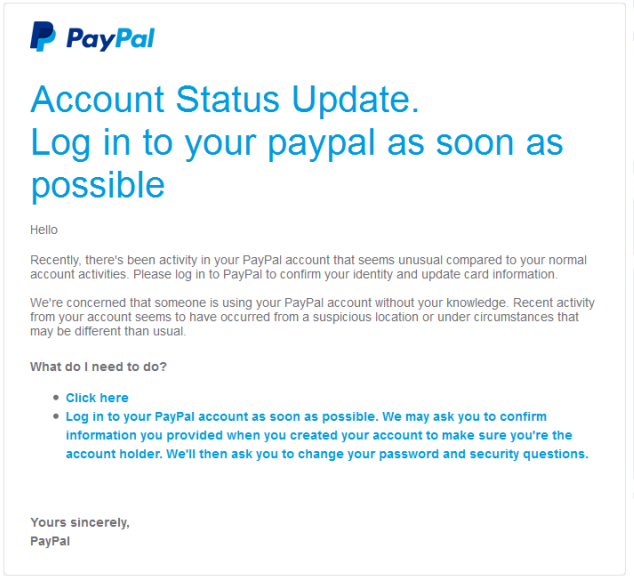
- Trust for ICT users
- Support decision making
- Cognitive psychology
- Conclusion

Major cyber threats



2001-2005	2006-2010	2011-2015
OS and services	Web and services	Users
Buffer Overflows Denial of Service	Heap Spraying Code Injection	Phishing APT

What is phishing?



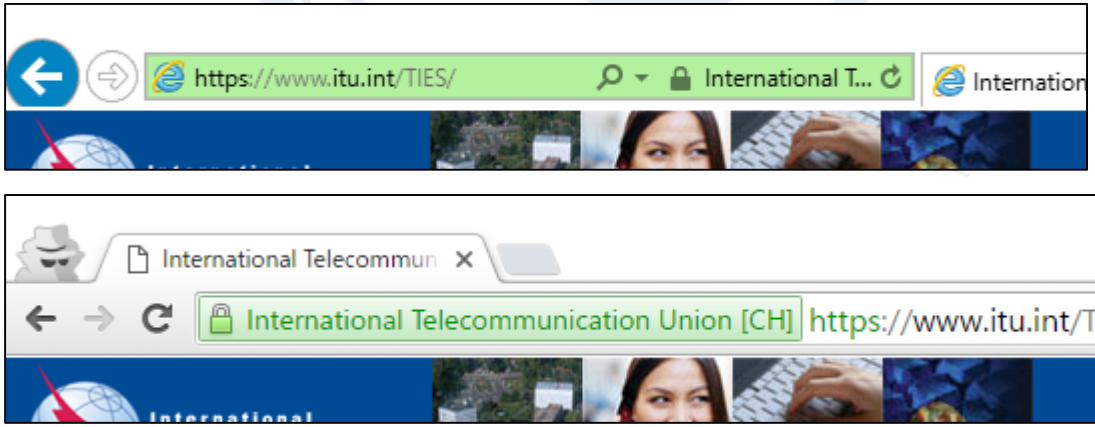
Amount loss due to phishing		
2005	$0.9 billion	Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce (Gartner)
2008	$3.6	Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks.（Gartner)
2013	$5.9	THE CURRENT STATE OF CYBERCRIME 2014(RSA)
2014	$8.5	Internet Crime Compliant Center (FBI)

CCITT / ITU-T

Scope of X.cogent (Q4/SG17)

- Scope
  - Provides design consideration for improved ICT users' perception of trustworthiness indicators
  - Symbols appeared by a user agent that will be used to inform the trustworthiness of the entity to ICT users.

The cases of web user agents – trustworthiness of websites is summarized in the browsers' address bar.

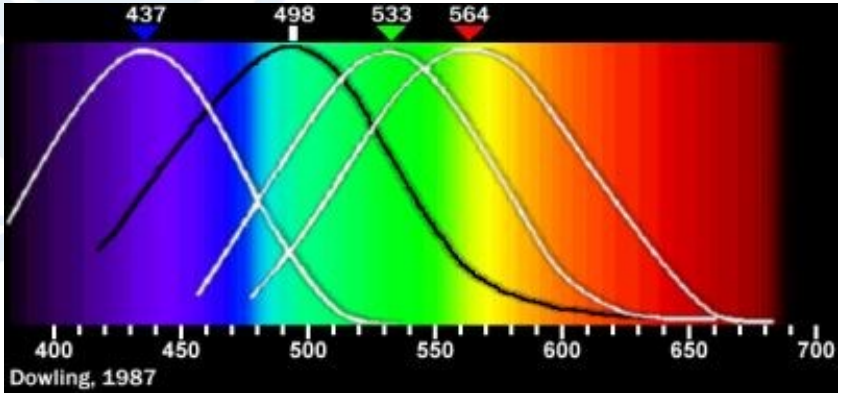


Visual elements

- Standardized visual elements
  - DANGER: white triangle, red background
  - CAUTION: black triangle, yellow background
- Coloring scheme

Color	Meaning
Green	Safety, Relax
Blue	Composure
Yellow	Concentration, Care
Red	Warning, Exciting

J. E. Dowling, "The Retina : An Approachable Part of the Brain," (1987)



Narrative elements

Google Chrome 36

Title: The site's security certificate is not trusted!

You attempted to reach example.com, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.

Google Chrome 37

Title: Your connection is not private

Attackers might be trying to steal your information from example.com (for example, passwords, messages, or credit cards).

1. Avoid Technical Terms
2. Brevity
   (Tradeoff between Accuracy)
3. Risk Description

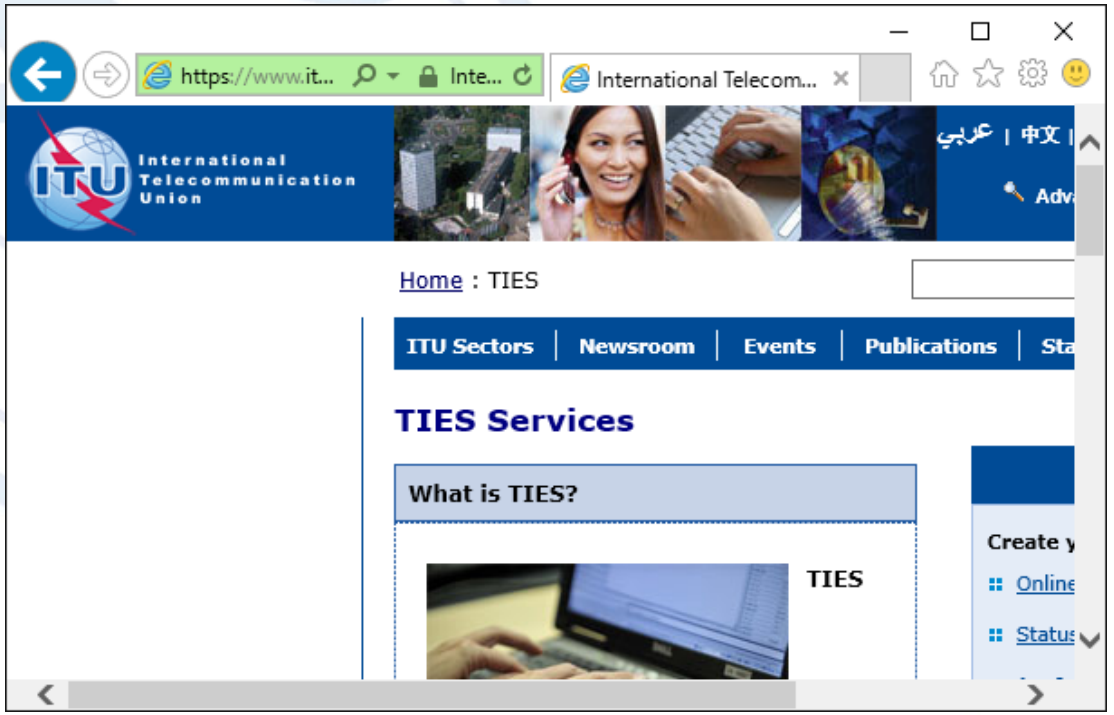
A.P. Felt "Improving SSL Warnings: Comprehension and Adherence", 2015

Peripheral design / Training mode

- Peripheral design transitions
  - Sudden transition in peripheral vision may be effective to signal potential risk
  - This contribute to improve situation awareness; ICT users are going to do risky instructions
- Training mode
  - ICT users' perception of risk will be inaccurate at best if he or she is very rarely exposed to such risks.
  - Moderate-risk events can be artificially generated and ICT users' perception can be trained.

Accessibility

- How people with visual impairment aware risky situation?



Accessibility - Screen readers

- Problem
  - The almost of all screen readers are designed to deal with web content, but are not capable to the information appeared at the address bar of the web browser.

OS	Application	API
Windows	IE	MSAA + UIA
	Firefox	MSAA + IAccessible2
	Chrome	MSAA + IAccessible2
Mac OS	Safari	AXAPI
Linux		Assistive Technology-Service Provider Interface

Accessibility - Standards

- ISO/IEC-40500:2012
  - Guideline document for people with disabilities, but it does not directly address trustworthiness indicators on the address bar.
- Baseline Requirements (CA/Browser Forum)
  - Standard for certificates and certificate authorities, although it does not define how browsers present certificates to users.
- Telecommunications Accessibility Checklist (FSTP-TACL)
  - This intends to ensure that the specified services and features are usable by diverse users, including people with disabilities.
  - The interface should provide media presentation to the user, and allow to be controlled in various modes and types of control action.

Cognitive psychology

seeing heart-beating breathing thinking

Cognitive Psychology		
Purpose	Object	Method
Investigation	Internal mental status / procedure	Observable action/behavior

Methods for cognitive task analysis

Methods	
Blinking, EOG (electrooculography) [Veltman 1998, Wilson 2003]	Gaze tracking [Marshall 2003, Zhai 1999]
Pupil dilation [Marshall 2002]	Facial warmth [Veltman & Vos, 2005]
Voice stress [Rothkrantz 2004]	Respiratory [Veltman 1998, Wientjes 1992]
Blood pressure [Veltman 1996, Miyake 2000]	EEG (electroencephalogram) [Wilson 2001, Prinzel 1999]
Skin conductivity [Haag 2004]	EMG (electromyography) [Lundberg 1994, Karthikeyan 2012]
Gesture recognition [Ehlert 2003]	Facial expression [Kuilenburg 2005, Jenifer 2007]

Requirements for cybersecurity

Considerations for cognitive task analysis in cybersecurity

Confidentiality — Privacy vs. Control

Integrity — Evasion (Fear of negative evaluation)

Availability — Easier to be equipped

Confidentiality vs. Privacy

- Biological information as observable data
  - Different requirements
    - medical science, neuroscience …
    - information technology
  - Potential differences in “Human Identifiable”
    - Anonymity
    - Technological evolution

Social Acceptance

- Informed consent
- Benefit from cognitive task analysis
- Risks of using systems
- Open guidelines

Confidentiality of data

- Data acquisition
- Data in network

Safety for users

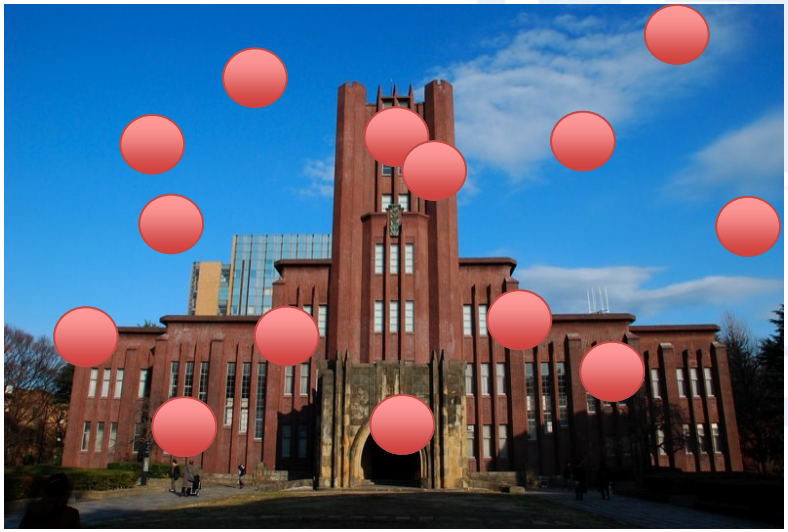
- Compromised devices must not control users
- Loss of network connectivity/packets must not damage users

Case study :
Eye movement and intention

Eye movement and intention

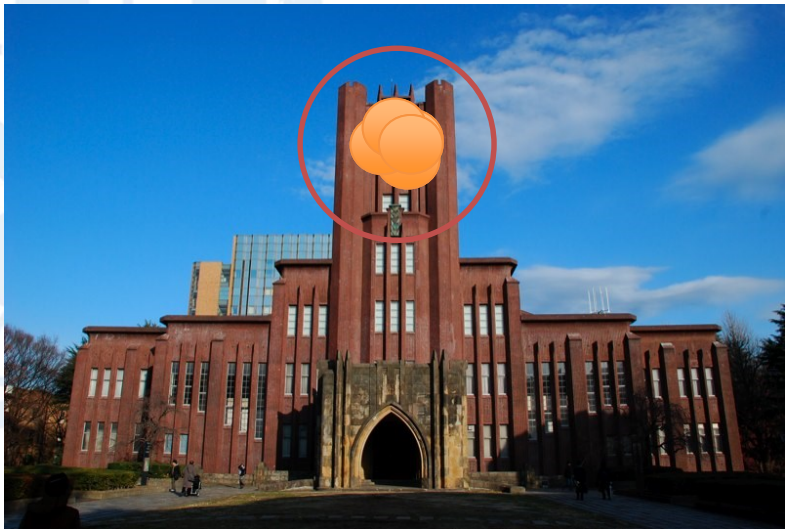
Navigational

- To find any object in a visual input
  - without a particular motivation

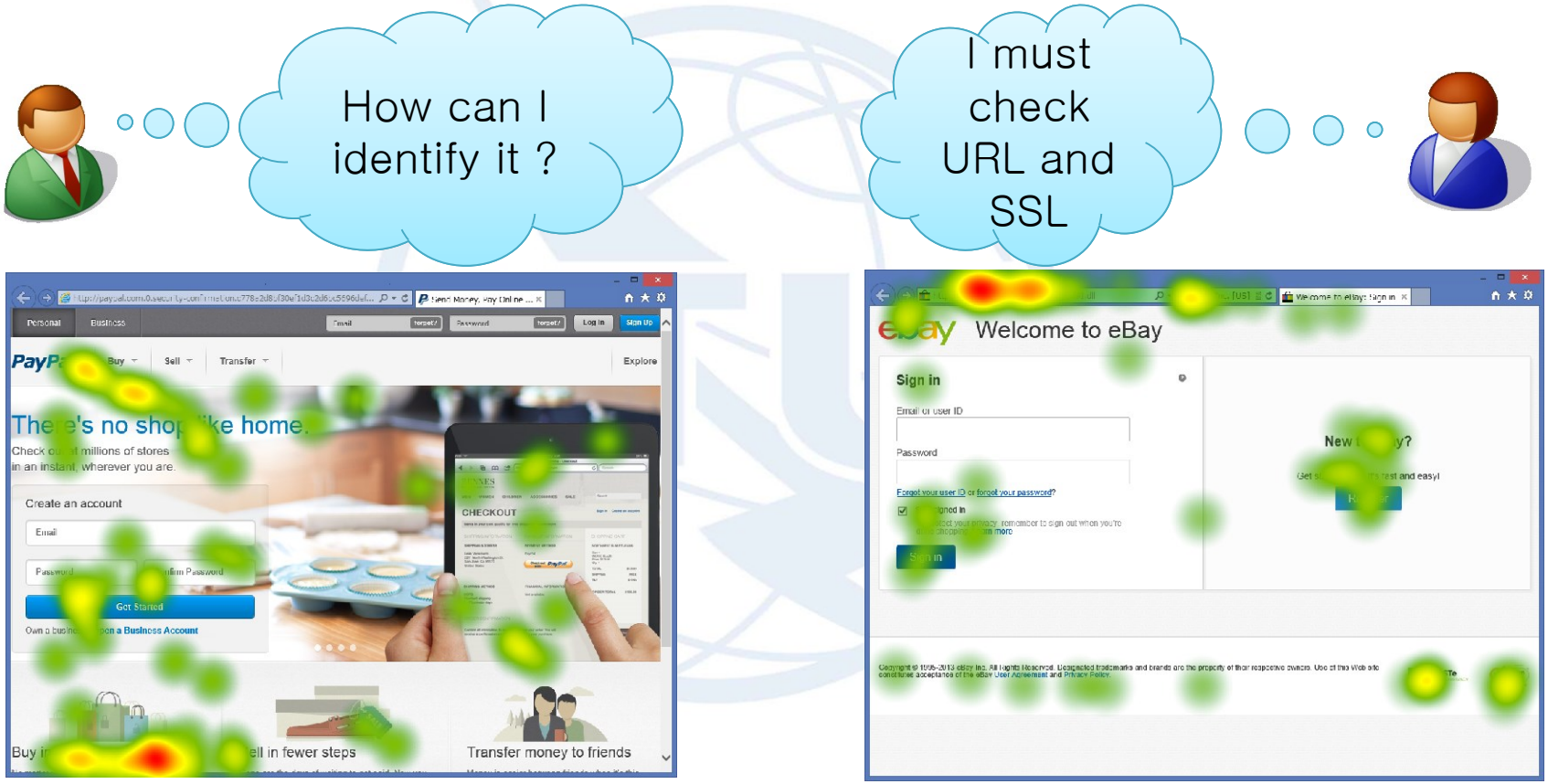


Informational

- To find a particular object of interest
  - with a motivation



Eye movement in phishing sites



(a novice)

(an expert)

Summary of findings (a case of eye movement)

- Fixation time and count in the address bar are good parameters.
- Legacy padlock icons tends to be ignored.

- Color green has slightly meanings.
  - "Why is it green ?" can be identified by analyzing other areas.
  - "This color is green" does not require eye-fixation

Conclusion

- Trust for ICT users
  - Threat target is ICT users, rather than ICT systems
- Support decision making
  - Improving situation awareness is necessary
  - X.cogent provides considerations about visual/narrative elements, peripheral design, training modes and accessibility
- Cognitive psychology
  - Prediction of ICT users' internal intention will be useful for performing cyber defenses