Security and Usability

Maritza Johnson

- “Computers are actually easy machines to secure: just turn them off, lock them in a metal-lined room, and throw away the key.”

L. Cranor and S. Garfinkle, “Security and Usability: Designing Secure Systems that People Can Use.”

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.

From Lecture 1: Security Engineering

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

SECURITY ENGINEERING

- What if a balance isn’t achieved?

SECURE BUT NOT USABLE

- The system is shipped with some level of theoretical security
- Can the user subvert your security mechanisms?
- Can the user opt for a more usable but less secure system?

USABLE BUT NOT SECURE

- A system focused on usability
- A compromised machine is not usable
- Reliability or availability might suffer
- Will users notice?

COMPLICATING FACTORS

- The unmotivated user property
- The abstraction property
- The lack of feedback property
- The barn door property
- The weakest link property

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

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.

Encrypted Email

- How does a user know which recipient key to encrypt with?
- Does the user know when to use encryption?
- Does the user know when they have successfully
- Public/Private key use

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
- Low cost to deploy

Disadvantages of Passwords

- User must memorize a string
- Must be kept a secret
- Easy to use for multiple accounts

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

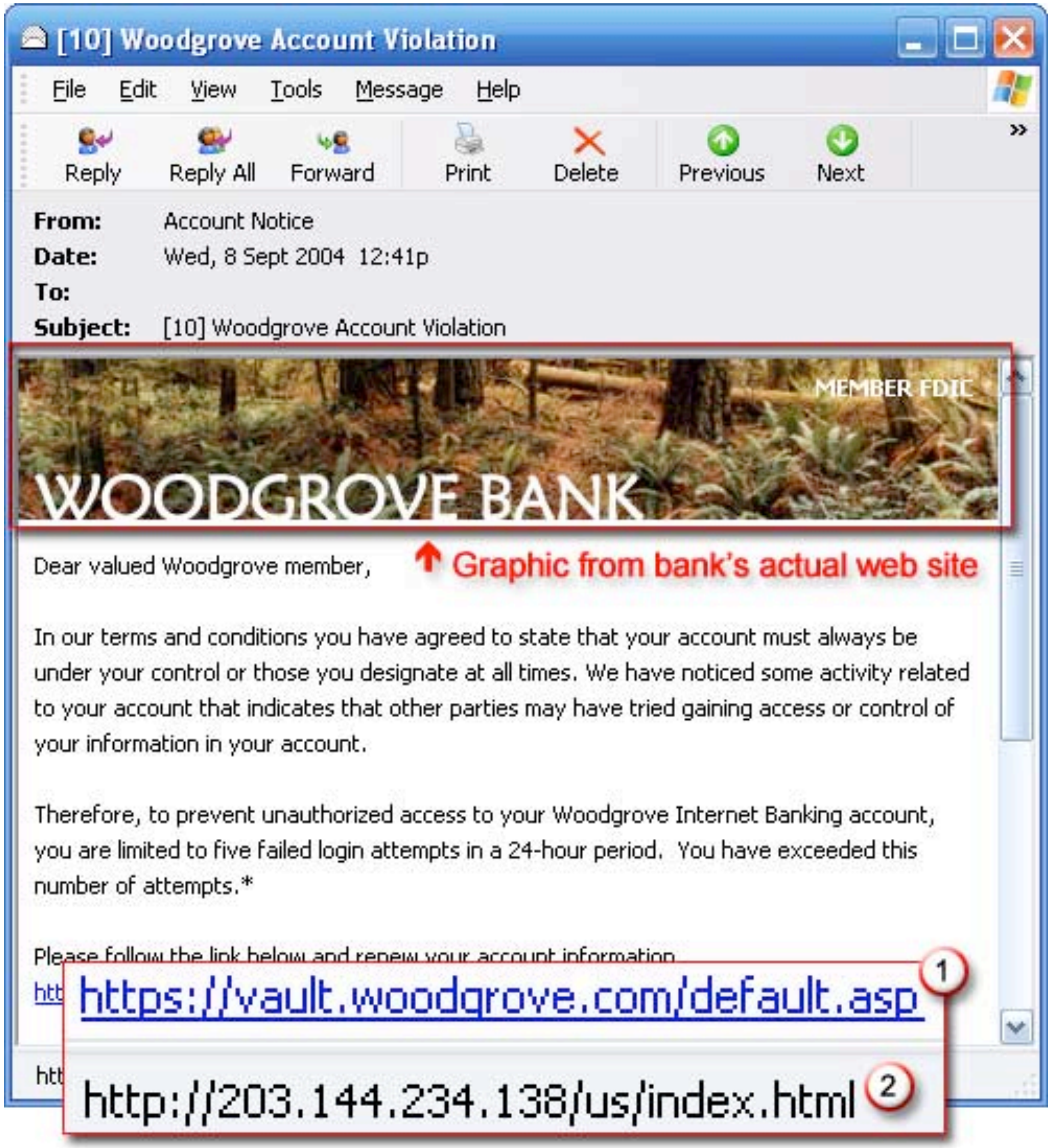
POLICY MANAGEMENT

- How does the user specify the policy?
- How is a change in policy expressed?
- How are multiple policies visualized?
- What about large systems?

PHISHING

- User receives an urgent email with a link
- The link leads them to a spoofed website
- The user is asked for sensitive personal information
- The problem has received a lot of attention
- Major scare factor for average user

PHISHING SOLUTION: BETTER SPAM FILTERS



From: Account Notice

Date: Wed, 8 Sept 2004 12:41p

To:

Subject: [10] Woodgrove Account Violation

Graphic from bank's actual web site

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.

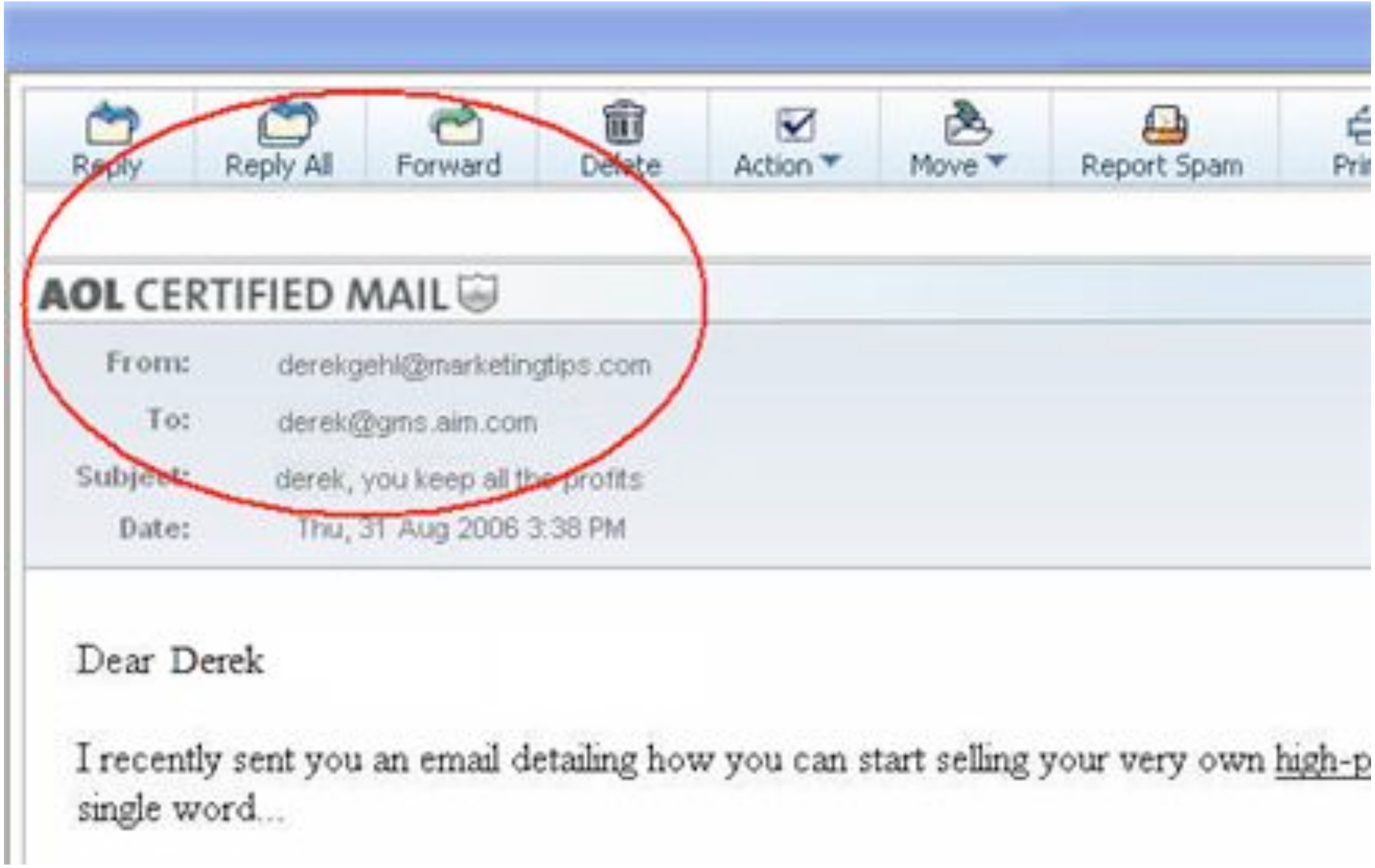
Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information.

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

http://203.144.234.138/us/index.html

Phishing Solution: Authenticate the Email Sender



AOL CERTIFIED MAIL

From: derekgehl@marketingtips.com

To: derek@gms.aim.com

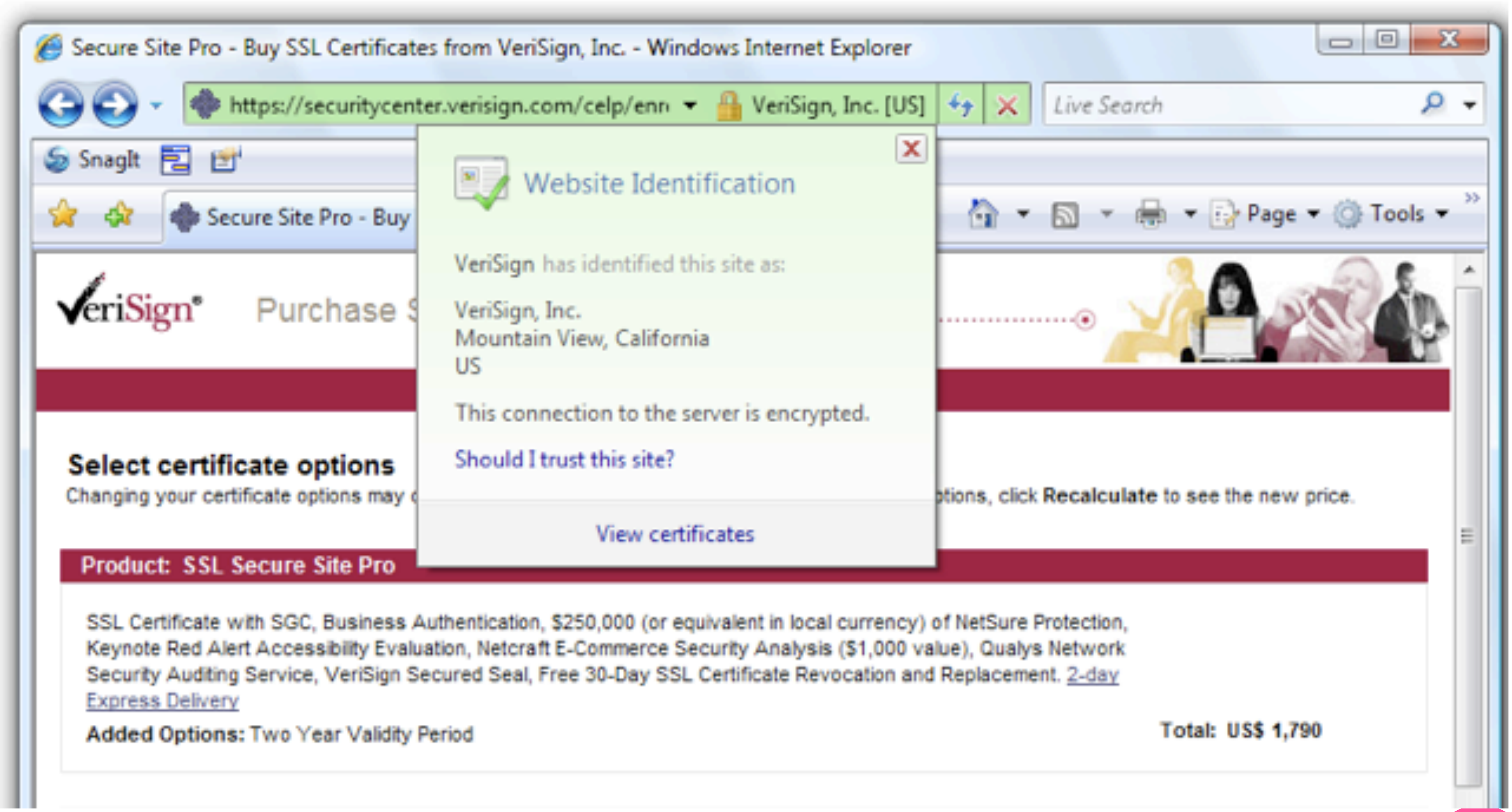
Subject: derek, you keep all the profits

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...

PHISHING SOLUTION: 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 ... ptions, click **Recalculate** to see the new price.

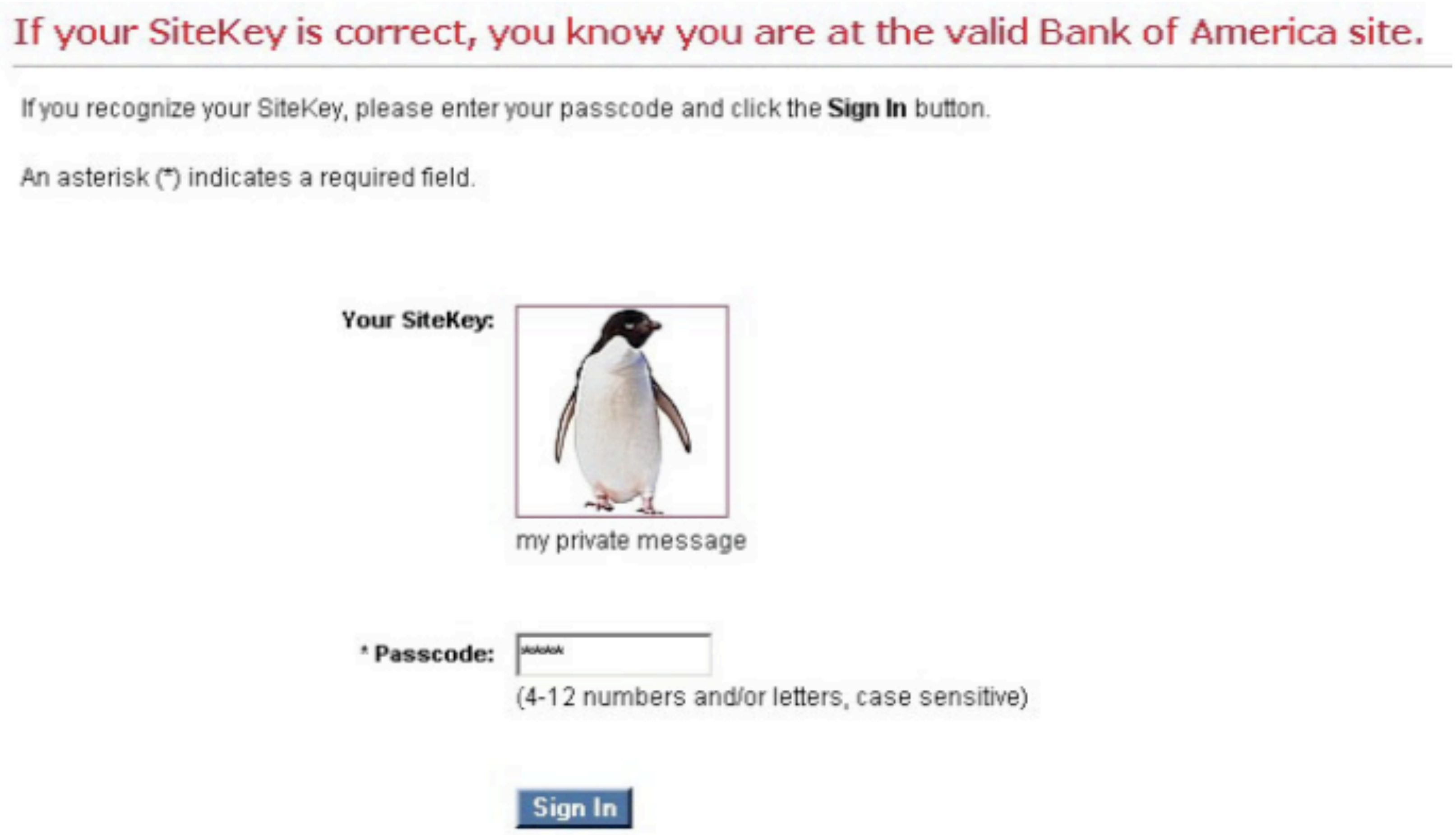
Product: SSL Secure Site Pro

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

Phishing Solution: Website Authentication



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.

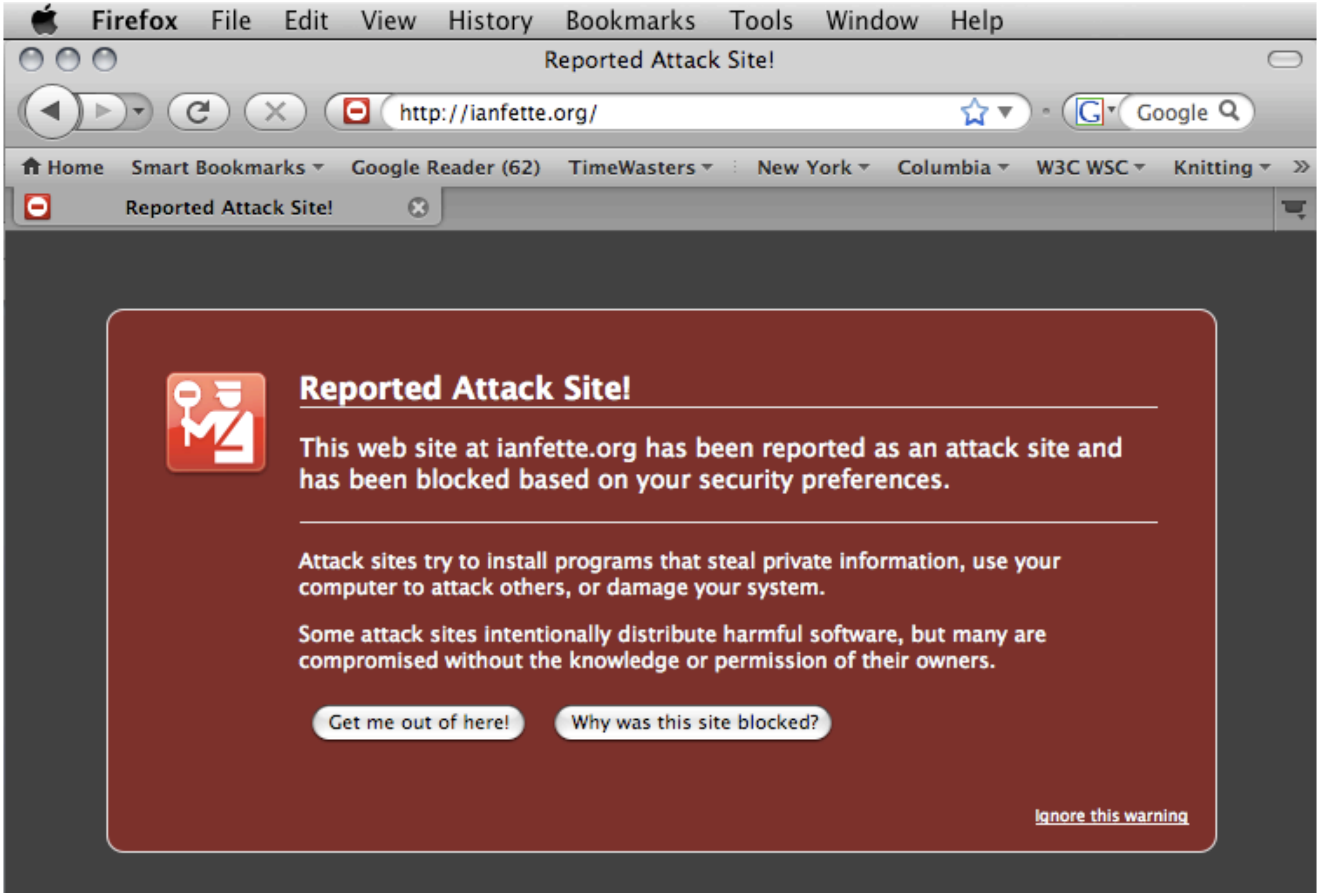
Your SiteKey:

my private message

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

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

Phishing Solution: Website Blacklists



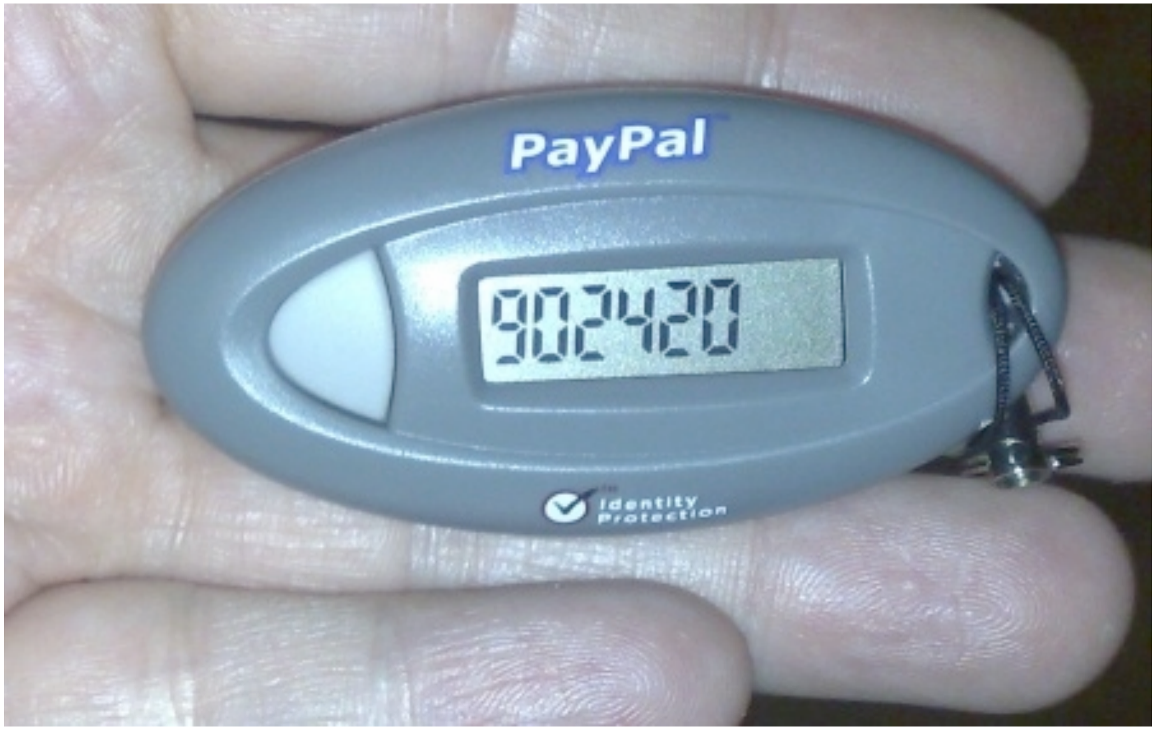
Reported Attack Site!

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.

Phishing Solution: Hardware



COMMON PROBLEM: MENTAL MODEL MISMATCH

- If the user’s mental model of the system doesn’t match the system model, vulnerabilities will exist
- Can metaphors bridge this gap?

Designing for Usable Security

- Know the 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
- Accessibility
- Design for robustness against potential attacks
  - Spoofability
  - Information overload

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

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

Designing Security Indicators

- Does the indicator behave correctly when not under attack
- Does the indicator behave correctly when under attack?
- Can the indicator be spoofed, obscured, or otherwise manipulated?
- Do users notice the indicator?
- Do the users know what the indicator means?
- Do users know what they are supposed to do when they see the indicator?
- Do they actually do it?
- Do they keep doing it?
- How does the indicator 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.

- If there is a human in the loop, usability evaluation is necessary
- Your user probably doesn’t have your level of technical expertise

EVALUATING USABLE SECURITY

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

Evaluating Usable Security

- 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/