New trends in Usability of Security

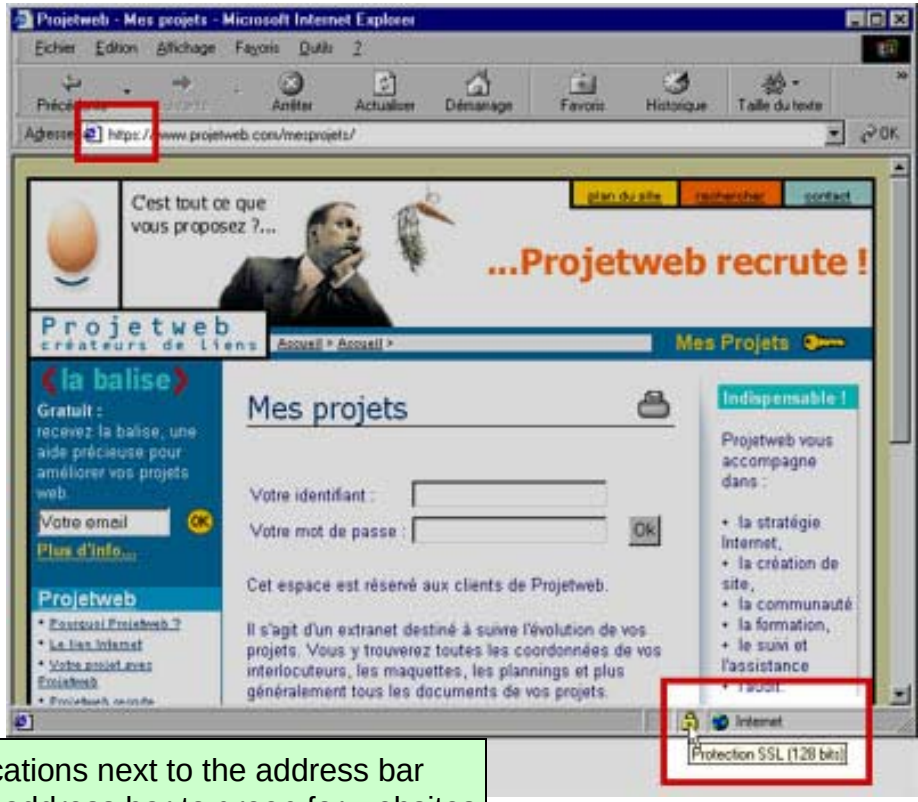
T-110.5220 Usability and Security

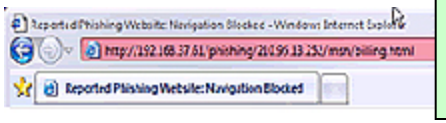
Today's topics

- Security indicators
- Design guidelines for security
- Identity theft & Phishing
- Usability of recommendation systems
- People, Places, Publications in usable sec

Security indicators

- Icons – the lock
- The ”s” in https
- Address bar colour
  - Extended Validation





It displays color-coded notifications next to the address bar in the browser, changing the address bar to green for websites bearing the new certificates, indicating the site owner has completed extensive identity verification checks.

It will also change the address bar to red if the user is on a known phishing website.

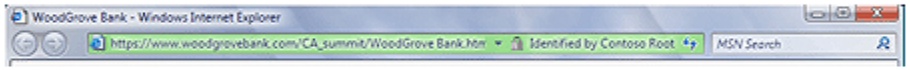
EV SSL certificates will prove particularly useful for companies whose Internet domains are considered at a high risk of being targeted by phishing schemes and other types of Internet fraud. High-risk domains include domains owned by high-profile online financial services, banking sites, auction sites, popular retailers and other sites that conduct Internet transactions with customers that are likely to be targeted by Internet fraud.

Are you ready to own an Extended Validation SSL Certificate? Find out with our Pre-Issuance Readiness Check.

Security Consumers Can See.

All major browsers are integrating new displays to give consumers a way to see a distinct difference between conventionally-vetted sites and sites whose identity has been confirmed by these new EV certificates.

It displays color-coded notifications next to the address bar in the browser, changing the address bar to green for websites bearing the new certificates, indicating the site owner has completed extensive identity verification checks.



It will also change the address bar to red if the user is on a known phishing website.

Getting Your EV Certificates.

Any online business that can demonstrate their business identity according to the extended validation process can receive an EV SSL certificate. The vetting process is more comprehensive than today's vetting standards to prevent phishers and pharmers from getting this highly trusted new EV certificate. This way, consumers can be confident that the site they are connecting to is genuine and safe for transactions.

The new specifications for verifying identities for these new EV SSL certificates were finalized in late 2006. Microsoft Internet Explorer 7 is the first browser to display a distinctive EV signal. In IE7, the address bar turns "trust" green.

Click here to pre-register for information on how you can subscribe to Cybertrust's managed PKI service that gives you the power to issue and manage EV SSL certificates in your community of users. You can also **email** us for more information.

If you are ready to buy a single EV SSL Certificate, **click here**.

Below are the top questions most people have about EV certificates. Please see our complete

:: Extended Validation SSL Certificates

Links

:: Certification Authority/Browser Forum
:: Extended Validation Vetting Process
:: Frequently Asked Questions

Documentation

:: CA/B EV Certificate Guidelines

Related Solutions

:: SSL Certificates
:: Identity Management
:: Security Management Program
:: PCI Compliance

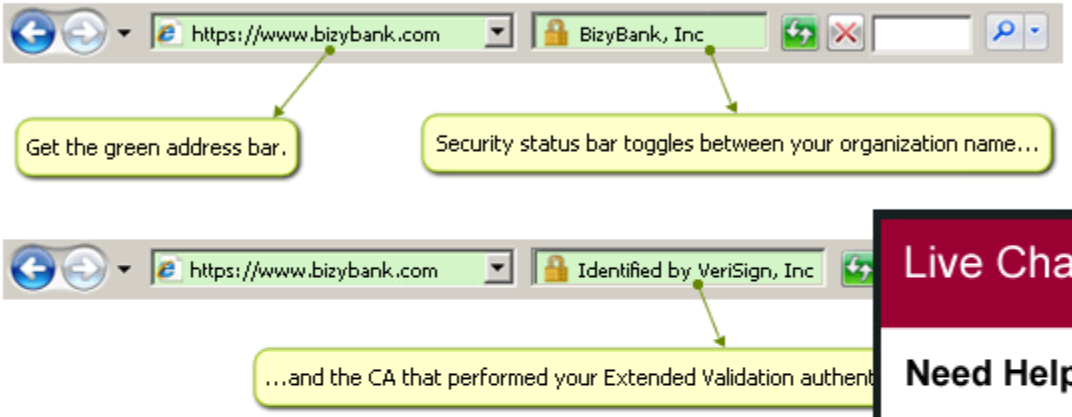
Contact Us

For more information about Cybertrust EV Certificates, e-mail EV@cybertrust.com.
To pre-register to receive an EV certificate when they become available, click here.

What is EV Upgrader™ and how does it work?

What is Extended Validation SSL?

Extended Validation SSL Certificates give high security Web browsers information to clearly identify a Web site's organizational identity. For example, if you use Microsoft® Internet Explorer 7 to go to a Web site secured with an SSL Certificate that meets the Extended Validation Standard, IE7 will cause the URL address bar to turn green. A display next to the green bar will toggle between the organization name listed in the certificate and the Certificate Authority (VeriSign, for example). Older browsers will display Extended Validation SSL Certificates with the same security symbols as existing SSL Certificates.



What is the Extended Validation Standard?

In 2006, a group of leading SSL Certificate Authorities (CAs) and browser vendors approv
for certificate validation and display called the Extended Validation Standard (known during
"High Assurance"). To issue an SSL Certificate that complies with the standard, a CA must
certificate validation practice and pass a Webtrust audit. The validation process requires th
the certificate applicant's domain ownership and organizational identity, as well as the indiv
employment with the applicant, and authority to obtain the Extended Validation SSL Certifica
Practice Statement outlines our authentication and verification processes.

How will Extended Validation SSL increase consumer confidence?

As people use the Web for commerce, business, and social activities, they share personal and confidential information. High profile incidents of fraud and phishing scams have made Internet users very concerned about identity theft. Before they enter sensitive data, they want proof that the Web site can be trusted and their information will be encrypted. Without it, they abandon their transaction and do business elsewhere. High security browsers and Extended Validation SSL Certificates provide third-party verification with a visual display that gives consumers confidence and builds trust in e-commerce.

What are the benefits of Extended Validation SSL to Web site owners?

An Extended Validation SSL Certificate helps your visitors complete secure transactions with confidence and puts your organization in a leadership position. If your site has the "green bar" in IE 7 and your competitor's site does not, you appear to be more trusted and more legitimate. That's a competitive advantage in the world of e-commerce. For businesses with a high profile brand, using Extended Validation SSL is the most effective defense against phishing scams. When customers see the green bar and the name of your security vendor,

More >>

SSL Information Center

SSL Security: How It Works

Extended Validation SSL FAQ

5 Ways to Increase Margins

E-Commerce Trust and SSL

SSL Certificates FAQ

Related SSL Resources

More >>

Current SSL Customers

Renew SSL Certificates Now

VERIFY >

ABOUT SSL CERTIFICATES

What goes wrong here

- Dhamija et al
- Users do not notice security indicators!
- Too many colours
- --> becomes confusing
- --> can be easily misused

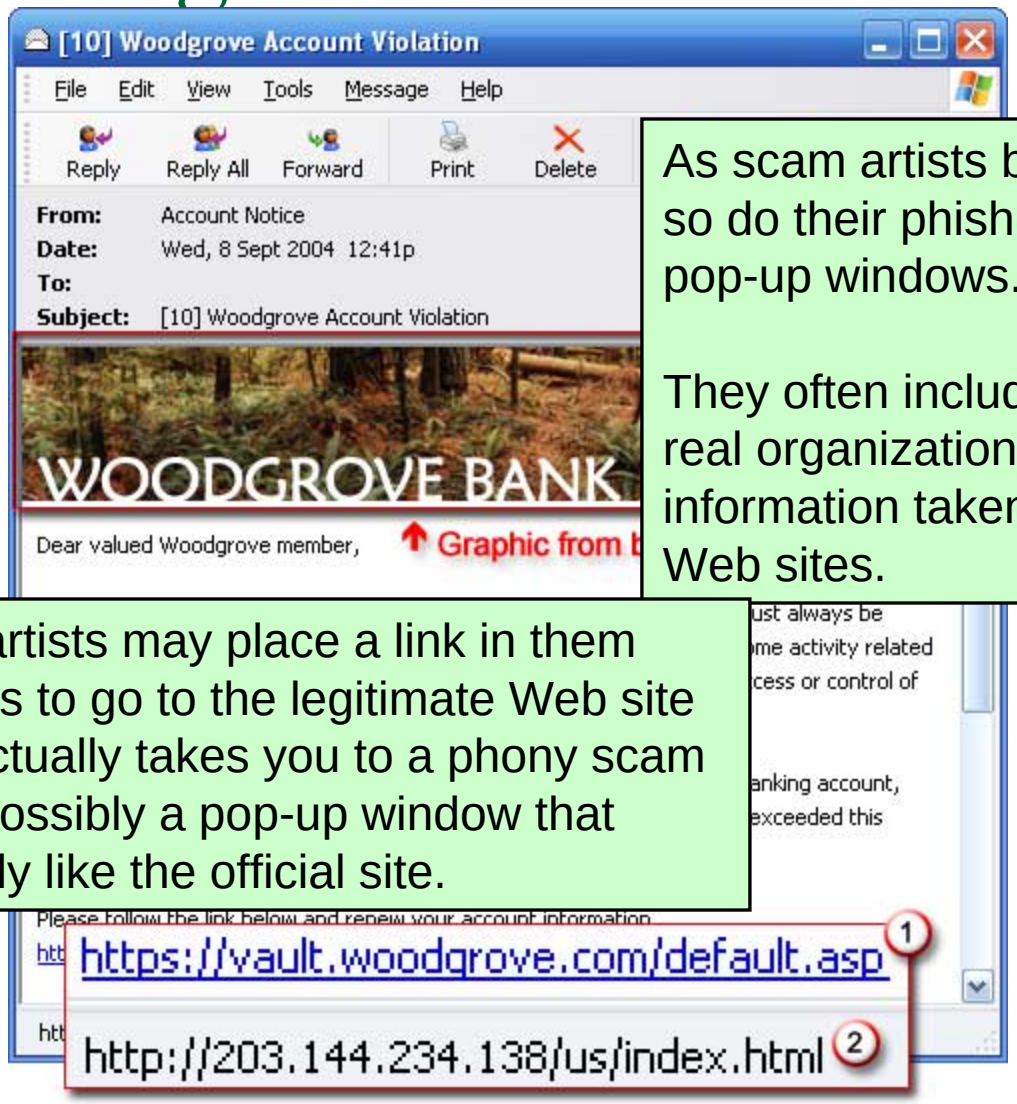
Phishing

- a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.
- difficult to prevent because it preys on the *absence* of resource identification information that is needed for valid trust decisions online
- e.g. websites looking almost identical to the authentic one
  - --> prove that you are who you claim to be
  - = prove that you are innocent = hard

Types of phishing attacks

- fake e-mail
- nearly identical website + web address
- picture-in-picture attacks
- social engineering offline

Phishing e-mail



As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows.

They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites.

The scam artists may place a link in them that appears to go to the legitimate Web site (1), but it actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

Identity theft

- fastest-growing white-collar crime in the United States.
- It happens when someone uses your name, Social Security number, credit card number or some other piece(s) of your personal information to apply for a credit card, make unauthorized purchases, gain access to your bank accounts or obtain loans under your name.
  - http://www.bbbonline.org/idtheft/consumers.asp

Multiple identities, Social networks

- users have multiple identities, associated with multiple social networks that may not overlap
  - e.g. colleagues are used for work-related information sharing only
  - Creates a lot of maintenance work
  - Can cause privacy issues if combined
- Users do not often understand the repercussions of joining and combining the networks
  - Privacy becomes real only when it’s gone
  - Immediate goal (socialising) overrides secondary goal (security, privacy)

Usability of Recommendation Systems

Recommendations by peers on

- films, music, hotels, etc.

How are recommendations used?

→ Currently, textual info reported most used,
visual info most looked at

Improve by:

- ..including more information of the recommenders
- ..enhance visually the important stuff
- ..allow for combining several pieces of info
- ..offer all or a part of info?

Yee's guidelines for usable security

Guidelines for secure interaction design

These 10 design guidelines are based on the actor–ability framework. Readers might find them helpful in designing and evaluating user interfaces for secure systems.

General principles

- *Path of least resistance.* The most natural way to do a task should also be the safest.
- *Appropriate boundaries.* The interface should draw distinctions among objects and actions along boundaries that matter to the user.

Maintaining the actor–ability state

- *Explicit authorization.* A user's authority should only be granted to another actor through an explicit user action understood to imply granting.
- *Visibility.* The interface should let the user easily review any active authority relationships that could affect security decisions.
- *Revocability.* The interface should let the user easily revoke authority that the user has granted, whenever revocation is possible.
- *Expected ability.* The interface should not give the user the impression of having authority that the user does not actually have.

Communicating with the user

- *Trusted path.* The user's communication channel to any entity that manipulates authority on the user's behalf must be unspoofable and free of corruption.
- *Identifiability.* The interface should ensure that identical objects or actions appear identical and that distinct objects or actions appear different.
- *Expressiveness.* The interface should provide enough expressive power to let users easily express security policies that fit their goals.
- *Clarity.* The effect of any authority-manipulating user action should be clearly apparent to the user before the action takes effect.

Some people in usable security

- Ross Anderson (”usec for laymen”)
- Bruce Shneier, www.schneier.com/blog (”usec for techs”)
- Rachna Dhamija (phishing; usec guru)
- Lorrie Faith Cranor (usability of privacy)
- Angela Sasse (”usec for HCI&tech”; usec guru)
- Ka-Ping Yee (Passpet)
- Cynthia Kuo, Adrian Perrig (”usec tech”)
- Jean Camp www.ljean.com (social networks)
- Rebecca Grinter (home networking & usec)
- Jacob Nielsen & Donald Norman (usability for all)

Places for usable security

- SOUPS http://cups.cs.cmu.edu/soups
- USEC http://usablesecurity.com
- ACM SIGCHI http://www.sigchi.org/

Also:

- USENIX Security
- IEEE Security and Privacy
- Financial Cryptography (FC) conference
- etc.

Publications

- No specialized journal in USEC…yet

- CACM
- interactions
- IEEE Security and Privacy
- IEEE Technology
- ACM Transactions (various)
- User Experience magazine by UPA