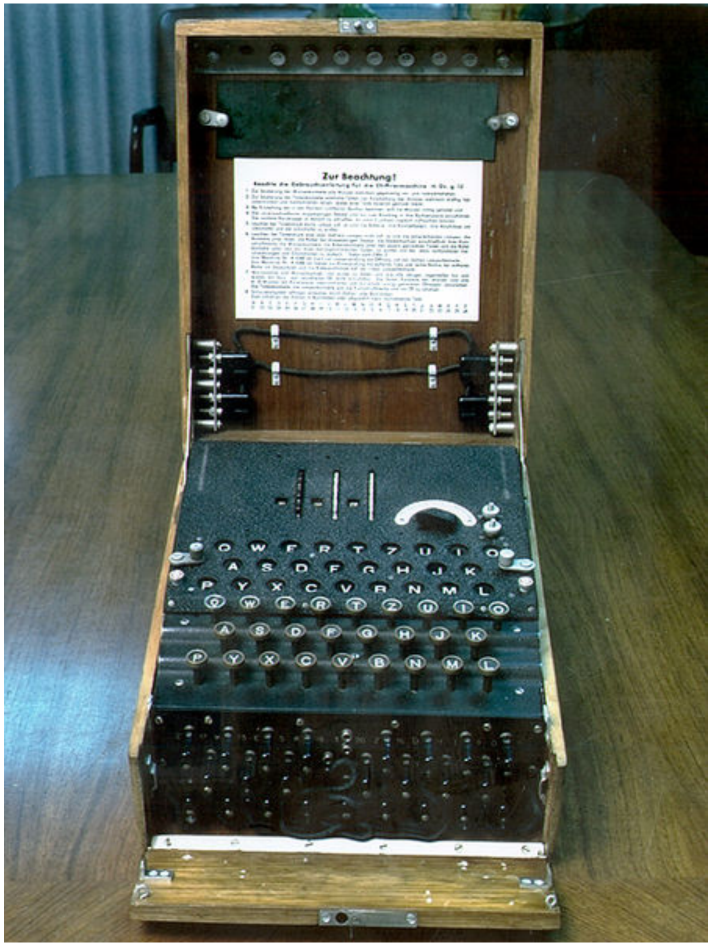
SECURITY AND HUMAN FACTORS

Maritza Johnson

Enigma Machine



Basic Principles of Information Protection

- Psychological acceptability
- Fail-safe defaults (default deny)
- Least privilege
- Separation of privilege
- Least common mechanism
- Complete mediation
- Open design
- Economy of mechanism

J. Saltzer and M. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE* 63:9 (1975), 1278-1308.

PSYCHOLOGICAL ACCEPTABILITY

- Designed for ease of use
- Users can routinely and automatically apply the protection mechanisms correctly
- The user’s mental image of his protection goals must match the mechanisms he must use

J. Saltzer and M. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE* 63:9 (1975), 1278-1308.

USABILITY

- “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of user.” - ISO 9241-11

From Lecture 1: Security Engineering

- Putting the pieces together
- Tradeoffs
- Balancing cost, **security, usability, acceptability**, and more

Security Engineering

- What if a proper balance is not reached?

SECURE BUT NOT USABLE

- A system designed to meet high security goals
- Can the user intentionally subvert your security mechanisms?
- Can they unknowingly influence the effective security?

Usable but Not Secure

- A system designed for usability
- If the result does not match the user’s intentions, the system is not usable
- A compromised machine is not usable
- Will users notice?
- When do users care?

Usability
Security

IT AIN'T EASY

- Unmotivated user
- Abstraction
- Lack of feedback
- Barn door
- Weakest link

A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999.

SECURITY SOFTWARE IS USABLE IF THE PEOPLE WHO ARE EXPECTED TO USE IT:

- Are reliably made aware of the security tasks they need to perform
- Are able to figure out how to successfully perform those tasks

A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999.

SECURITY SOFTWARE IS USABLE IF THE PEOPLE WHO ARE EXPECTED TO USE IT:

- Don’t make dangerous errors
- Are sufficiently comfortable with the interface to continue using it.

A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999.

A Few Usable Security Problems

- Encrypted Email
- Passwords
- Policy Management
- Phishing

ENCRYPTED EMAIL

- When should I use encryption?
- Which recipient key should I use?
- Is this message correctly encrypted?
- How do I differentiate between Public/Private keys?

A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999.

PASSWORDS

- Acceptable to users
- Cheap and easy to deploy
- Minimal maintenance costs

DISADVANTAGES OF PASSWORDS

- Must be memorized
- Must be kept a secret
- Easy to use for multiple accounts
- Very popular
- Existing password policies

Password Reset Mechanisms

- Challenge Questions
- Rely on “shared secrets”
- Effect of information availability

Palin's Hacked Yahoo Account

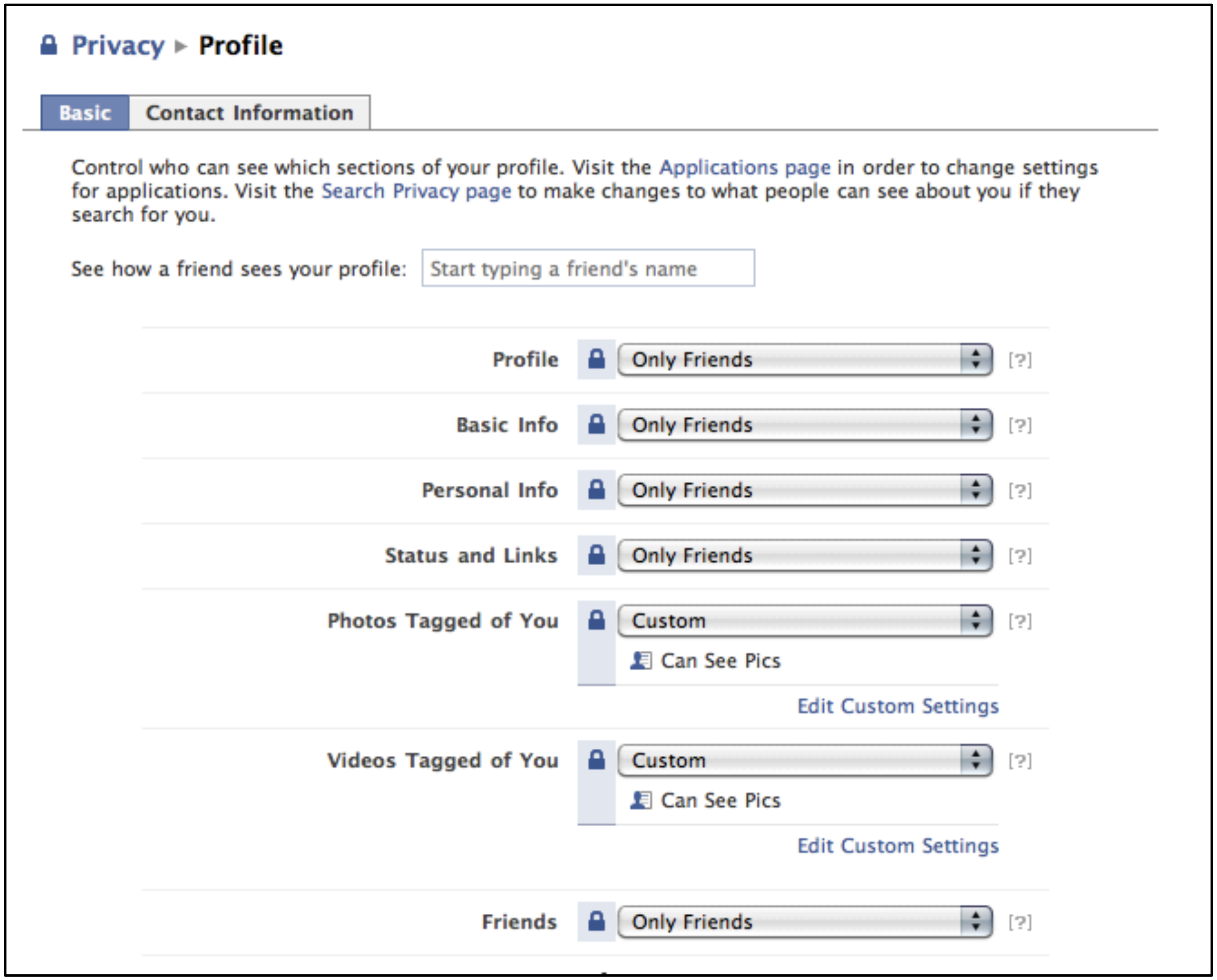
"The hacker guessed that Alaska's governor had met her husband in high school, and knew Palin's date of birth and home Zip code. Using those details, the hacker tricked Yahoo Inc.'s service into assigning a new password, "popcorn," for Palin's e-mail account"

http://www.huffingtonpost.com/2008/09/18/palin-email-hacker-impers_n_127538.html

POLICY MANAGEMENT

- Firewall policy
- Privacy policy
- Access Control
- Privacy settings
- Distributed systems management
- Location-aware devices

POLICY MANAGEMENT



Privacy ▸ Profile

Control who can see which sections of your profile. Visit the Applications page in order to change settings for applications. Visit the Search Privacy page to make changes to what people can see about you if they search for you.

See how a friend sees your profile: Start typing a friend's name

Profile: Only Friends [?]

Basic Info: Only Friends [?]

Personal Info: Only Friends [?]

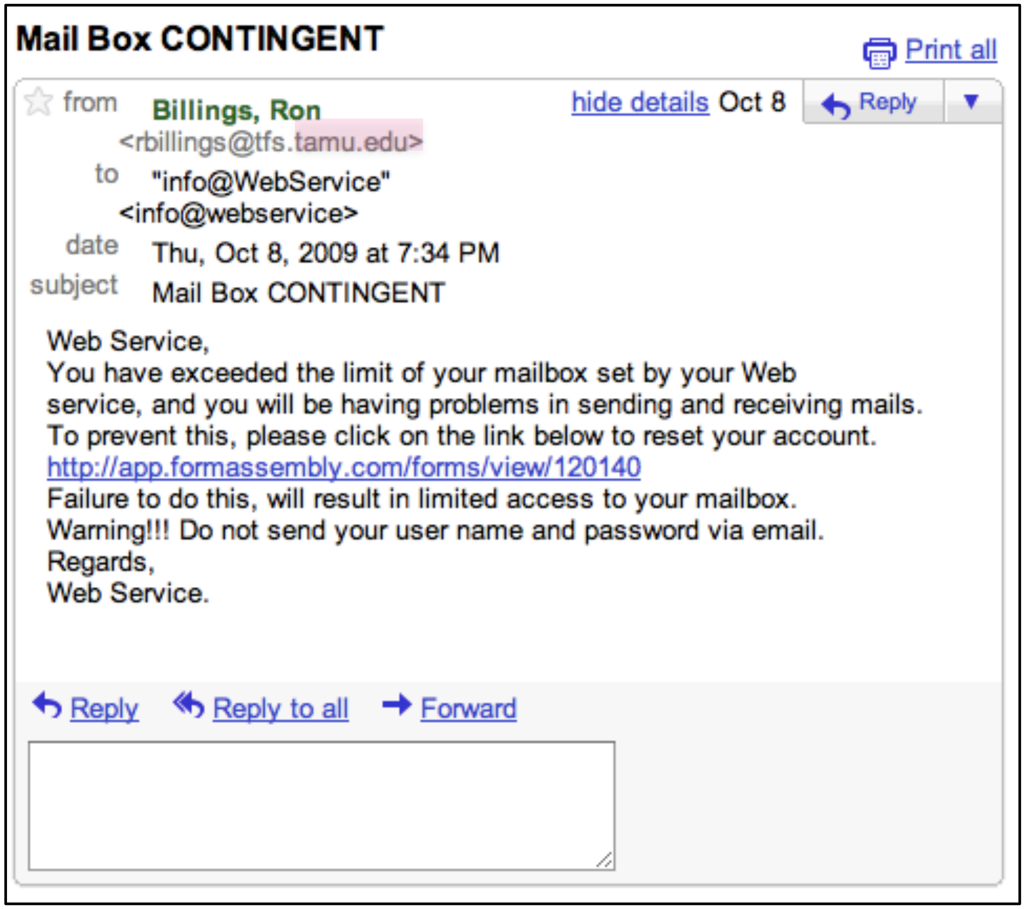
Status and Links: Only Friends [?]

Photos Tagged of You: Custom [?]
Can See Pics
Edit Custom Settings

Videos Tagged of You: Custom [?]
Can See Pics
Edit Custom Settings

Friends: Only Friends [?]

PHISHING



Mail Box CONTINGENT

from Billings, Ron <rbillings@tfs.tamu.edu>

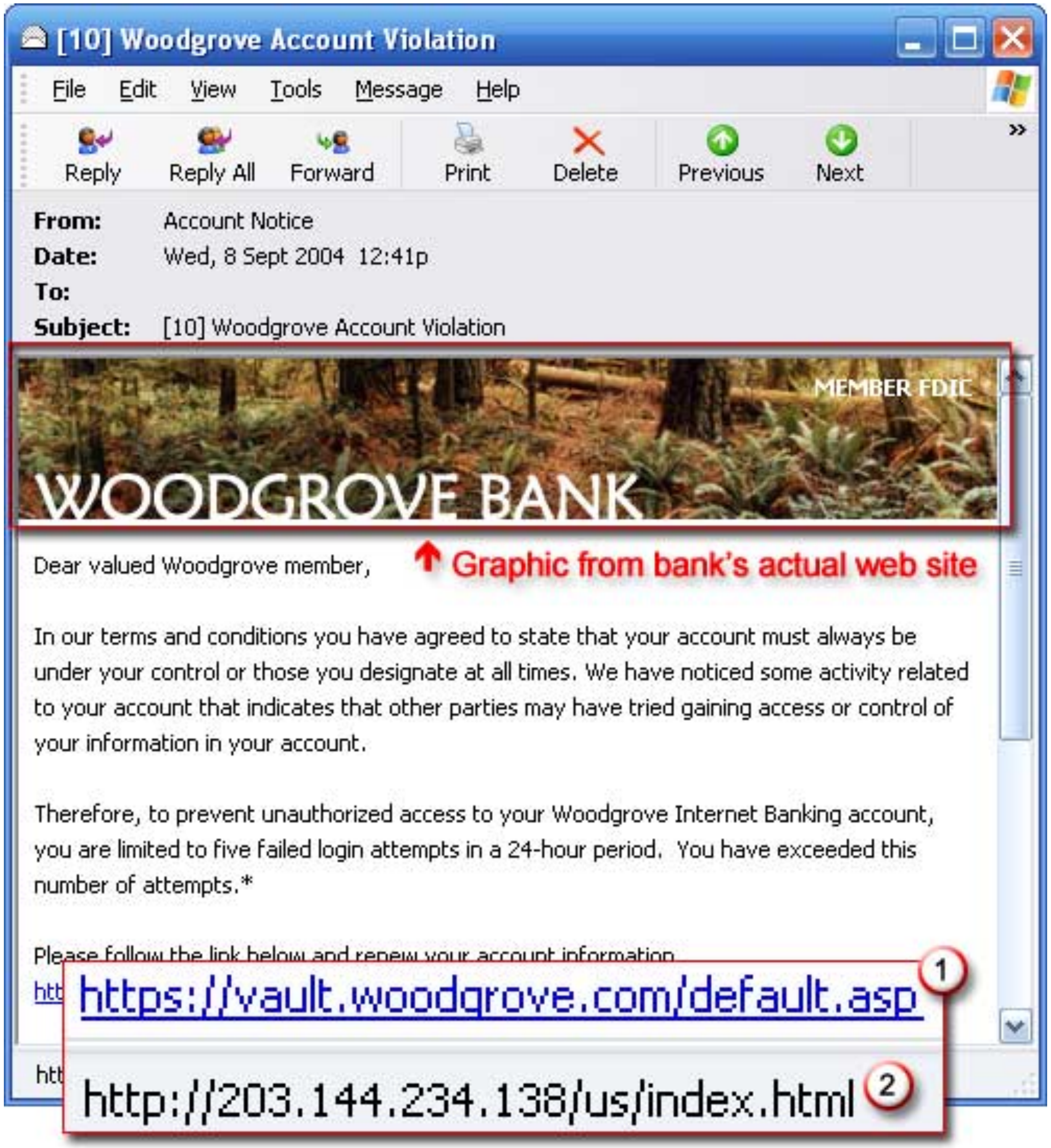
to "info@WebService" <info@webservice>

date Thu, Oct 8, 2009 at 7:34 PM

subject Mail Box CONTINGENT

Web Service,
You have exceeded the limit of your mailbox set by your Web service, and you will be having problems in sending and receiving mails.
To prevent this, please click on the link below to reset your account.
http://app.formassembly.com/forms/view/120140
Failure to do this, will result in limited access to your mailbox.
Warning!!! Do not send your user name and password via email.
Regards,
Web Service.

Better Spam Filters



From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation

Dear valued Woodgrove member,

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information

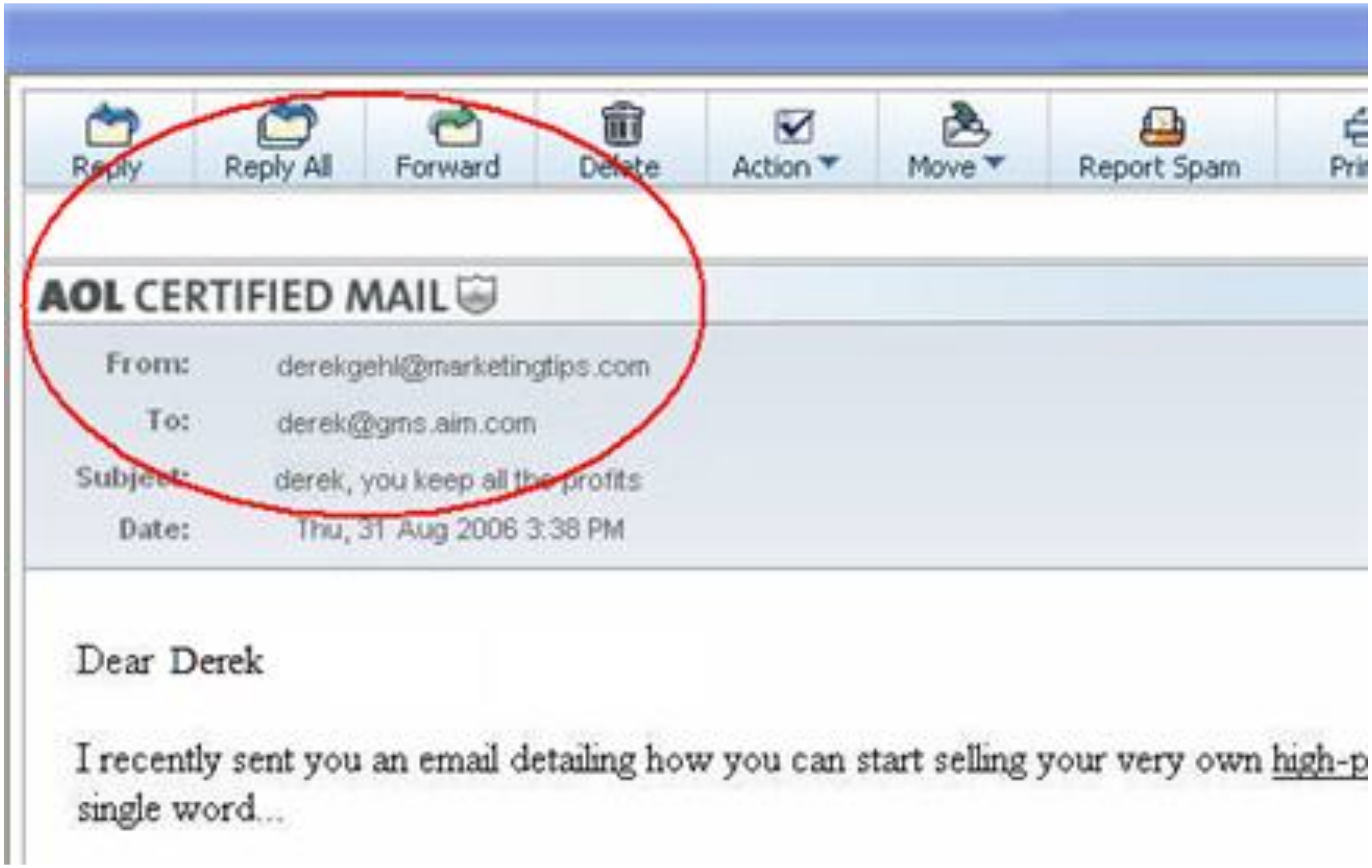
htt

https://vault.woodgrove.com/default.asp

htt

http://203.144.234.138/us/index.html

Authenticate the Email Sender



AOL CERTIFIED MAIL

From: derekgehl@marketingtips.com

To: derek@gms.aim.com

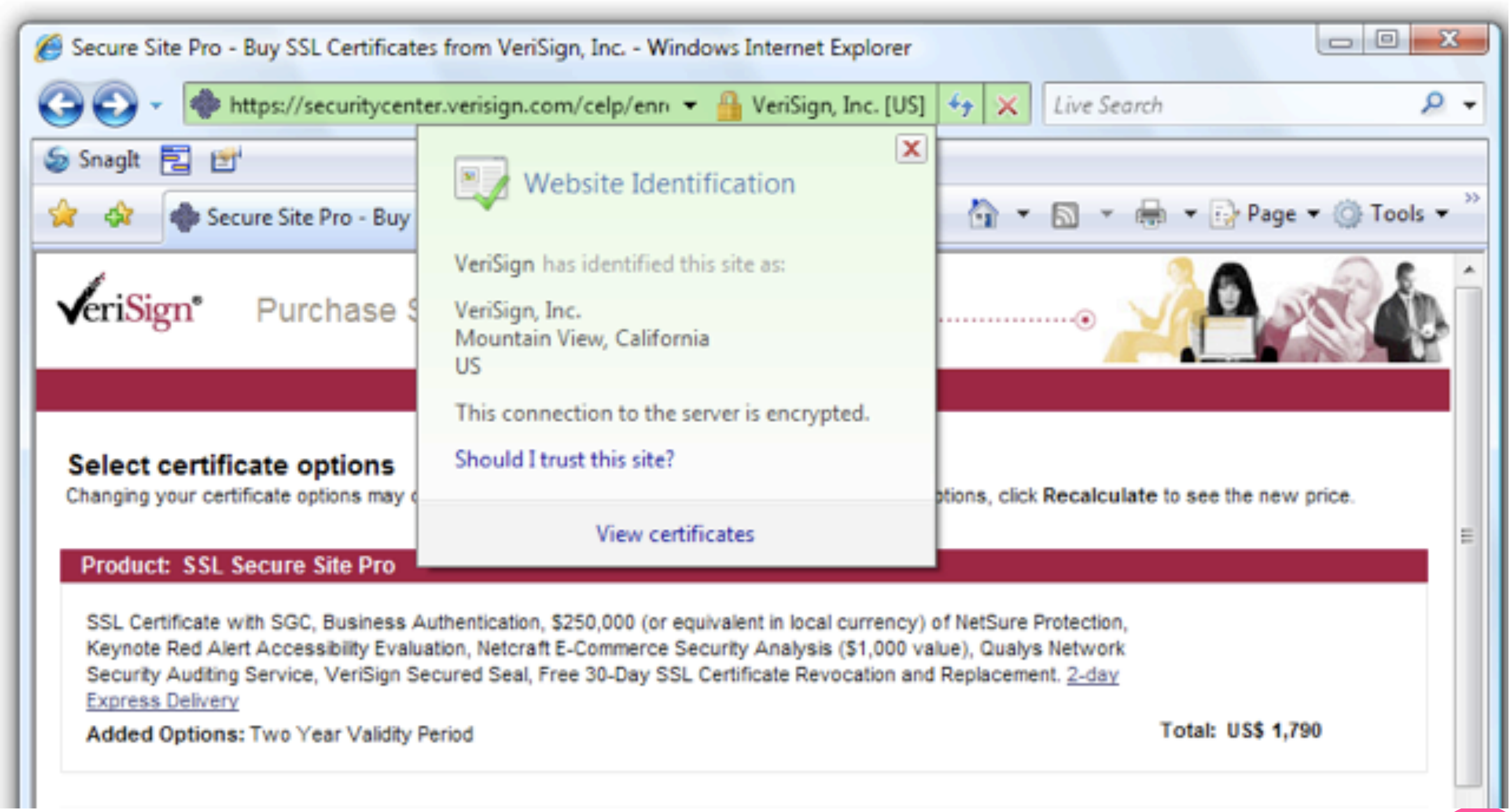
Subject: derek, you keep all the profits

Date: Thu, 31 Aug 2006 3:38 PM

Dear Derek

I recently sent you an email detailing how you can start selling your very own high-p
single word...

WEBSITE AUTHENTICATION



Secure Site Pro - Buy SSL Certificates from VeriSign, Inc. - Windows Internet Explorer

https://securitycenter.verisign.com/celp/enr

VeriSign, Inc. [US]

Website Identification

VeriSign has identified this site as:

VeriSign, Inc.
Mountain View, California
US

This connection to the server is encrypted.

Should I trust this site?

View certificates

Select certificate options

Changing your certificate options may c… …tions, click **Recalculate** to see the new price.

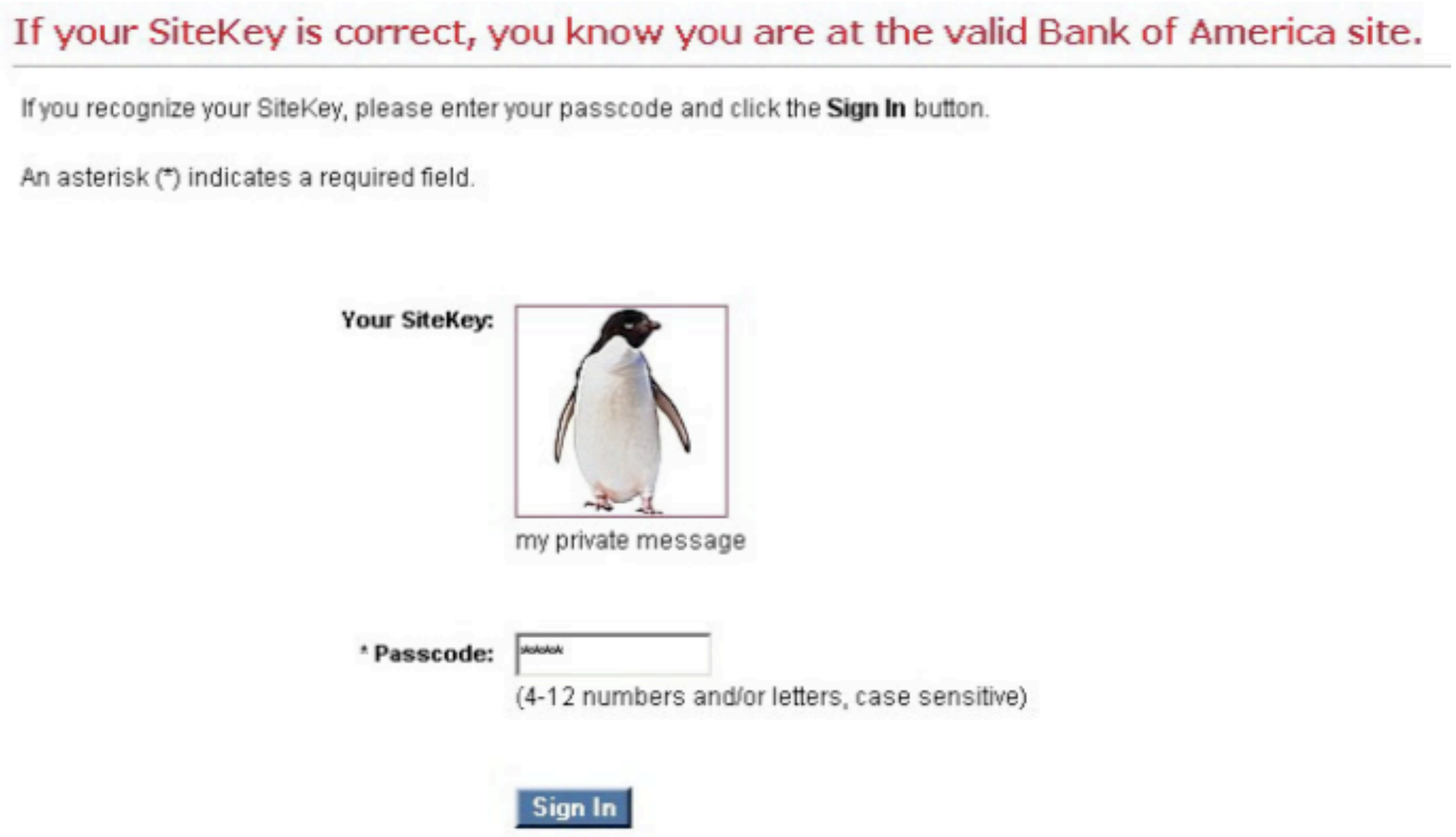
Product: SSL Secure Site Pro

SSL Certificate with SGC, Business Authentication, $250,000 (or equivalent in local currency) of NetSure Protection, Keynote Red Alert Accessibility Evaluation, Netcraft E-Commerce Security Analysis ($1,000 value), Qualys Network Security Auditing Service, VeriSign Secured Seal, Free 30-Day SSL Certificate Revocation and Replacement. 2-day Express Delivery

Added Options: Two Year Validity Period

Total: US$ 1,790

Website Authentication with Shared Secret



If your SiteKey is correct, you know you are at the valid Bank of America site.

If you recognize your SiteKey, please enter your passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

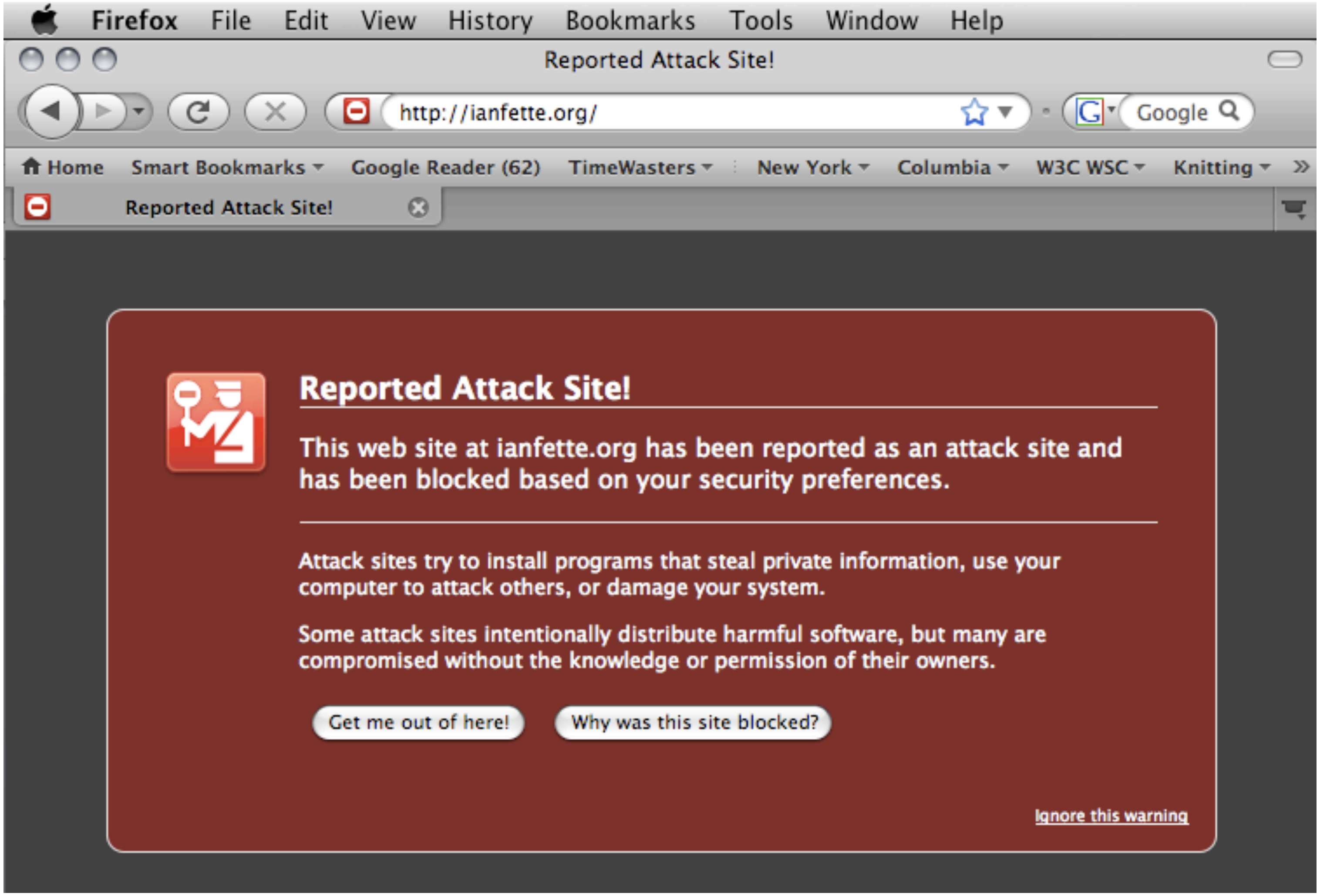
Your SiteKey:

my private message

*** Passcode:** ******

(4-12 numbers and/or letters, case sensitive)

WEBSITE BLACKLISTS



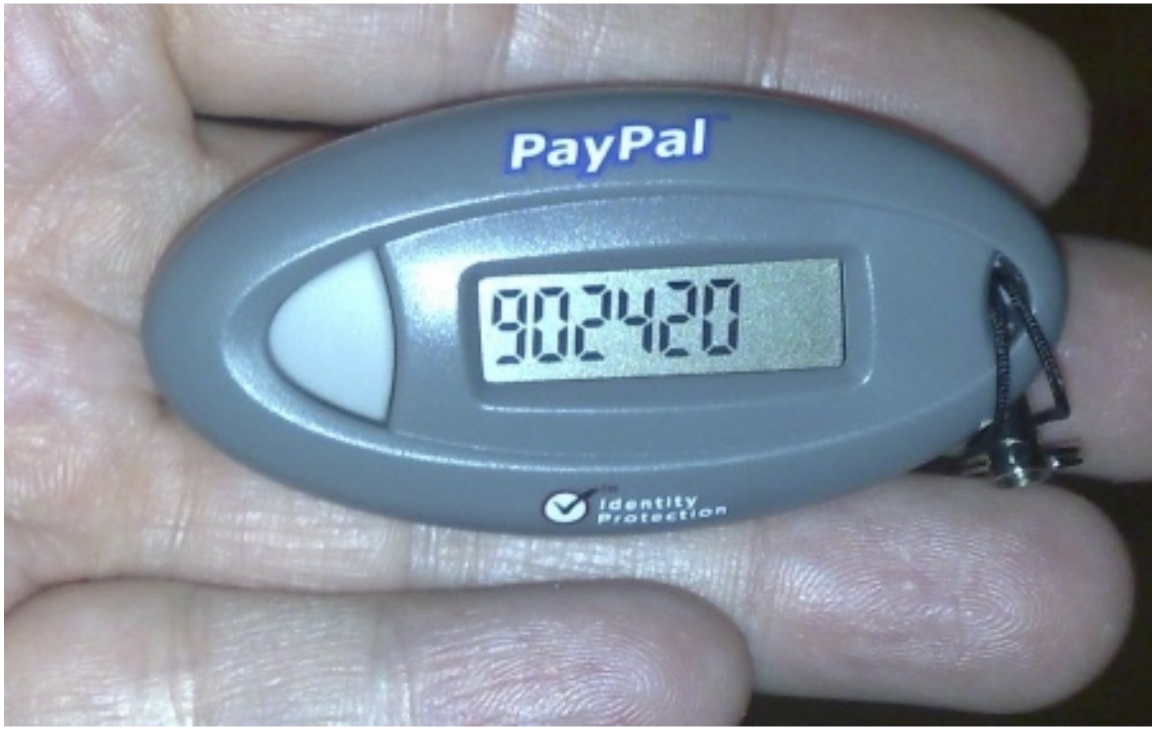
Reported Attack Site!

This web site at ianfette.org has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Hardware Tokens



Designing for Usable Security

- Know your user
  - Role
  - Background
  - Ability
  - Limitations/Handicaps
- Acceptability

Designing for Usable Security

- Know the user goals and tasks
- Consider any environmental factors that may affect their behavior
- Design for robustness against potential attacks
  - Spoofability
  - Information overload
  - Warning fatigue

Designing Warning Messages

- Use a warning appropriate to the situation
- Clearly state the situation in natural language
- Ask the question in context
- Give the user reasonable choices to resolve the issue

GENERAL RULES

- Make the default settings secure
- Use automation when possible
- Don’t “punt” to the user when there’s a problem

Evaluating Security Indicators

- Does it behave correctly when not under attack?
- Does it behave correctly when under attack?
- Can it be spoofed, obscured, or otherwise manipulated?
- Do users notice it?
- Do the users know what it means?
- Do users know what they are supposed to do when they see it?
- Do they actually do it?
- Do they keep doing it over time?
- How does it interact with other indicators that may be installed on a user's computer?

Lorrie Cranor, What do they "indicate?": evaluating security and privacy indicators. interactions, May/June 2006, p. 45-57.

USABILITY TESTING

- If there is a human in the loop usability evaluation is necessary
- Test under real conditions
- Use real users

Early Evaluation

- Low fidelity prototyping
- Expert evaluation
- Cognitive walk-through

Evaluation Methods

- Ethnographic studies
- In-lab studies
- In-the-wild studies

IRB: Institutional Review Board

- A committee that reviews research projects involving human subjects to assure the protection and safety, rights and welfare of research participants (human subjects).
- Informed consent
- http://www.rascal.columbia.edu

Additional Resources

- HCISec Bibliography
  - http://www.gaudior.net/alma/biblio.html
- Usable Security Blog
  - http://usablesecurity.com/
- Symposium on Usable Privacy and Security
  - http://cups.cs.cmu.edu/soups/2009/
- HCI Bibliography
  - http://www.hcibib.org/