

LFE Medieninformatik • Tobias Stockinger

Enhancing SSL Awareness in Web Browsers

Abschlussvortrag Bachelorarbeit

Betreuer: Max-Emanuel Maurer

Verantwortlicher Hochschullehrer: Prof. Dr. Hußmann

Datum: 28. 09. 2010





Gliederung

1. Motivation
2. Related Work
3. SSLPersonas
4. User Study
5. Zusammenfassung und Ausblick



Motivation – Problemstellung

- Woran erkennt man eine „sichere“ Web-Seite?
- Was sind SSL Zertifikate?
- Was ist zu tun, wenn ein Problem mit den Zertifikaten besteht?

Ziel:
effektive SSL Visualisierung
+
Umgestaltung von Warnhinweisen

Praktische Umsetzung: Entwicklung eines Firefox Add-Ons

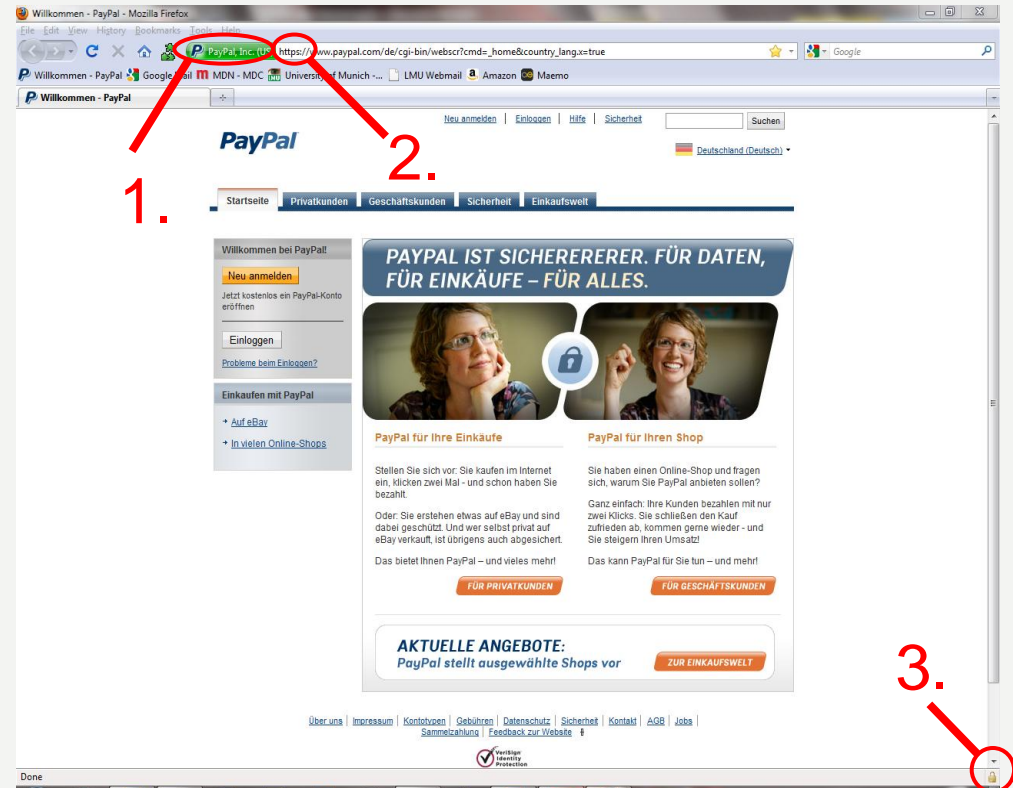
Motivation – Ziele

Sicherheitsindikatoren

Bisherige Indikatoren:

1. Site Identity Button
2. https://
3. Schloss Symbol

Ziel:
Auffälligere Lösung





Motivation – Ziele

Warnmeldungen

Bisher:

Viel Text,
viele Klicks nötig,
generisch

Häufig harmlose Fehler [7]

Ziel:

Habituation vermeiden,
Einfacher gestalten



This Connection is Untrusted

You have asked Firefox to connect securely to **amazon.de**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

▼ Technical Details

amazon.de uses an invalid security certificate.

The certificate is only valid for www.amazon.de

(Error code: ssl_error_bad_cert_domain)

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

[Add Exception...](#)



Related Work – wichtigste Ergebnisse

- Security == sekundäres Ziel (Whitten & Tygar, 1999 - [1])
- Sicherheitsindikatoren ineffektiv (Schechter et al., 2007 - [2])
- SSL Zertifikate und deren Warnungen schwer zu verstehen (Sunshine et al., 2009 - [3])
- Unterscheidung *Content* <> *Browser Chrome* erfolgt oft nicht (Dhamija et al., 2005 - [4])
- Aktive Warnungen effektiver als passive Warnungen (Egelman et al., 2008 - [5])

Related Work – andere Ansätze

Dynamic Security Skins [4]

→ auf Hash Wert basierende Browser Skins

→ Ansatz nicht zu Ende geführt



The screenshot shows a web browser window titled "Credit Card Form" with the URL "https://www.bank.com/creditcard.html". The page content is titled "Credit Card Payment Details... (* required fields)". The form includes the following fields:

- *Full name:
- *Email:
- *Re-enter Email:
- Current Address:
- Logos for VISA and MasterCard.
- *Credit Card Type:
- *Cardholder's Name: (as it appears exactly on your card)
- *Card Number:

The browser's address bar and the top of the page are highlighted with a red and black striped pattern, representing the "Dynamic Security Skin". The status bar at the bottom of the browser window shows "Done".



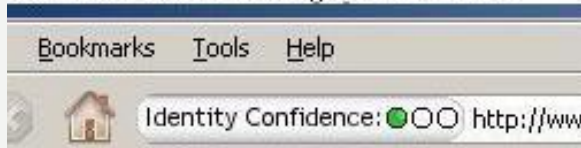
Related Work – andere Ansätze

Identity Confidence Indicator [6],[3]:

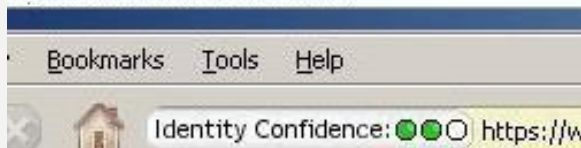
→ Ampel für SSL Zustände

→ Bewusste Trennung zwischen *Privacy* und *Identity*

No certificate or self-signed certificate



Traditional SSL certificate



Extended Validation SSL certificate



Identity Confidence: ●○○ http://standardbank.com

Identity Confidence: Low
This web site has not provided a name for identity confirmation.

Privacy Protected: No
Information sent to and from this web site is vulnerable to eavesdropping.

[More information...](#)

Identity Confidence: ●○○ https://standardbank.com

Identity Confidence: Low
This web site claims to be **standardbank.com** but this has not been confirmed by any authority

Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.

[More information...](#)

Identity Confidence: ●●○ https://standardbank.com

Identity Confidence: Medium
This web site claims to be **standardbank.com** and this has passed *basic* confirmation by **Verisign, Inc.**

Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.

[More information...](#)

Identity Confidence: ●●● https://standardbank.com

Identity Confidence: High
This web site claims to be **Standard Bank Ltd.** and this has passed *extended* confirmation by **Verisign, Inc.**

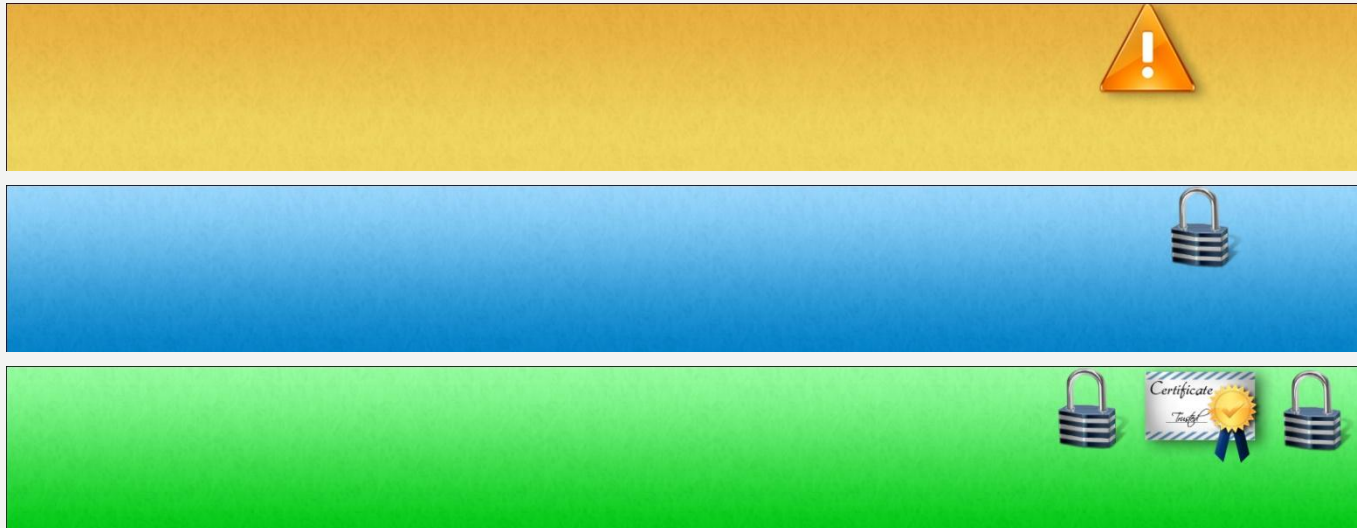
Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.

[More information...](#)

SSLPersonas – Firefox Extension

Personas als Indikatoren

- Persona = LightWeight Browser Theme / Skin
- Gleiches Farbschema wie der Site Identity Button
- Große, auffällige Schloss-, Zertifikat- und Warn-Symbole



SSLPersonas – Firefox Extension

Personas als Indikatoren

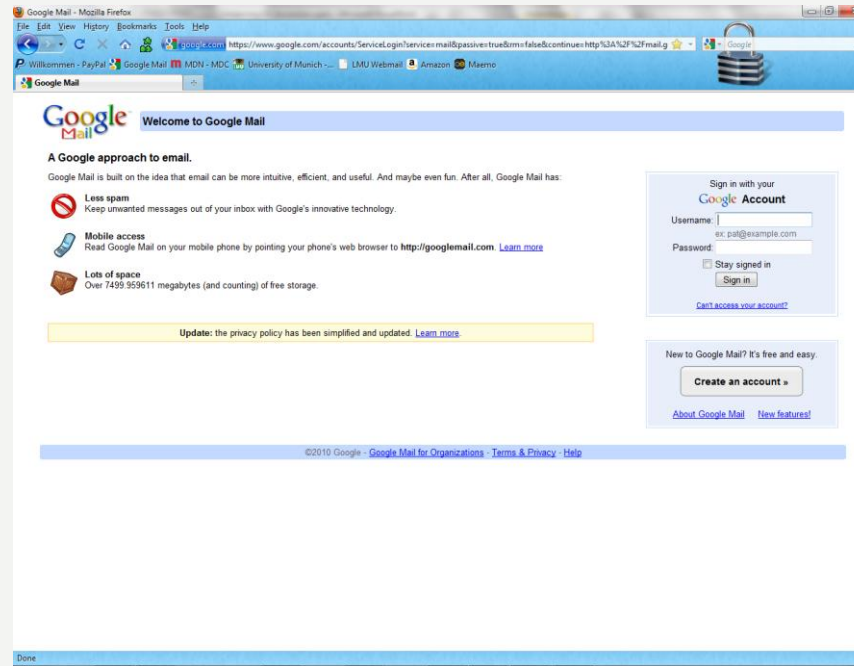
- Zustand 1: Extended Validation SSL Zertifikat (EV)
- Domain und Betreiber der Webseite überprüft



SSLPersonas – Firefox Extension

Personas als Indikatoren

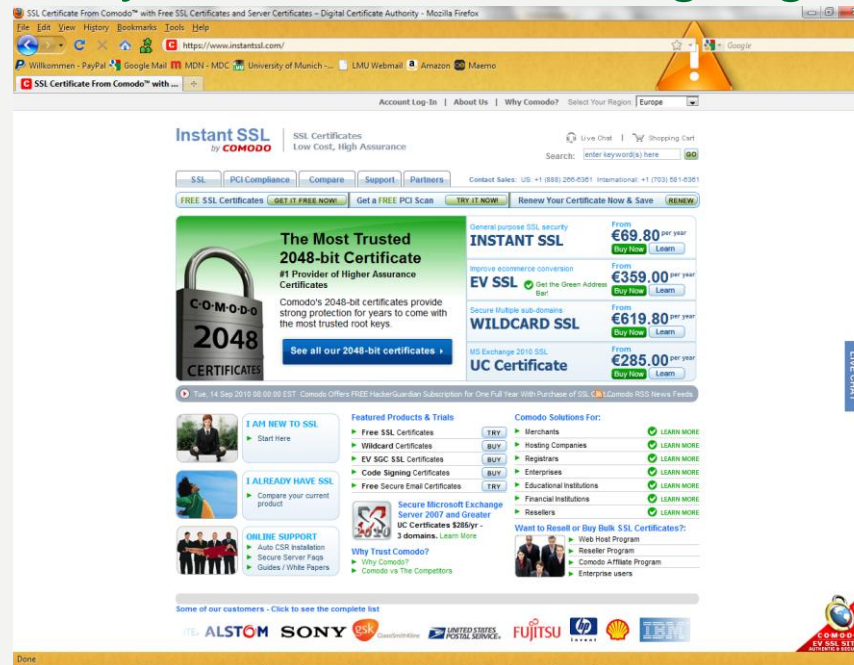
- Zustand 2: Domain Validation SSL Zertifikat (DV)
- Nur Domain verifiziert



SSLPersonas – Firefox Extension

Personas als Indikatoren

- Zustand 3: Nur teilweise verschlüsselte Verbindung
- Häufig durch asynchronen Ladevorgang



The screenshot shows the InstantSSL website by Comodo. The main heading is "InstantSSL by COMODO". Below this, there are several promotional banners and product listings:

- The Most Trusted 2048-bit Certificate:** #1 Provider of Higher Assurance Certificates. Comodo's 2048-bit certificates provide strong protection for years to come with the most trusted root keys. Price: From €69.80 per year.
- EV SSL:** Improve ecommerce conversion. Get the Green Address Bar. Price: From €359.00 per year.
- WILDCARD SSL:** Secure Multiple sub-domains. Price: From €619.80 per year.
- UC Certificate:** MS Exchange 2010 SSL. Price: From €285.00 per year.

There are also sections for "I AM NEW TO SSL", "I ALREADY HAVE SSL", and "ONLINE SUPPORT". The website footer lists several client logos including ALSTOM, SONY, and FUJITSU.



SSLPersonas – Firefox Extension

Personas als Indikatoren

Vorteile:

- **Auffällig** weil ganzer Navigations- und Footer-Bereich eingefärbt werden kann
- LightweightThemes („Personas“) **schnell austauschbar**
- Keine Platzverschwendung (vgl. Toolbars)
- Hoher Grad an Individualisierung
- Natives Browser „Feel“ bleibt erhalten

Nachteil:


Wenig Browser-Chrome → geringere Anzeige-Fläche

SSLPersonas – Firefox Extension

Neues Design der Warnmeldungen

amazon.de kann sich nicht ordnungsgemäß ausweisen.

Seitenvorschau:



Firefox hat versucht **amazon.de** zu erreichen, aber **www.amazon.de** hat geantwortet. Dies kann in manchen Fällen ein Sicherheitsrisiko sein.

Was sollte ich tun?

- Rufen Sie www.amazon.de auf, um das Risiko zu vermeiden und die sichere Seite anzuzeigen.
-

[Weitere Informationen](#)

- Weniger Text, Seitenvorschau, Signalfarben, wechselnde Überschriften
- Klare Empfehlungen, was zu tun ist
- 1-Click Exception: mit einem Klick gelangt man auf die Seite



SSLPersonas – Firefox Extension

LIVE DEMO

aufgerufene Seiten (in verschiedenen Tabs):

<https://www.paypal.com>

<https://www.googlemail.com>

<https://www.one.de/shop/>

<https://amazon.de>



User Study – Überblick

- Between Subjects
- 24 Teilnehmer
- Kein Briefing zur Funktionsweise des Add-On
- 7 Task-Kategorien: EV-SSL, DV-SSL, Partial SSL, No SSL, Domain Mismatch Error, Self-Signed Certificate und Phishing Sites
- Tasks:
 - 14 Lesezeichen anklicken - je zwei Seiten pro Kategorie (eine bekannte und eine unbekante)
 - Anschließend Webseiten bzgl. Sicherheit / Vertrauenswürdigkeit/ Login-Bereitschaft beurteilen
 - Bei Warnungen: Entscheidung treffen



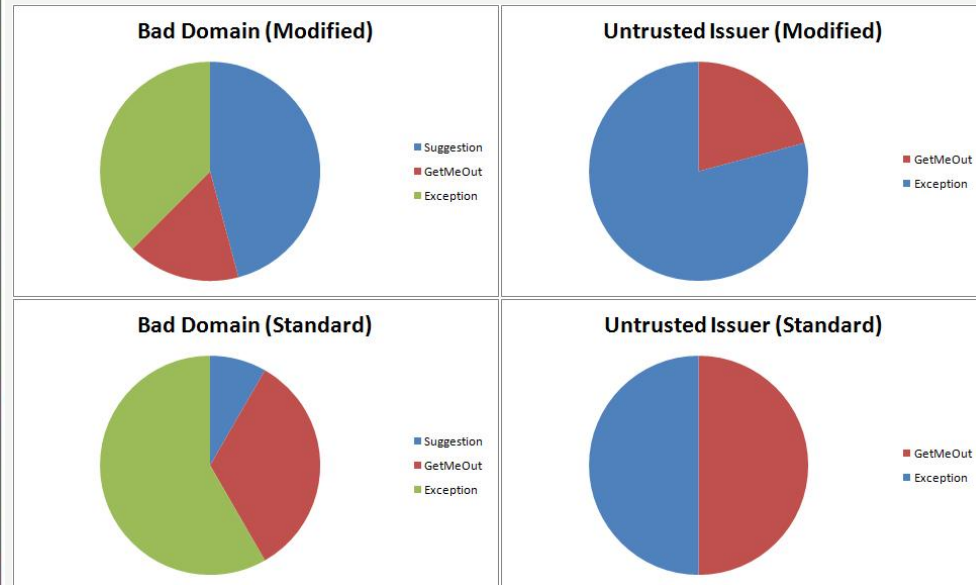
User Study - Hypothesen

- Das grüne und das blaue Persona wirken sich positiv auf die Vertrauenswürdigkeit einer Seite aus (H1)
- Das orange Persona wirkt sich negativ auf die Vertrauenswürdigkeit der Seite aus (H2)
- Wenn kein Persona vorhanden ist, wird die Seite von der Plugin-Gruppe als weniger sicher eingestuft (H3)
- Die angepassten Warnungen führen dazu, dass die Seiten häufiger aufgerufen werden (H4)



User Study - Ergebnisse

	No Plugin	SSLPersonas	Difference
EV Certificate			
Trustfulness	1.13	1.63	0.5
Secure login	0.87	1.16	0.29
Signs for security	0.45	0.96	0.51
DV Certificate			
Trustfulness	0.99	1.42	0.43
Secure login	0.33	0.54	0.21
Signs for security	0	0.63	0.63
Partially Encrypted			
Trustfulness	0.75	-0.21	-0.96
Secure login	0.46	-0.54	-1
Signs for security	-0.04	-0.17	-0.13
Unencrypted			
Trustfulness	0.5	0.29	-0.21
Secure login	0.04	-0.21	-0.25
Signs for security	-0.29	-0.83	-0.54



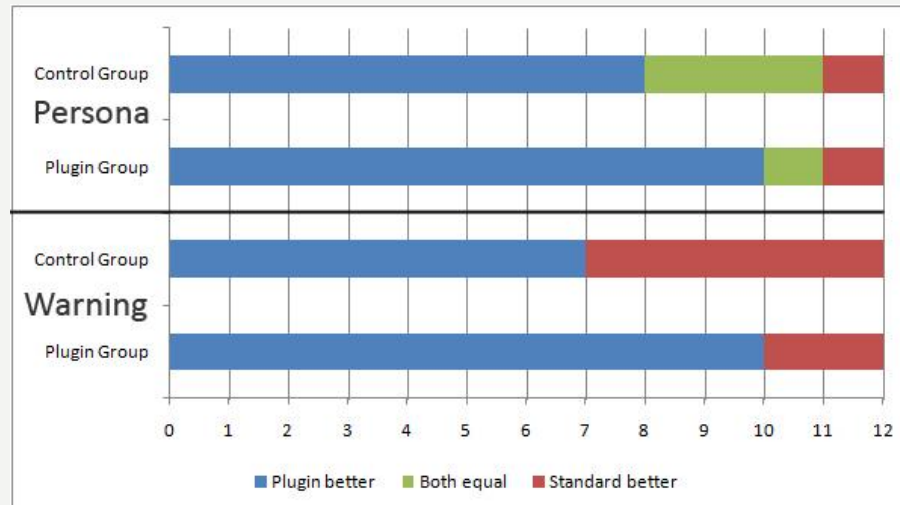
Durchschnittswerte auf einer 5-Punkt Likert Skala (-2 bis +2) // grünes Feld = SSLPersonas besser

Entscheidungen bei Warnmeldungen (rot = falsch)



User Study - Ergebnisse

- Indizien für H1, H2 und H4 vorhanden
- Qualitative Ergebnisse sowie informelles Feedback sprechen deutlicher für SSL Personas
- Design der Warnungen zu bunt / unseriös





Zusammenfassung

- Vermutlich geeignetes Konzept für effektive SSL Visualisierung
- Für den täglichen Gebrauch geeignet → Vorteile überwiegen Nachteile
- Gegen Phishing nur bedingt wirksam
- Umgestaltung der Warnhinweise birgt Potential – aktuelle Fassung jedoch nicht am Optimum



Ausblick

- Verbindung mit Web-of-Trust
- SSLPersonas für andere Browser
- Zusätzliche Flags in SSL Zertifikaten für weitere Personas

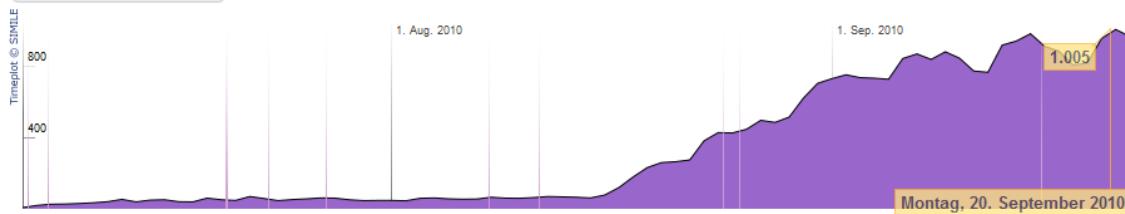


Statistiken für SSLPersonas

[Entwicklerecke](#) | [Statistische Auswertung](#) | [Hilfe](#)

Tägliche Nutzer

Gruppieren nach: Tag

**Downloads insgesamt**
Seit 23. Jun. 2010**5.030****Tägliche Nutzer**
Für Mittwoch, 22. Sep.**966**

twitter

Startseite

**getpersonas**

+ Folgen

List

want your persona to change when you view an encrypted website?
check out SSLPersonas <http://bit.ly/bd3wax>

3:49 AM Aug 24th via CoTweet



Vielen Dank für die Aufmerksamkeit!

SSLPersonas Download:

<https://addons.mozilla.org/de/firefox/addon/183341/>



Quellen

1. WHITTEN, A., AND TYGAR, J. D. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium (Berkeley, CA, USA, 1999), USENIX Association, pp. 14–14.
2. SCHECHTER, S. E., DHAMIJA, R., OZMENT, A., AND FISCHER, I. The emperors new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In In Proceedings of the 2007 IEEE Symposium on Security and Privacy (2007)
3. SUNSHINE, J., EGELMAN, S., ALMUHIMEDI, H., ATRI, N., AND CRANOR, L. F. Crying wolf: An empirical study of SSL warning effectiveness. *usenix security*, 2009
4. DHAMIJA, R., AND TYGAR, J. D. The battle against phishing: Dynamic security skins. In SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security (New York, NY, USA, 2005), ACM, pp. 77–88
5. EGELMAN, S., CRANOR, L. F., AND HONG, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In CHI '08: Proceeding of the twenty sixth annual SIGCHI conference on Human factors in computing systems (New York, NY, USA, 2008), ACM, pp. 1065–1074
6. SOBEY, J., BIDDLE, R., OORSCHOT, P. C., AND PATRICK, A. S. Exploring user reactions to new browser cues for extended validation certificates. In ESORICS '08: Proceedings of the 13th European Symposium on Research in Computer Security (Berlin, Heidelberg, 2008), Springer-Verlag, pp. 411–427
7. HERLEY, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In NSPW '09: Proceedings of the 2009 workshop on New security paradigms workshop (New York, NY, USA, 2009), ACM, pp. 133–144