Crying Wolf: An Empirical Study of SSL Warning Effectiveness

Joshua Sunshine
Serge Egelman
Hazim Almuhimedi
Neha Atri
Lorrie Faith Cranor

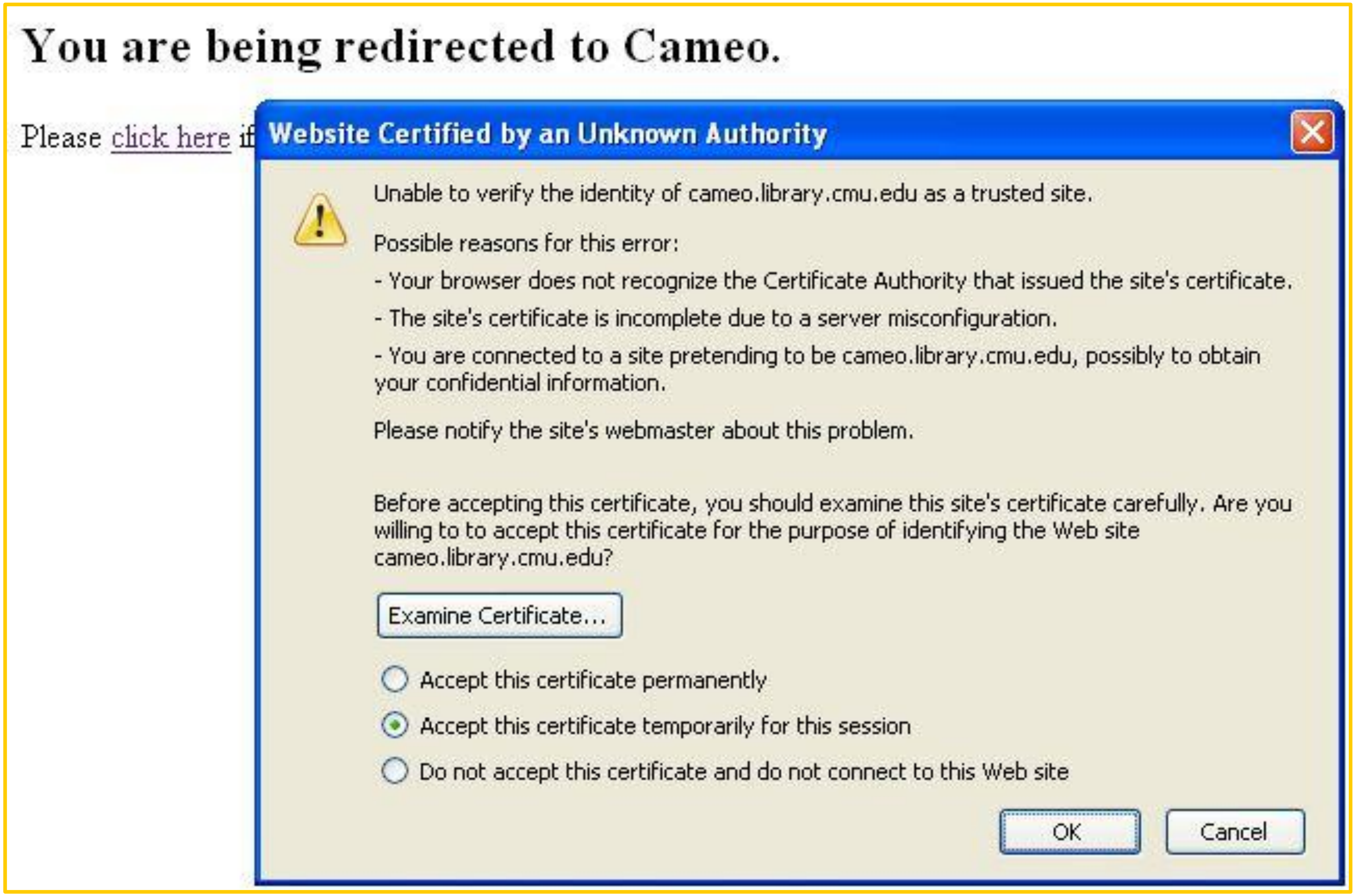
Carnegie Mellon

CyLab Usable Privacy and Security Laboratory
http://cups.cs.cmu.edu/

SSL Certificate Warnings

- Browser's warn about SSL Cert problems:
  - Domain Mismatch
  - Unknown Certificate Authority
  - Expired
- These warnings:
  - May be user's only protection
  - Commonly encountered when connecting to legitimate servers

FF2 Warning



You are being redirected to Cameo.

Please click here if

Website Certified by an Unknown Authority

Unable to verify the identity of cameo.library.cmu.edu as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be cameo.library.cmu.edu, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

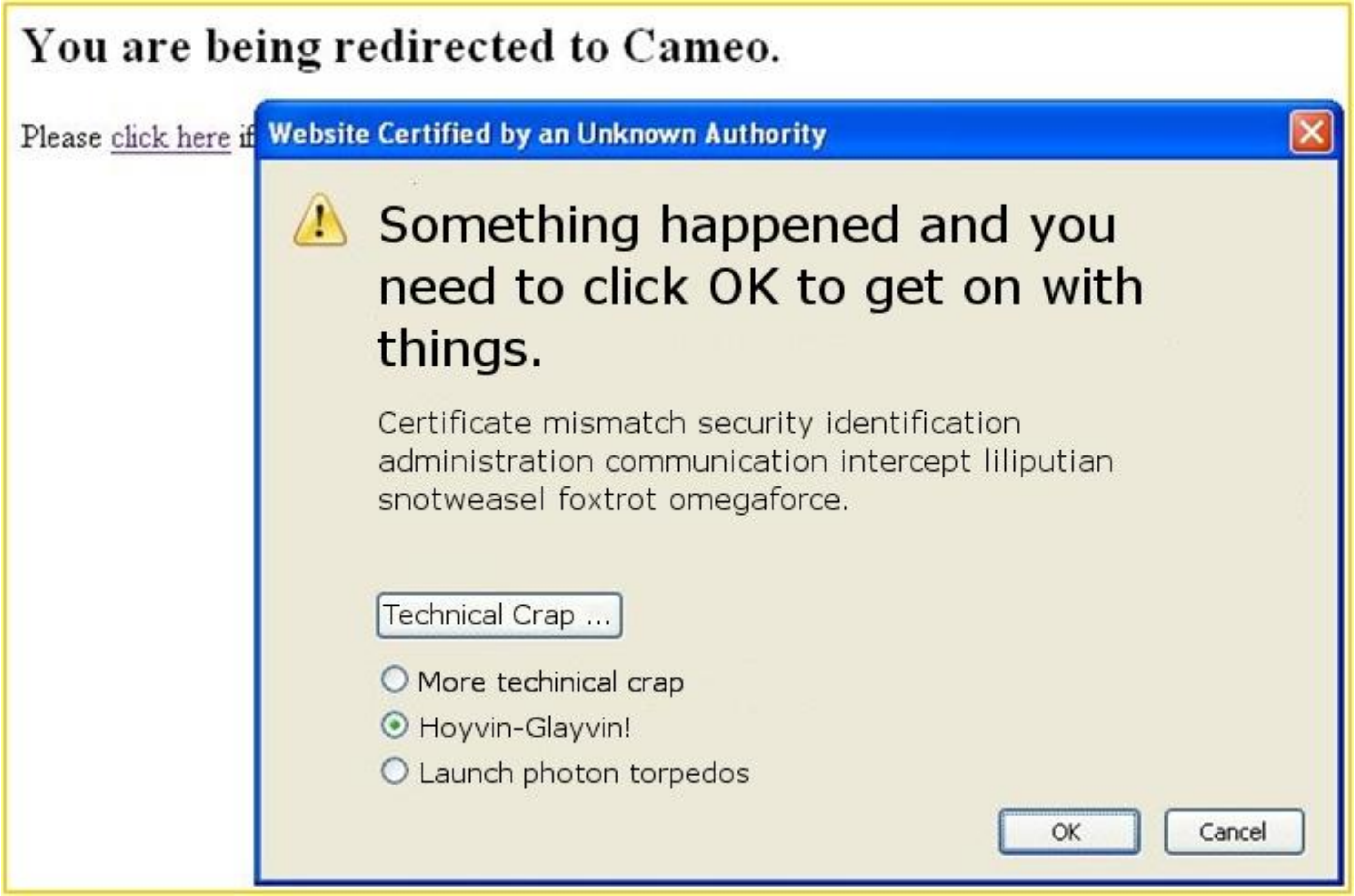
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site cameo.library.cmu.edu?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

FF2 Warning



You are being redirected to Cameo.

Please click here if

Website Certified by an Unknown Authority

Something happened and you need to click OK to get on with things.

Certificate mismatch security identification administration communication intercept liliputian snotweasel foxtrot omegaforce.

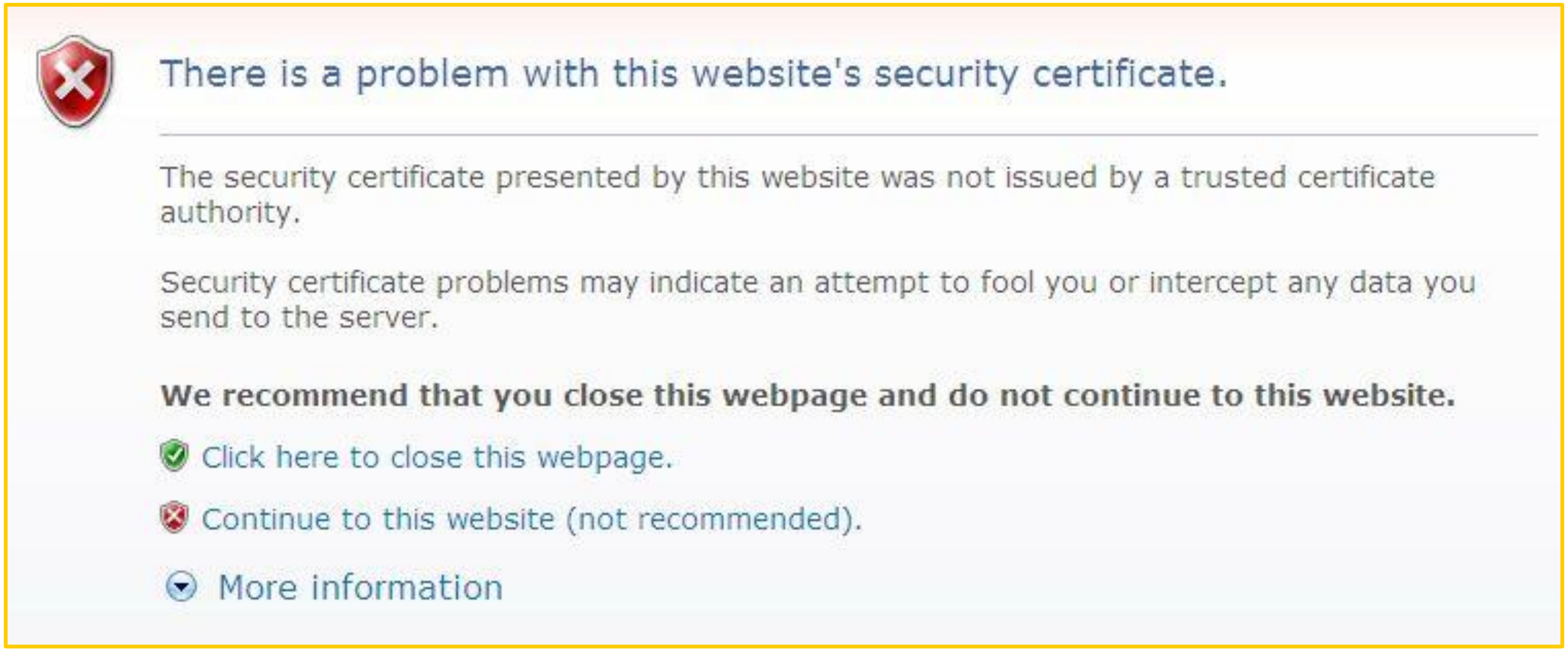
○ More techinical crap

● Hoyvin-Glayvin!

○ Launch photon torpedos

Adapted from Jonathan Nightingale

IE7 Warning



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

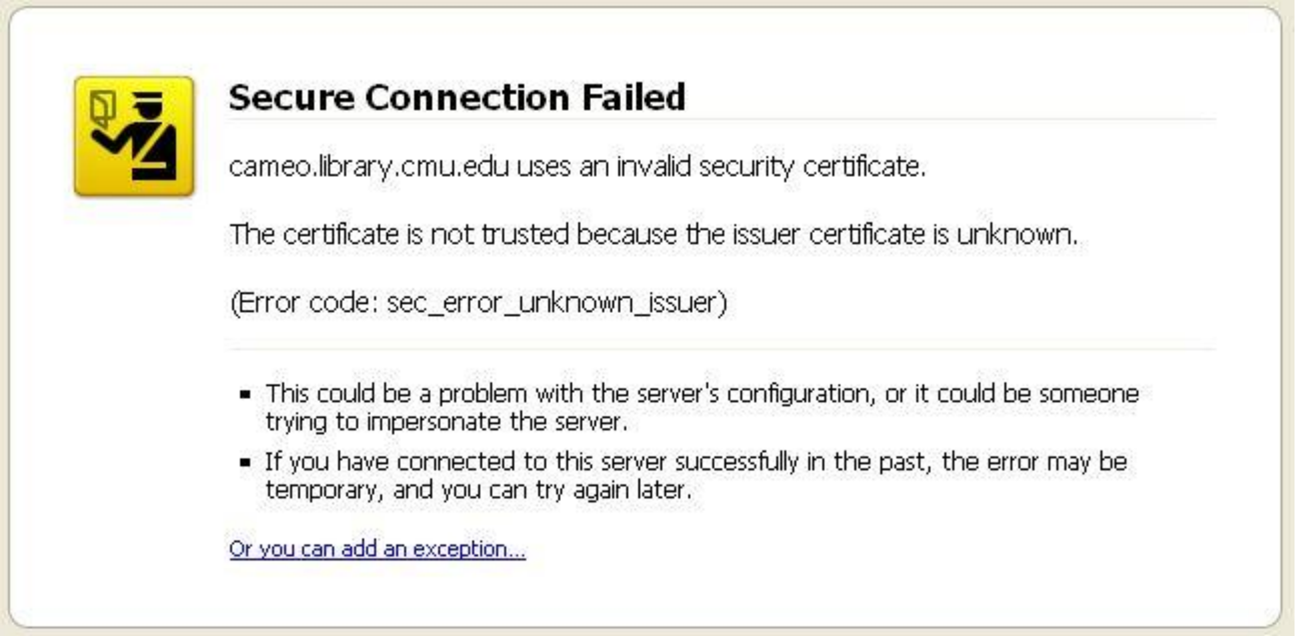
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

✓ Click here to close this webpage.

☒ Continue to this website (not recommended).

FF3 Warning



Secure Connection Failed

cameo.library.cmu.edu uses an invalid security certificate.

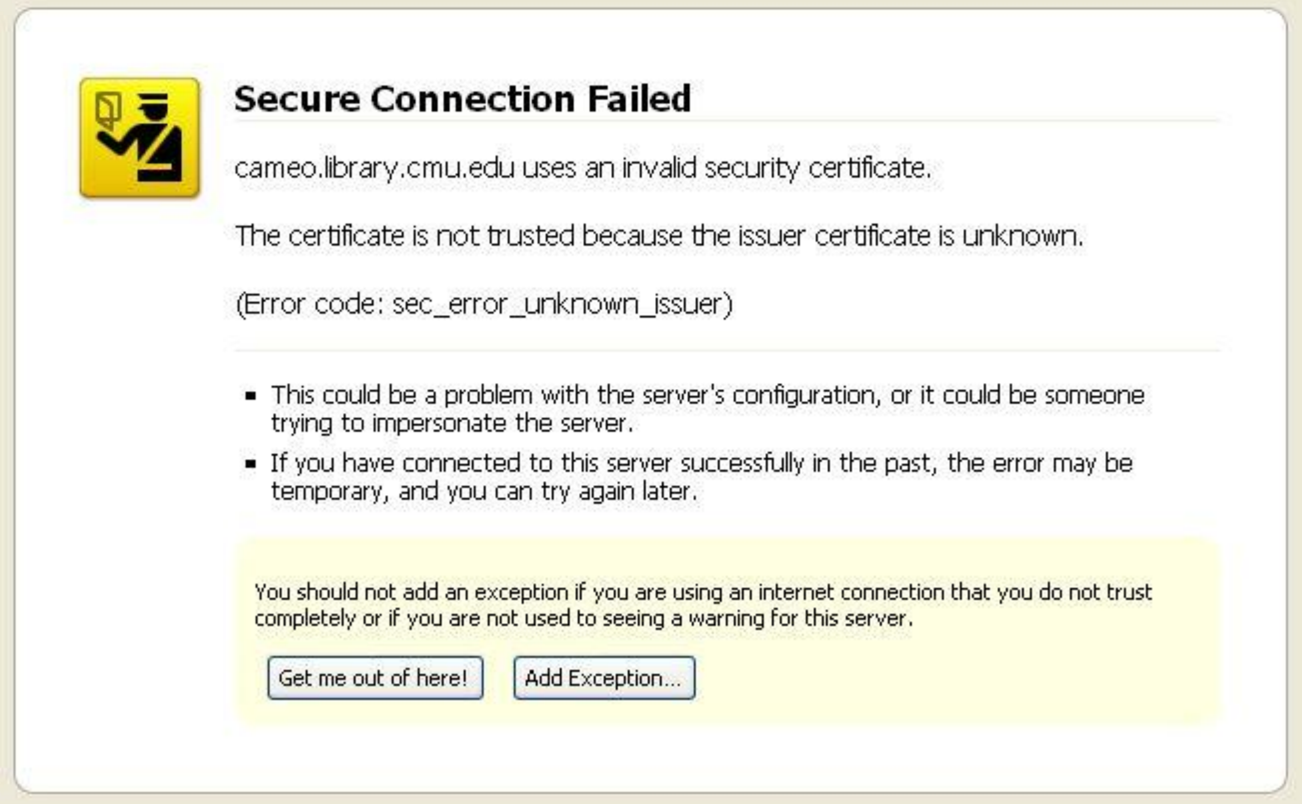
The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…

FF3 Warning



Secure Connection Failed

cameo.library.cmu.edu uses an invalid security certificate.

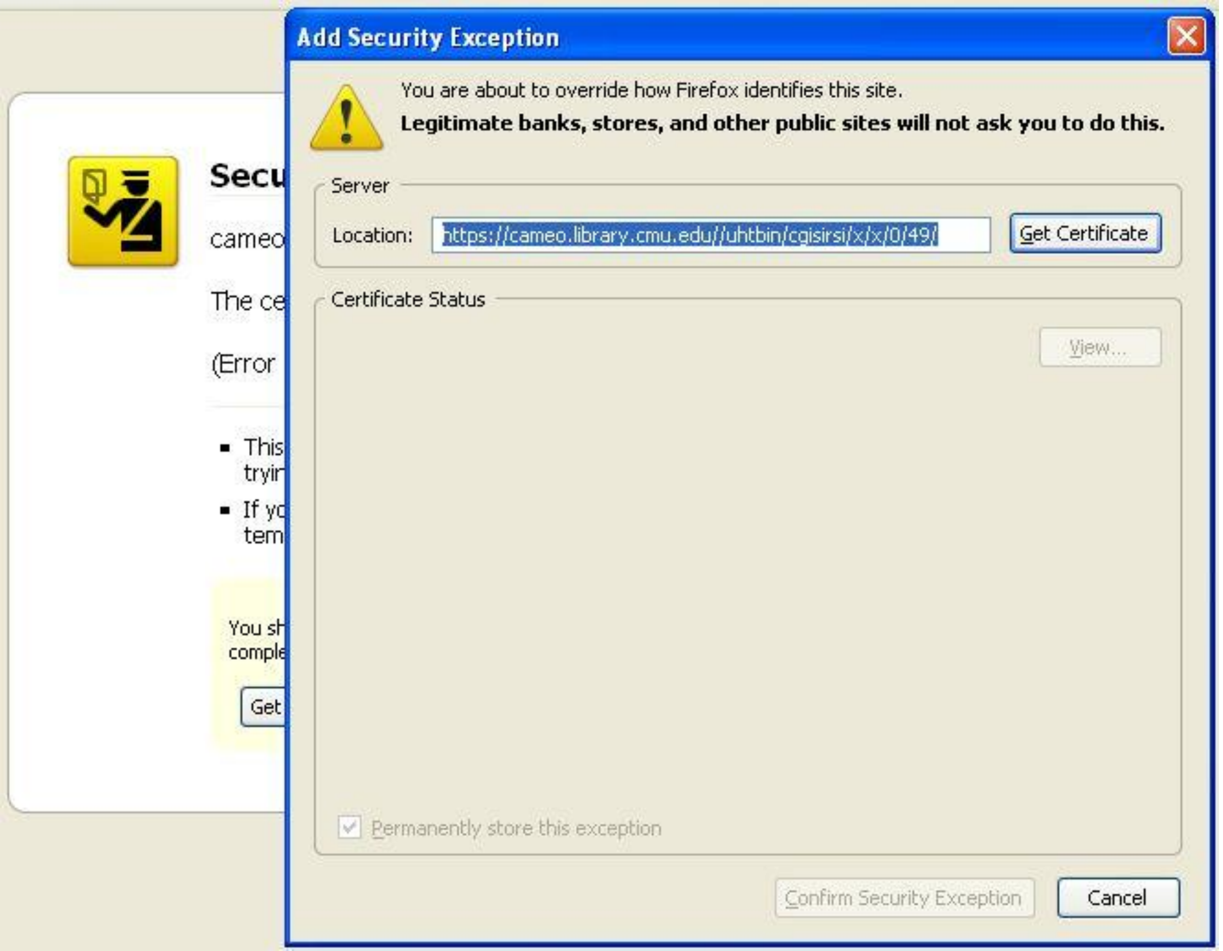
The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

FF3 Warning



Secu

cameo

The ce

(Error

- This tryir
- If yo tem

You sh comple

Get

Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

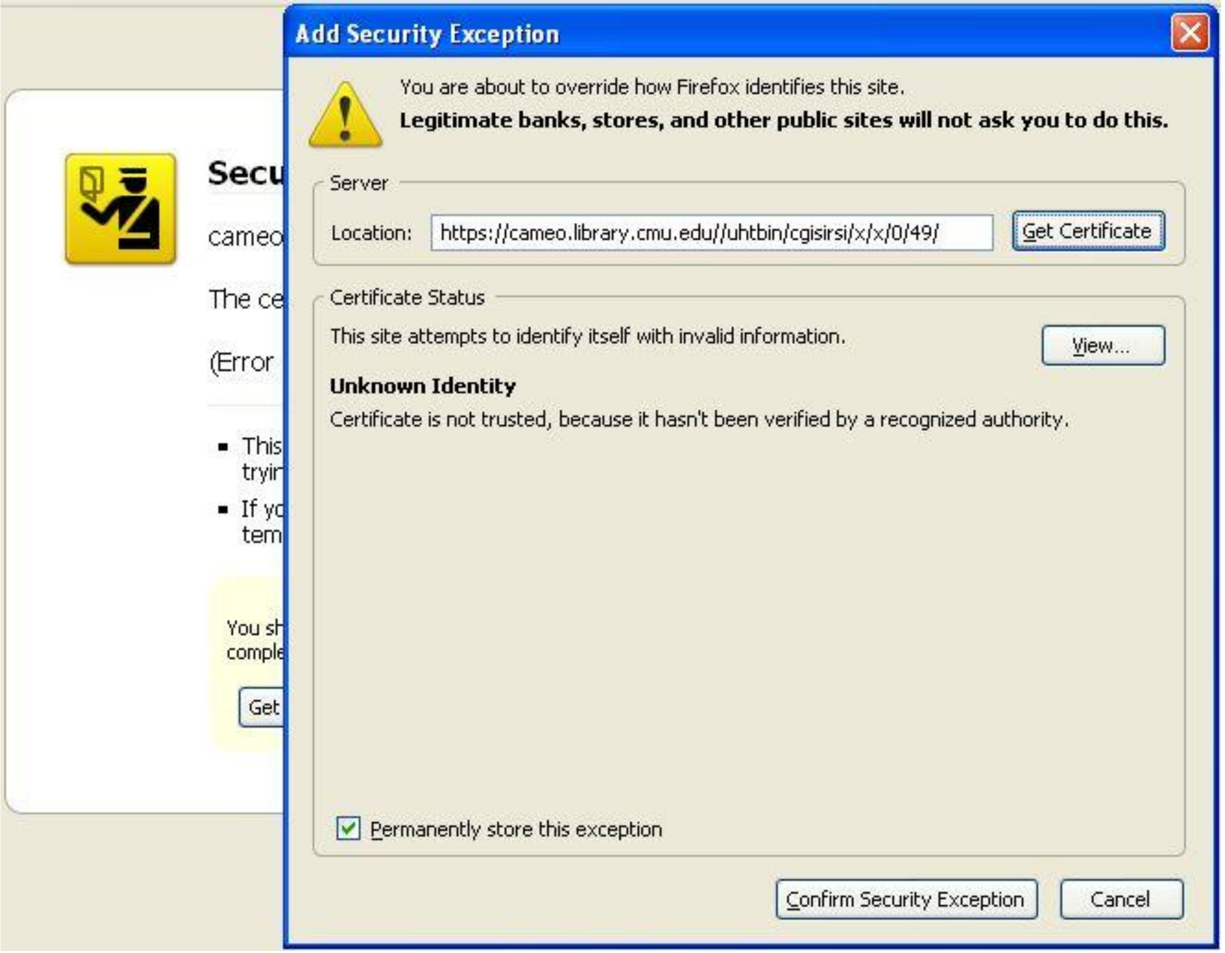
Server

Location: https://cameo.library.cmu.edu//uhtbin/cgisirsi/x/x/0/49/

Certificate Status

☑ Permanently store this exception

FF3 Warning



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://cameo.library.cmu.edu//uhtbin/cgisirsi/x/x/0/49/

Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

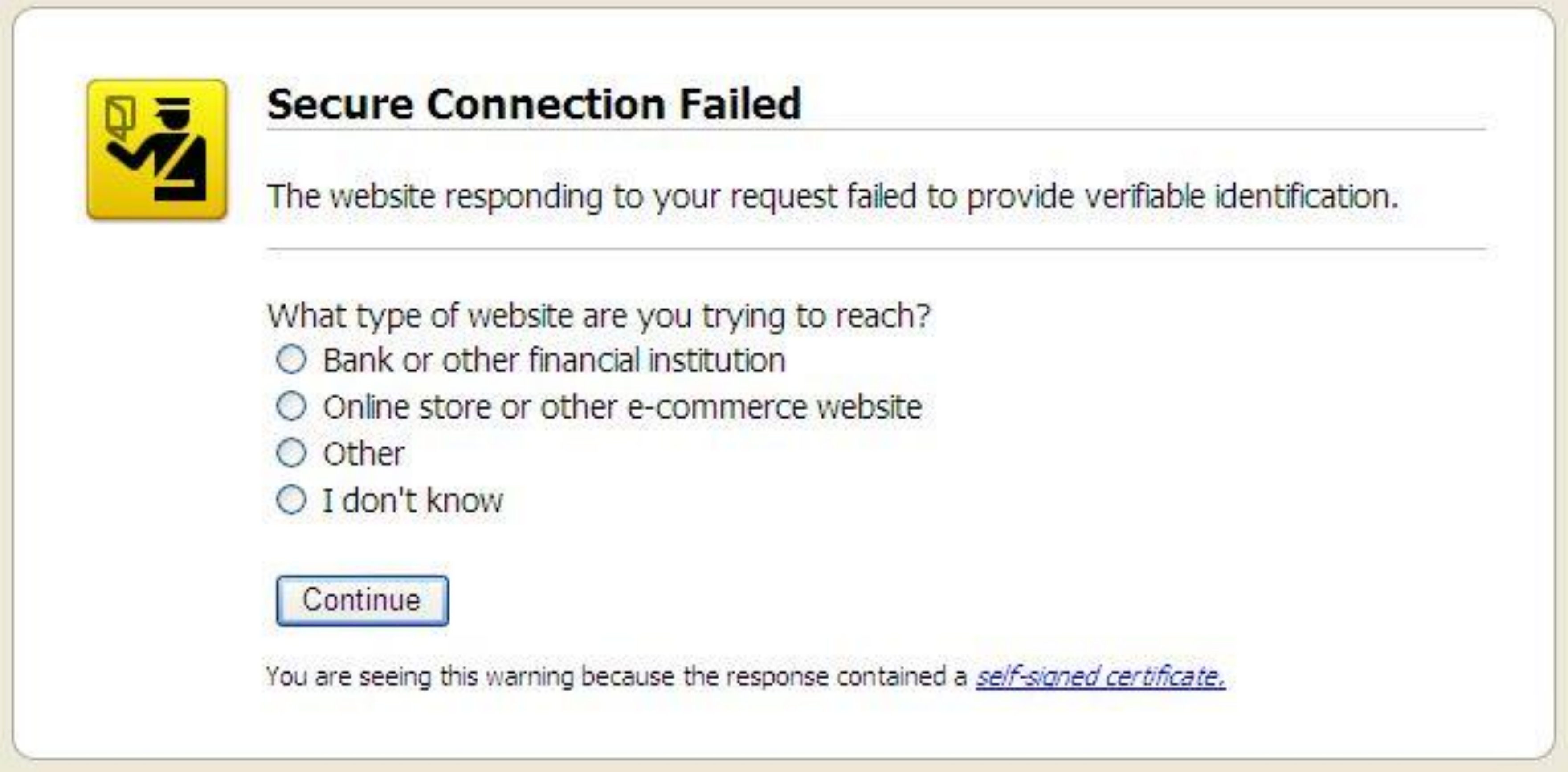
☑ Permanently store this exception

Warning Design Strategies

- Lessons from online survey:
  - Context sensitivity
  - Prevent habituation
  - Avoid confusion with other, less serious, warnings
- Warning science guidance:
  - Avoid warnings when possible
  - Clearly explain risk
  - Provide straightforward instructions for avoiding the hazard

Idea: Ask users a question

Multi-page warning



Secure Connection Failed

The website responding to your request failed to provide verifiable identification.

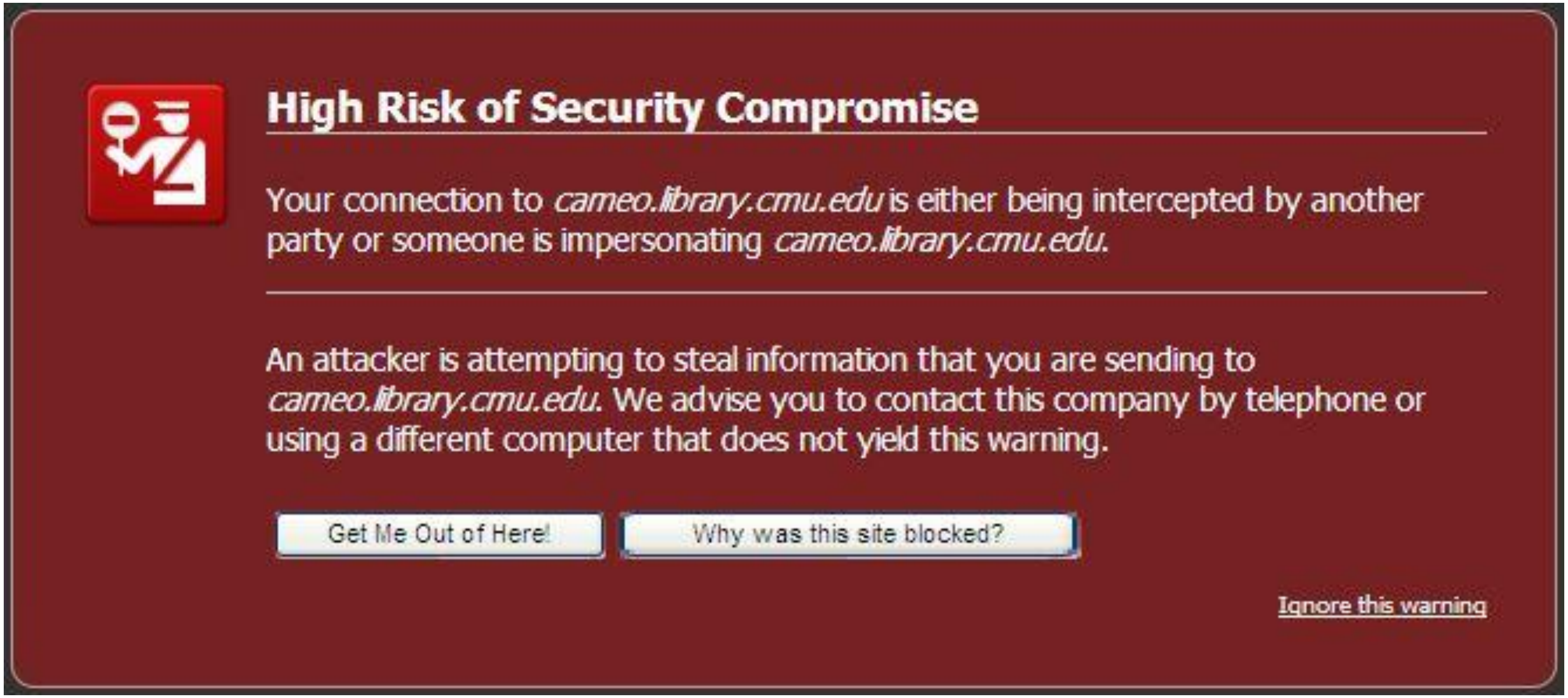
What type of website are you trying to reach?

○ Bank or other financial institution
○ Online store or other e-commerce website
○ Other
○ I don't know

You are seeing this warning because the response contained a *self-signed certificate.*

Idea: Make risk obvious

Single-page warning



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Laboratory Study

- 100 participants
  - CMU students
  - Recruited by fliers, emails, and participant list
- 5 Randomly-assigned conditions: FF2, FF3, IE7, Single page custom warning and multi-page custom warning
- Warning was triggered twice:
  - Bank
  - Library catalog

Laboratory Study

- Users were instructed to find:
  - Total area of Italy using Google
  - Account balance at bank website*
  - Price of *Freakonomics* at Amazon
  - *Richistan* call number with CMU library catalog*

      *warning appeared
- Alternate tasks provided
  - Required calling or using a different site
- Post-experiment survey on reactions

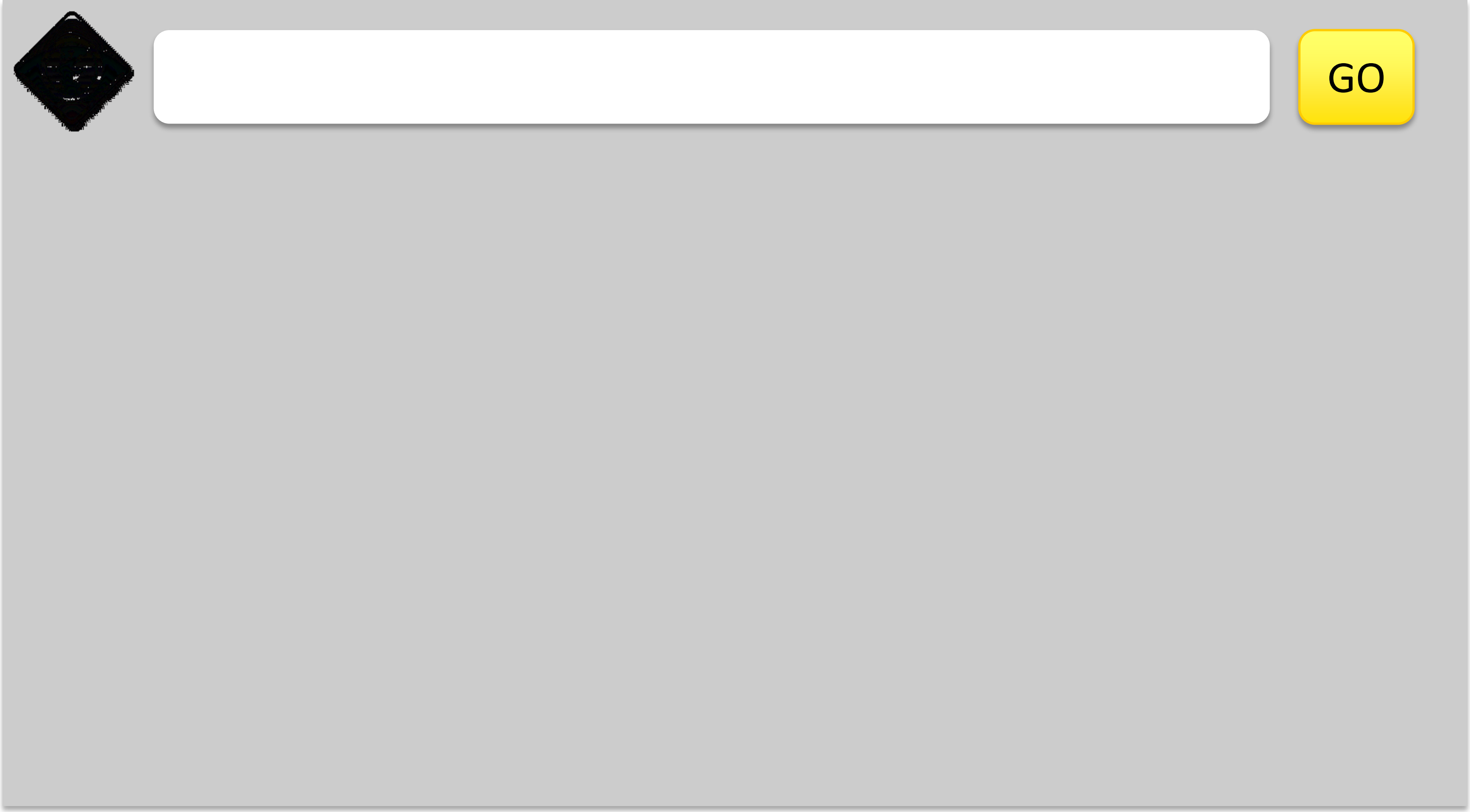
Task Step 1

Use online banking (https://www.bank.com) to find your current account balance. Write down only the **last two digits of your account balance**.

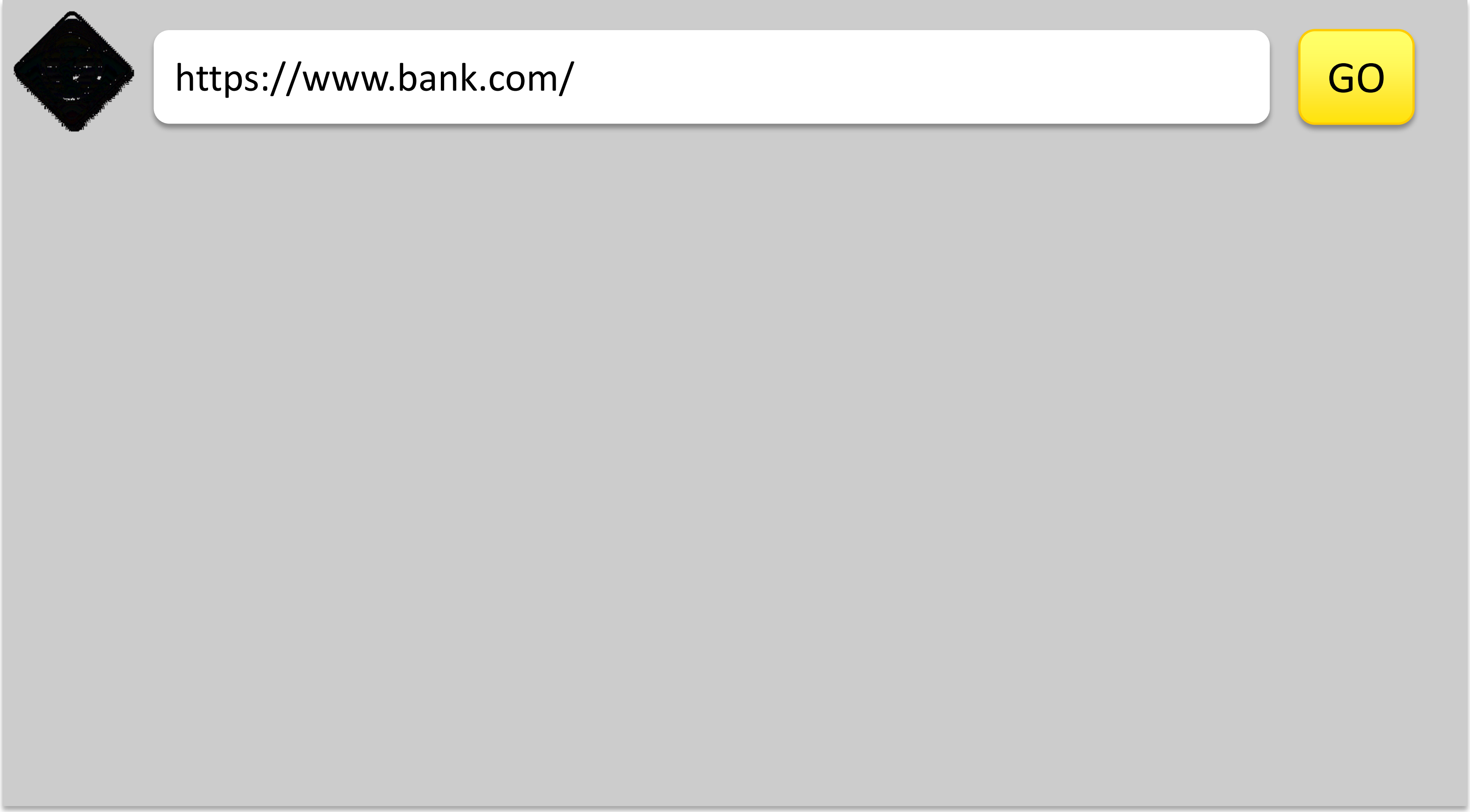
Alternate: Use automated phone banking (Phone: **1-888-555-1212**). Please use the campus phone in front of you and don’t forget to first dial ‘9.’

Please remember to “think aloud” as you complete this task.

Task walkthrough

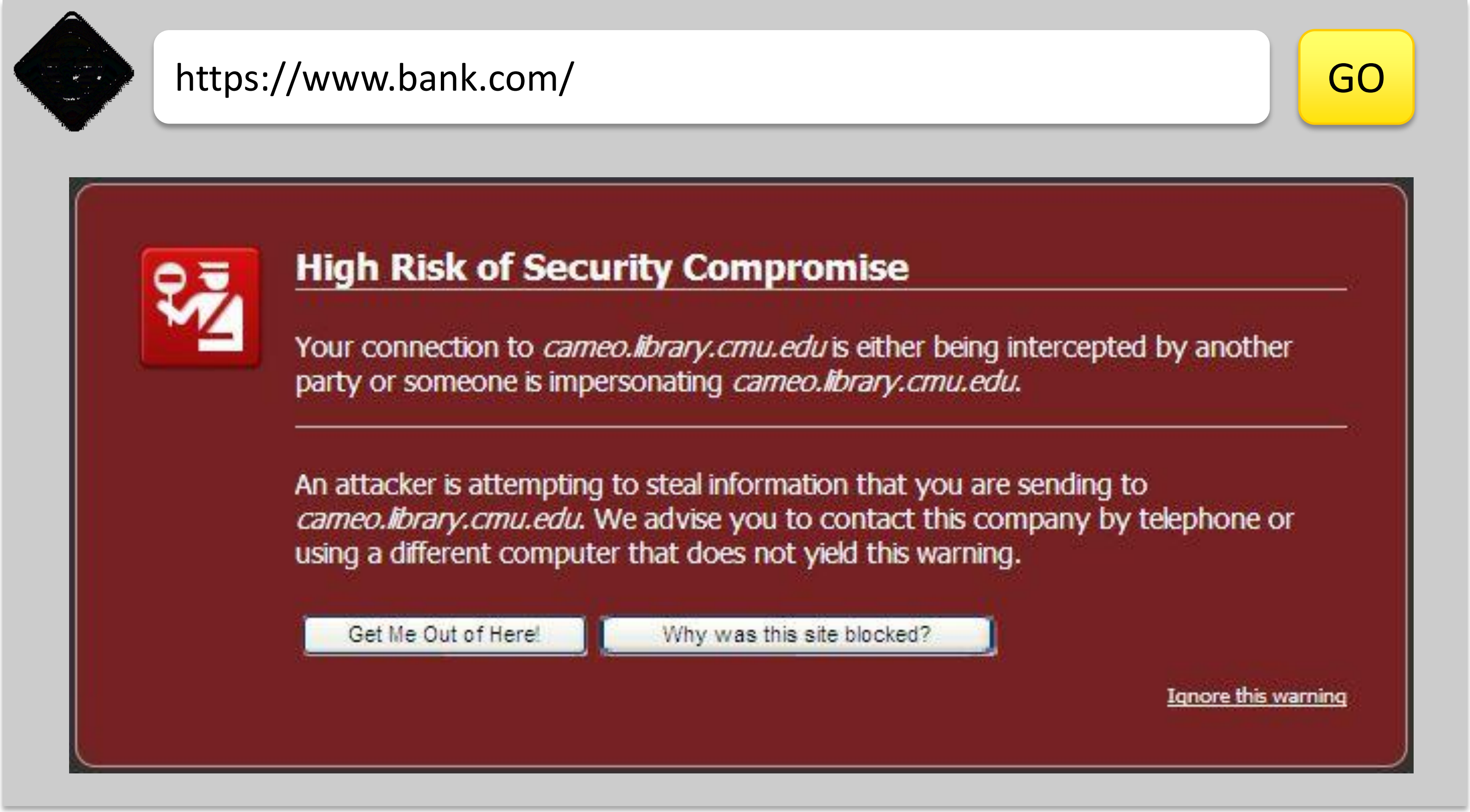


Task walkthrough



https://www.bank.com/

Task walkthrough

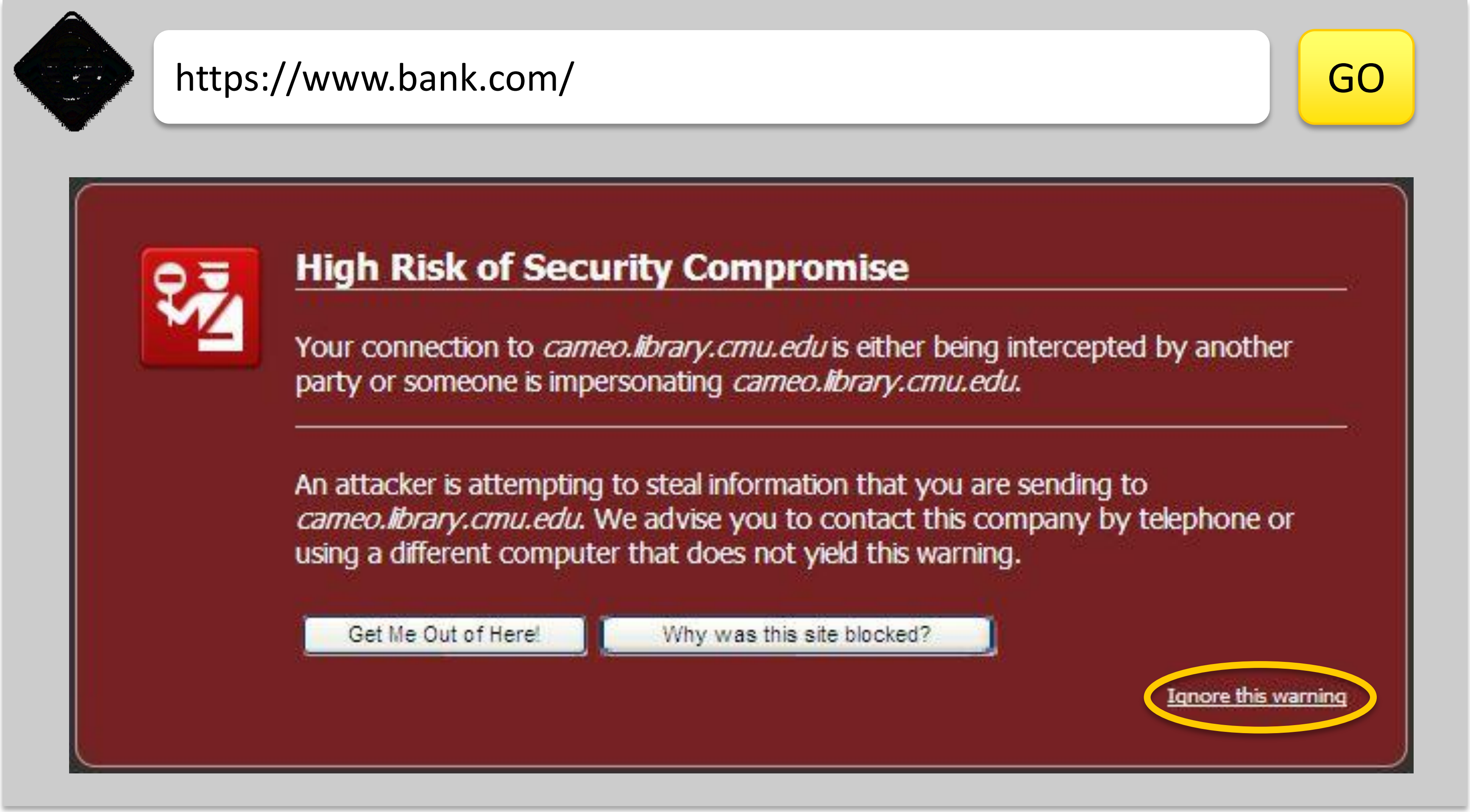


High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu.*

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu.* We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Task walkthrough



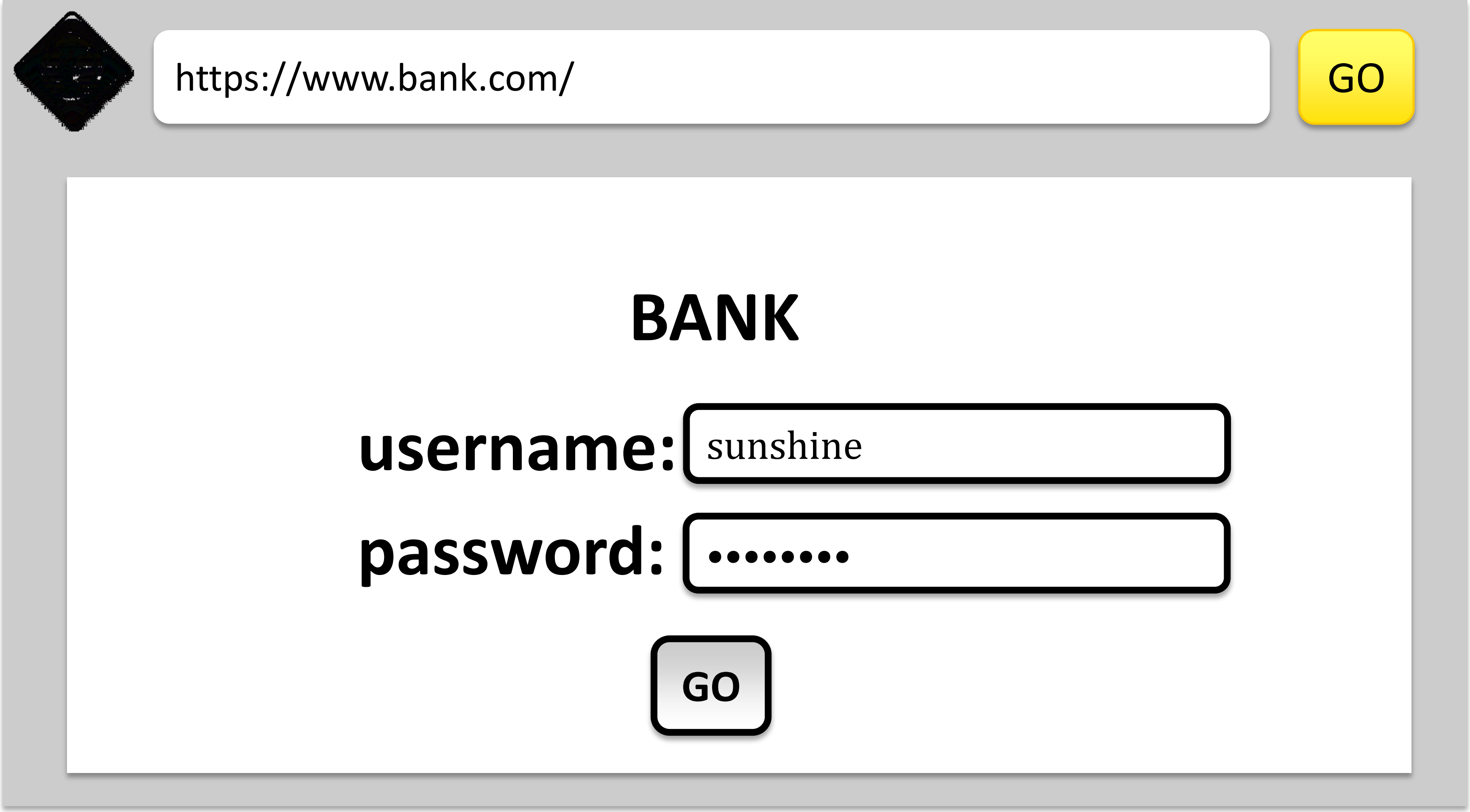
https://www.bank.com/

High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu.*

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu.* We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Task walkthrough



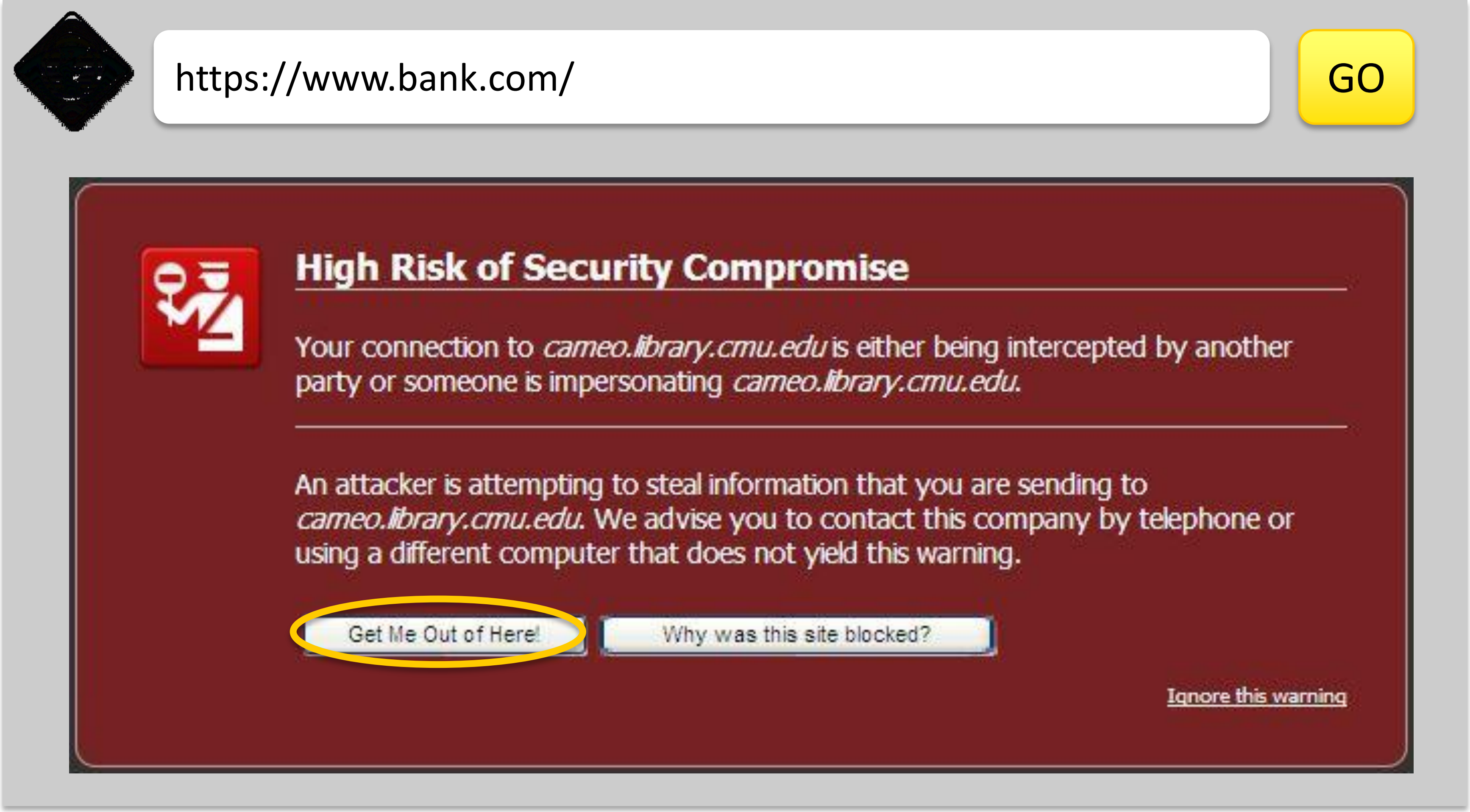
https://www.bank.com/

BANK

username: sunshine

password: ••••••••

Task walkthrough alternate



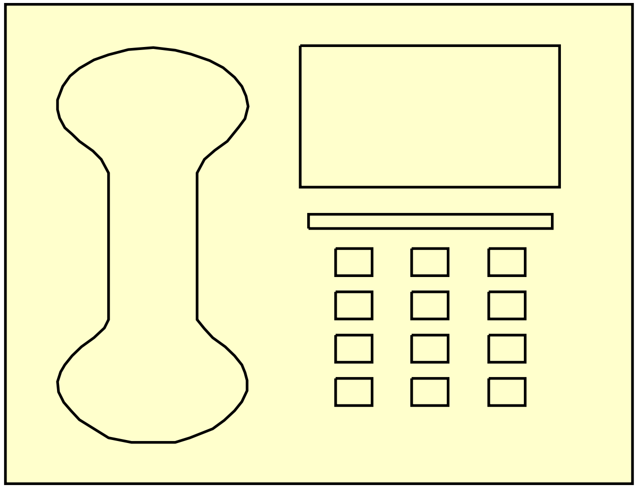
https://www.bank.com/

High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu.*

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu.* We advise you to contact this company by telephone or using a different computer that does not yield this warning.

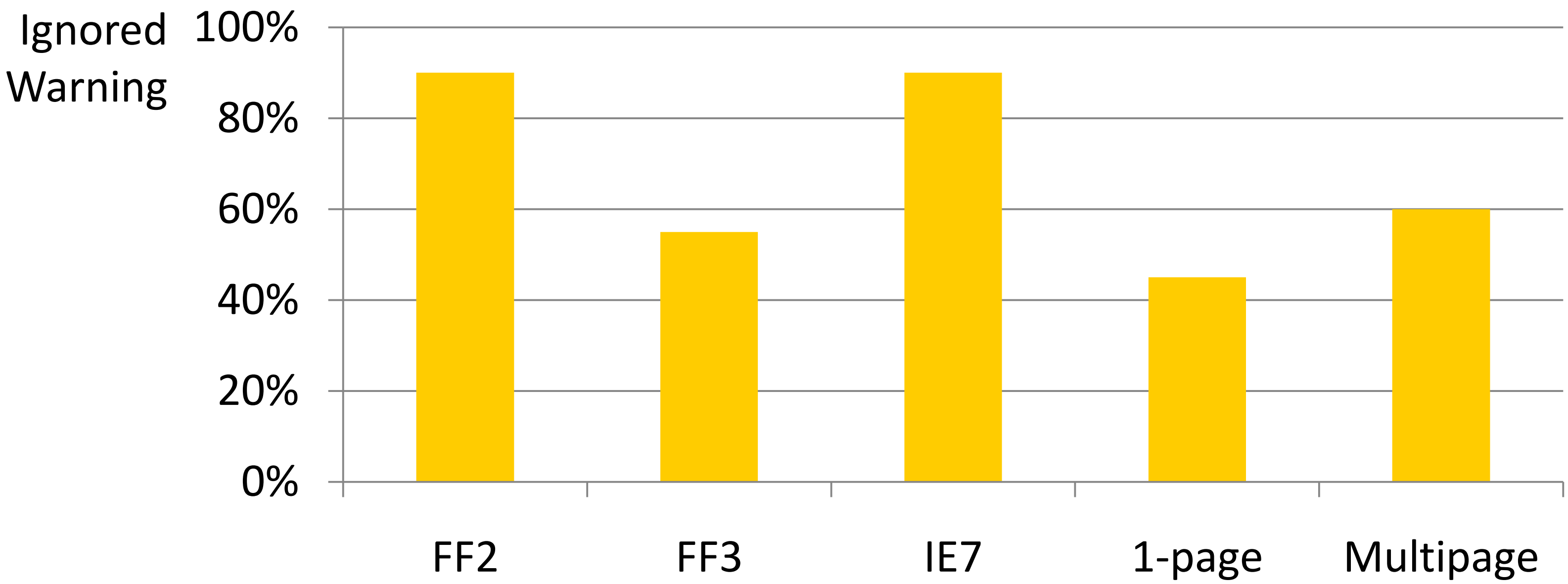
Task walkthrough alternate



Hypotheses

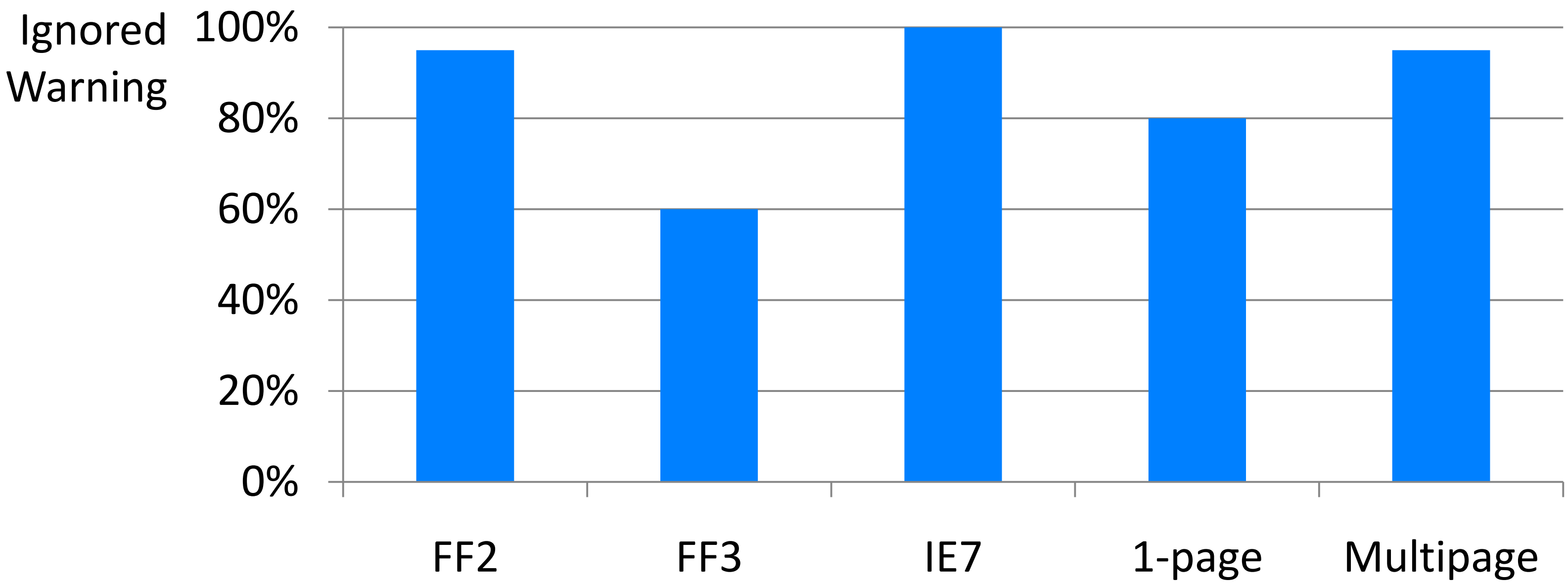
- Participants would be likely to ignore the IE7 and FF2 warnings on both websites
- Participants would be likely to obey the FF3 and our single-page warning on both websites
- Participants who saw our multi-page warning would obey on bank website, but continue to library website

Bank Results



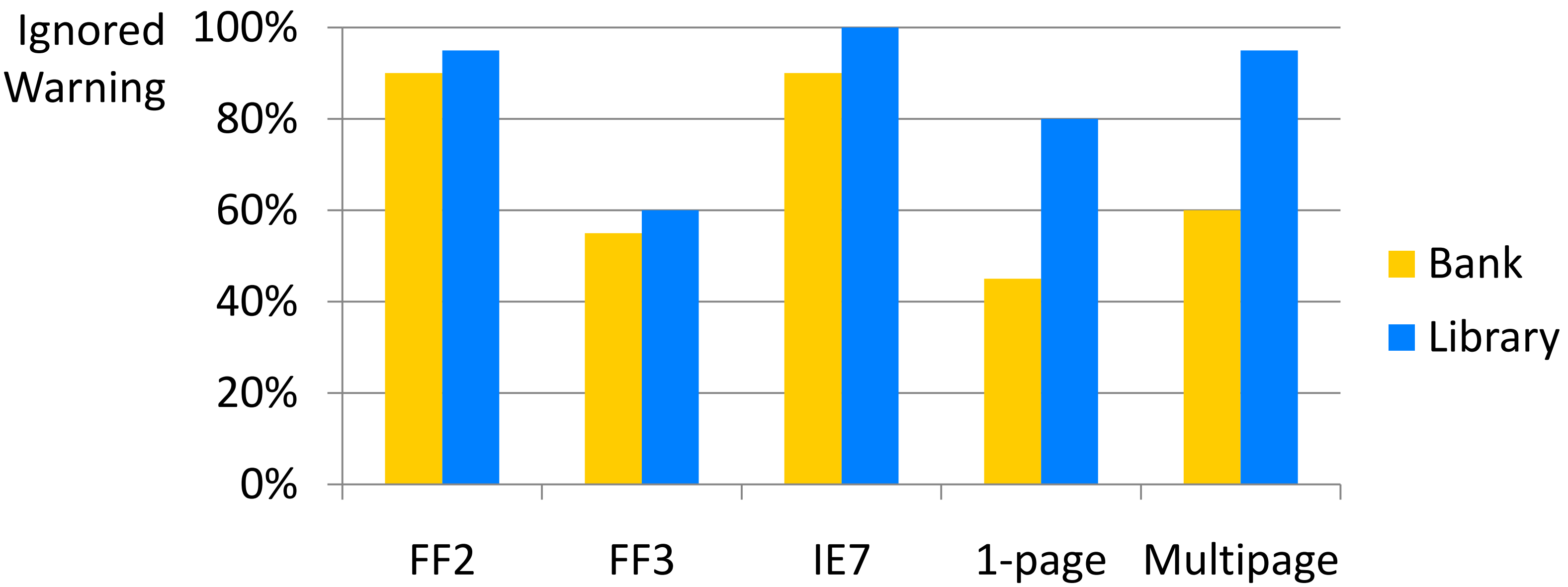
- In risky situation, significantly fewer people heeded IE7 and FF2 than other warnings

Library Results



- In low risk situation, almost all users overrode warnings except in FF3 condition

Library vs. Bank



- In native warning conditions, no significant difference in reactions at library and bank
- In new warning conditions, users more likely to heed warnings at bank than at library

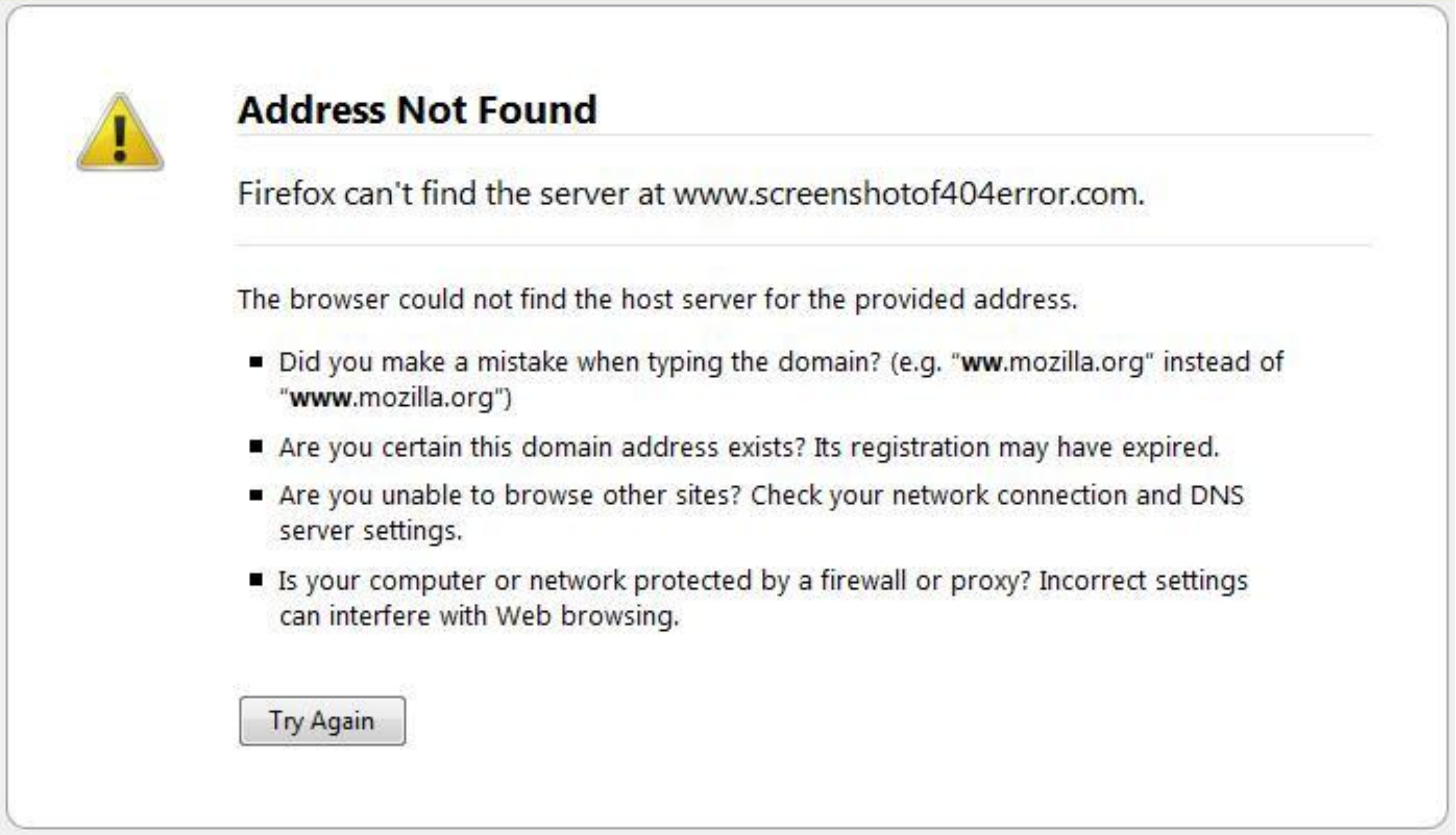
Explain what to do

- “Why did you choose to heed or ignore the warning?”
- Mentioned risk:
  - FF2: 2
  - FF3: 2
  - IE7: 2
  - Single-Page: 11

Explain what to do

- “What action(s) did you think the warning at the bank wanted you to take?”
- Wanted them *not* to proceed:
  - FF2: 3
  - FF3: 2
  - IE7: 4
  - Single-page: 10

Making It Difficult



Address Not Found

Firefox can't find the server at www.screenshotof404error.com.

The browser could not find the host server for the provided address.

- Did you make a mistake when typing the domain? (e.g. "**ww**.mozilla.org" instead of "**www**.mozilla.org")
- Are you certain this domain address exists? Its registration may have expired.
- Are you unable to browse other sites? Check your network connection and DNS server settings.
- Is your computer or network protected by a firewall or proxy? Incorrect settings can interfere with Web browsing.

Asking a Question

- 15/20 participants answered correctly at bank
  - – 3 knowingly gave the wrong answer
  - – 2 confused warning with server unavailable error
- Critical Weakness: Finer grained origins attack
  - – attacker circumvents question by forcing connection to unintended website
  - – See paper for details
- Need a different context sensitive approach

Conclusion

- We evaluated a wide class of warnings embodying three solid strategies
- Custom warnings conveyed risks and allowed users to take risk into account when making a decision
- Custom warnings were still not good enough
- Need systems solutions that avoid warnings altogether (e.g. Perspectives, ForceHTTPs)
  - Need to evaluate false positive rate