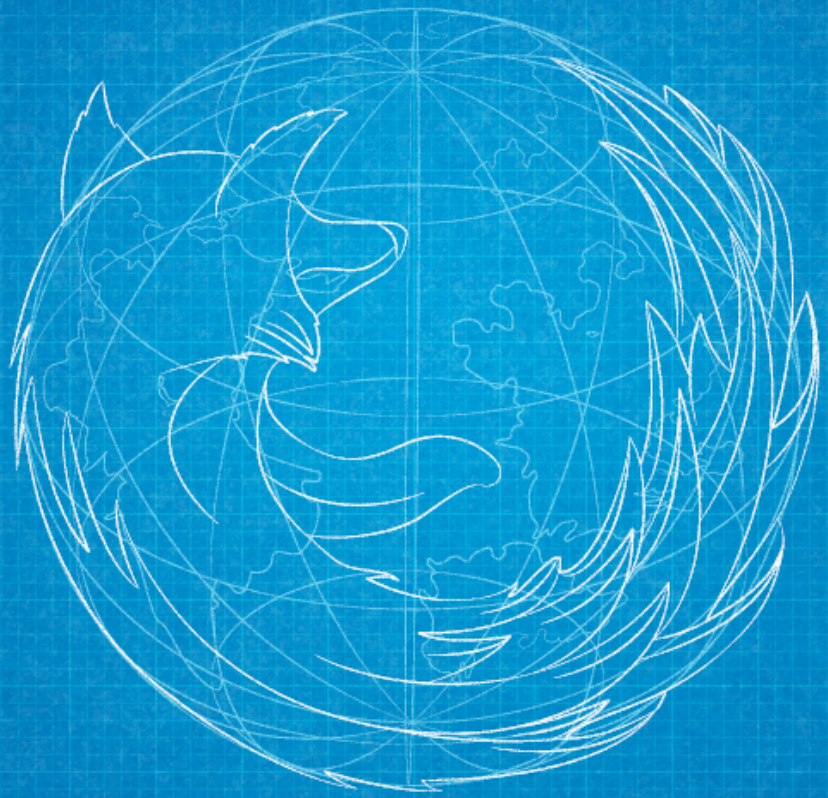


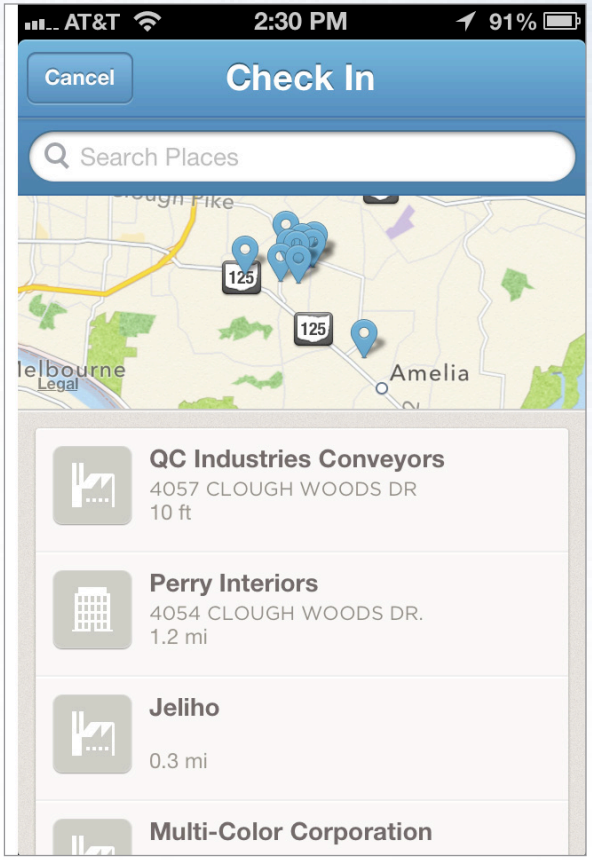
Designing Meaningful Security and Privacy Experiences

(In a world where nobody cares?)

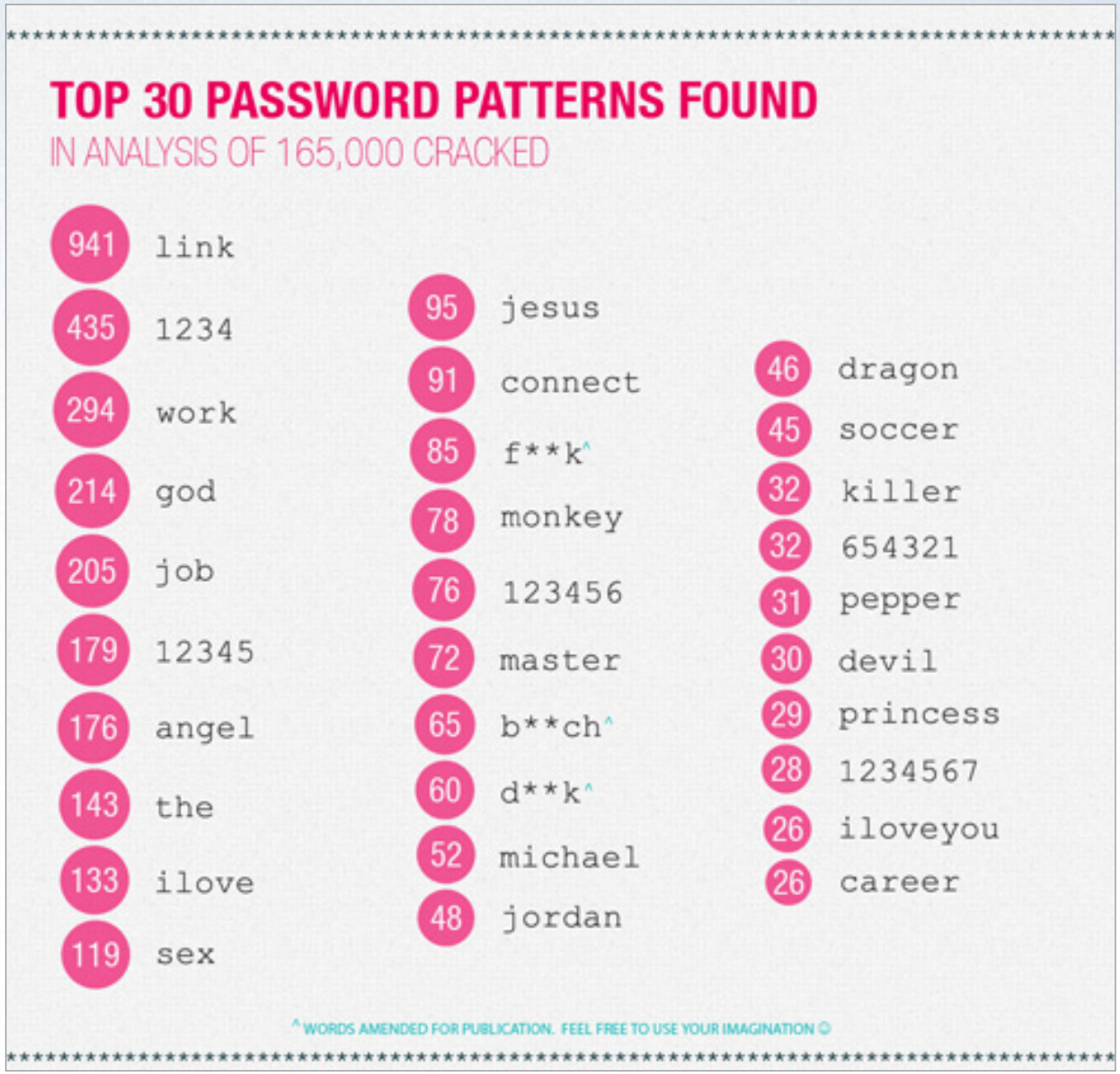
Larissa Co | lco@mozilla.com | Jan 16, 2012

Do people even care about security and privacy?

Usability and Security/Privacy are often perceived as opposites

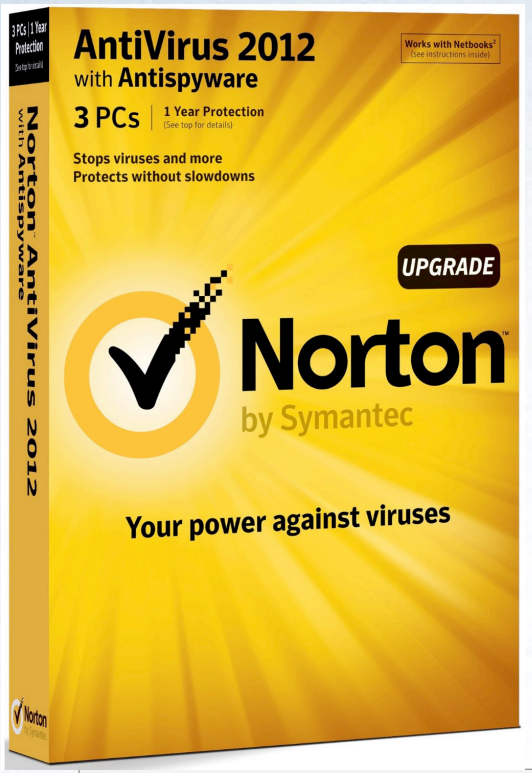


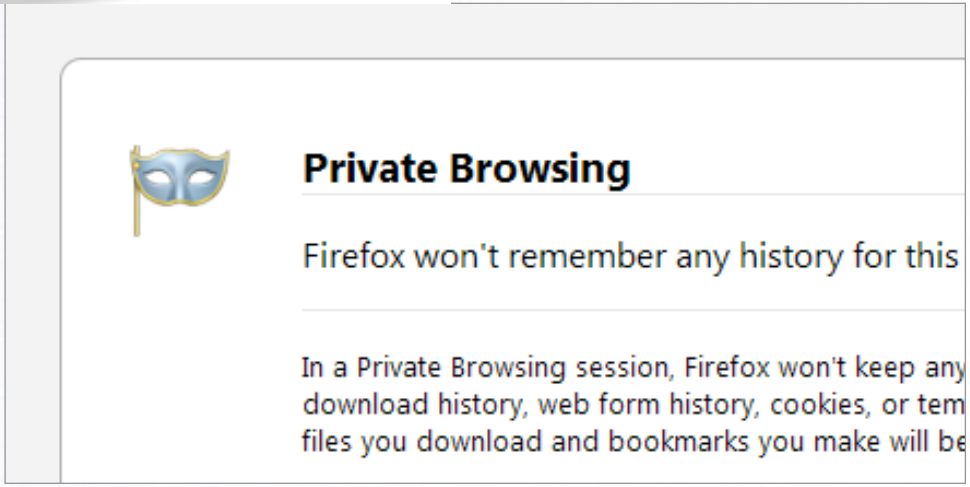
Privacy in the age of social media?



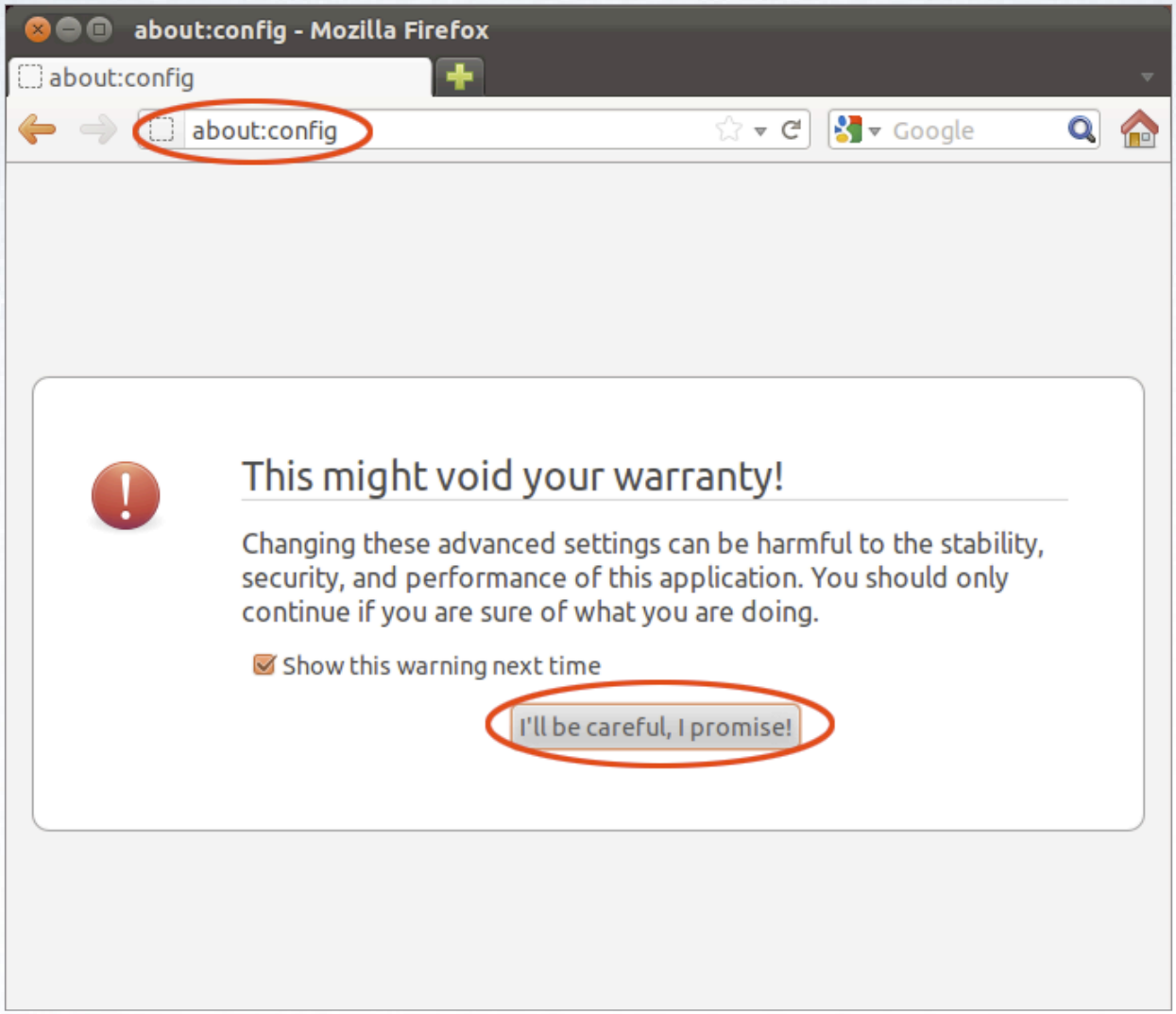
Source: http://www.rapid7.com/resources/infographics/linkedIn-passwords-lifted.html

Security as we work and play more online?

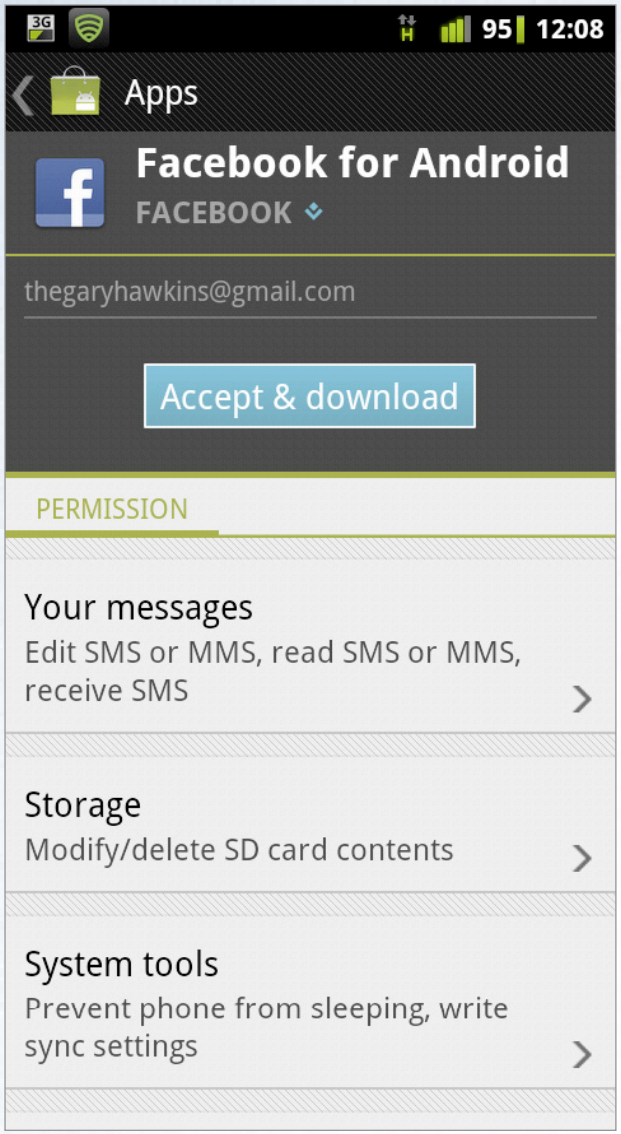


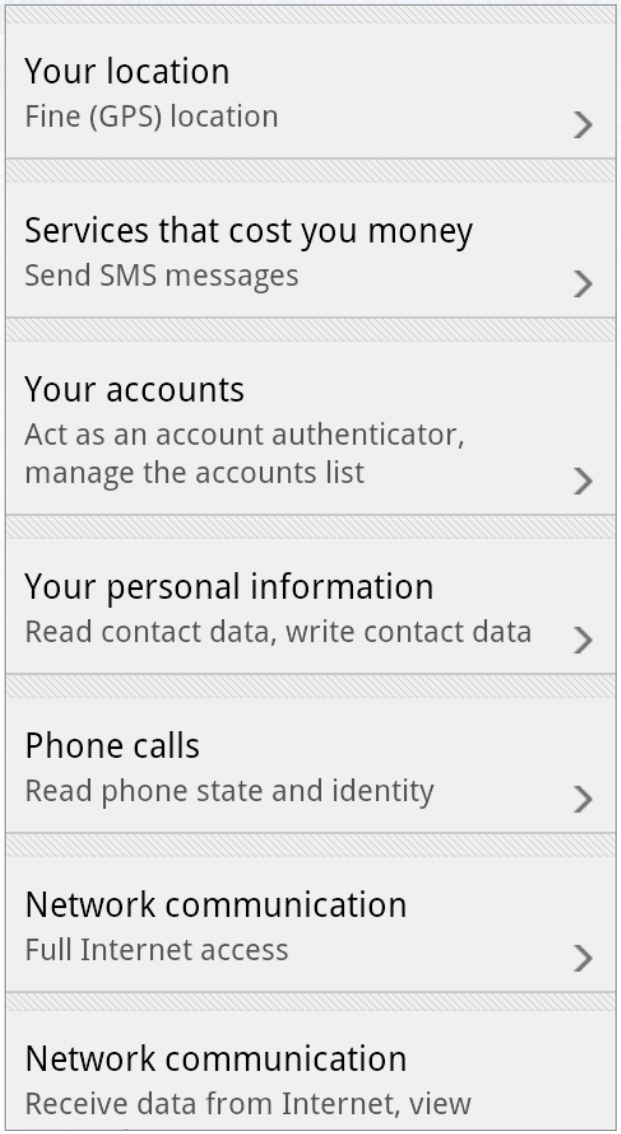


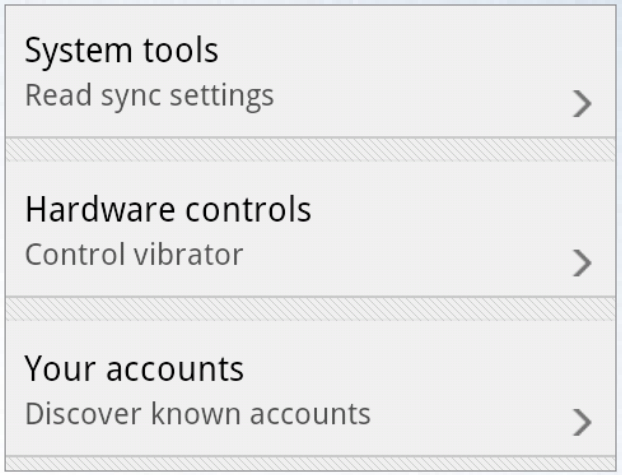
People want to care, but…



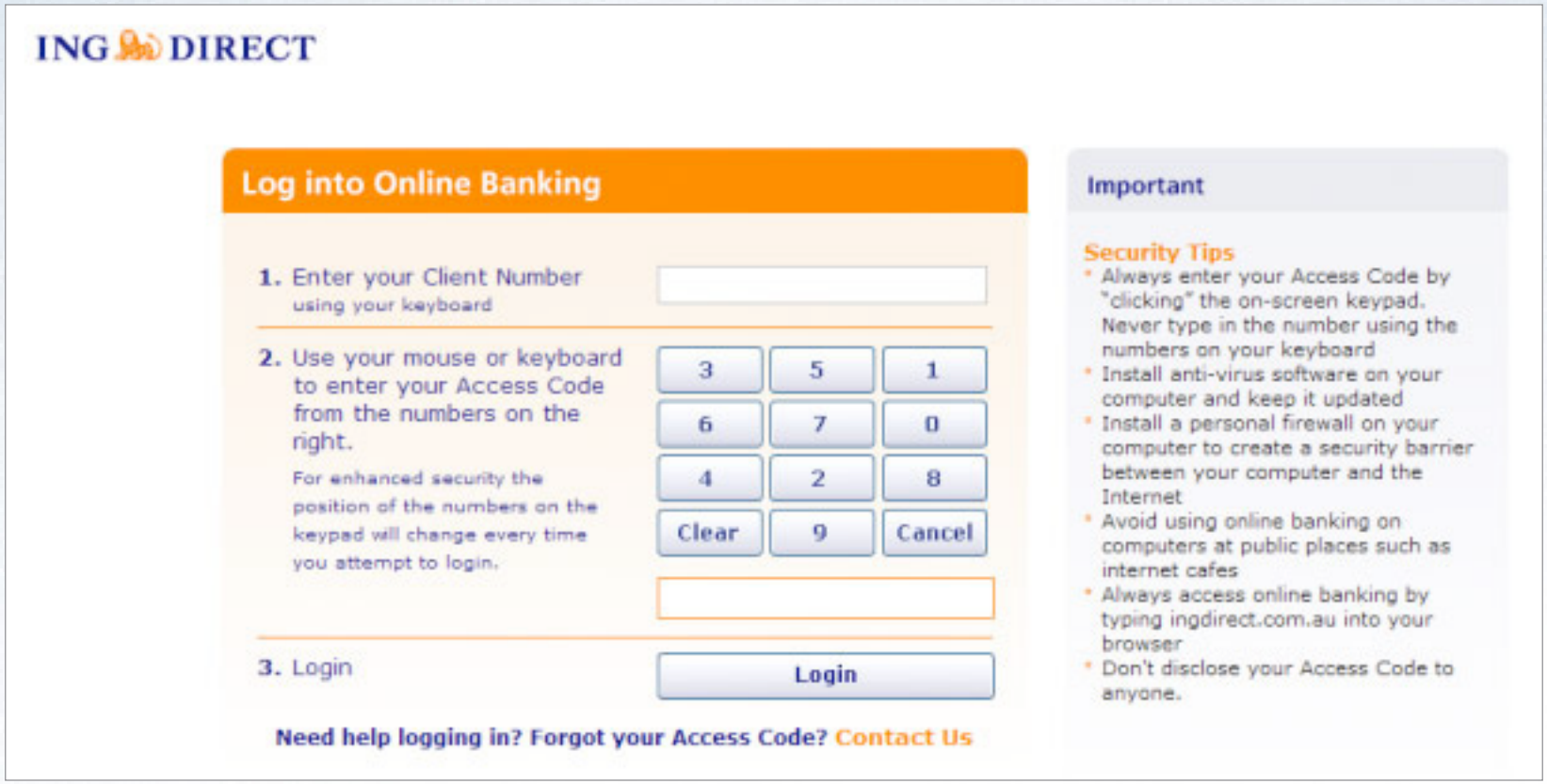
People don't know what will protect them.







People feel helpless.



Security and privacy choices are overwhelming.

*How do we make security and privacy **meaningful** in the context of people's online lives?*

Need to Trust

+

Need to Have Control

Two Fundamental Needs

Need to Trust

Earn and Keep My Trust

Respect My Time and Task

Help Me Make a Thoughtful Decision

Offer Control Without Harming Me

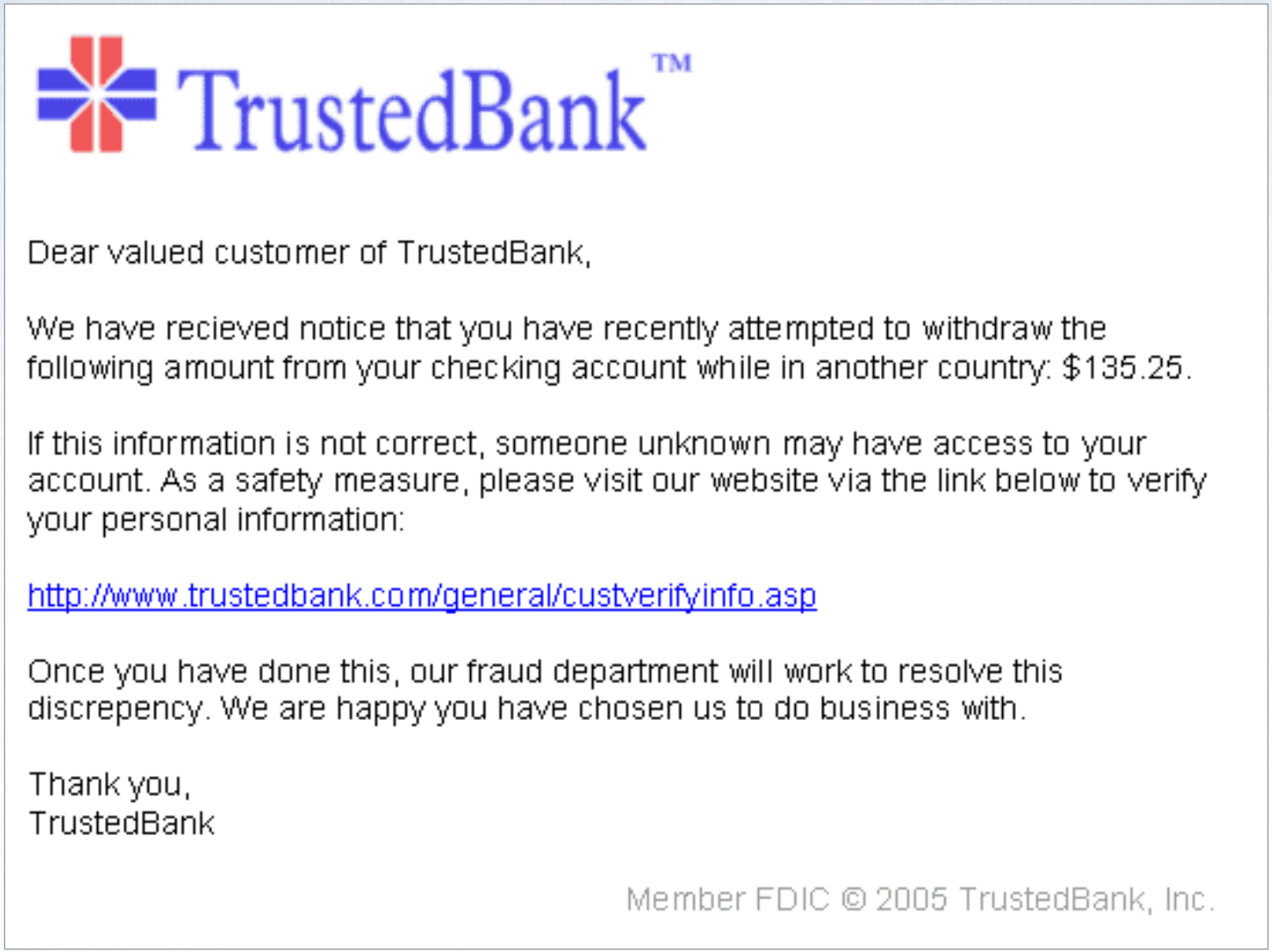
Need to Have Control

Four Design Imperatives

Earn and Keep My Trust

Design Imperative 1

In the real world, it's (often) easier to evaluate trustworthiness.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

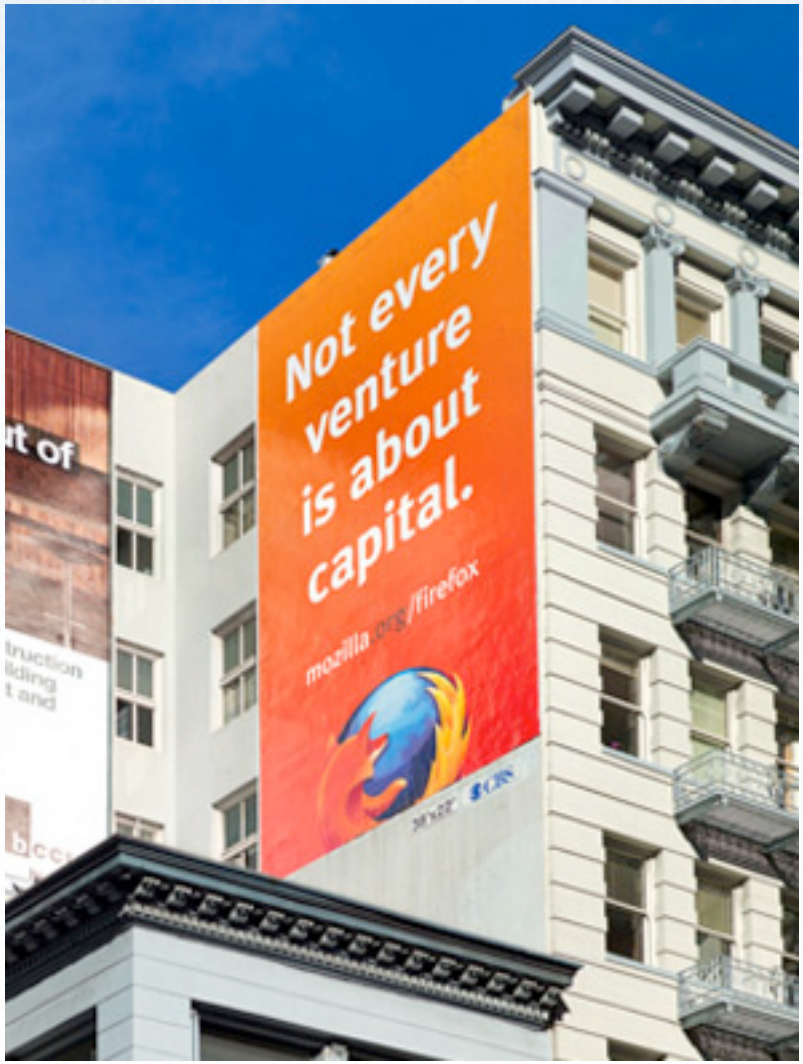
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

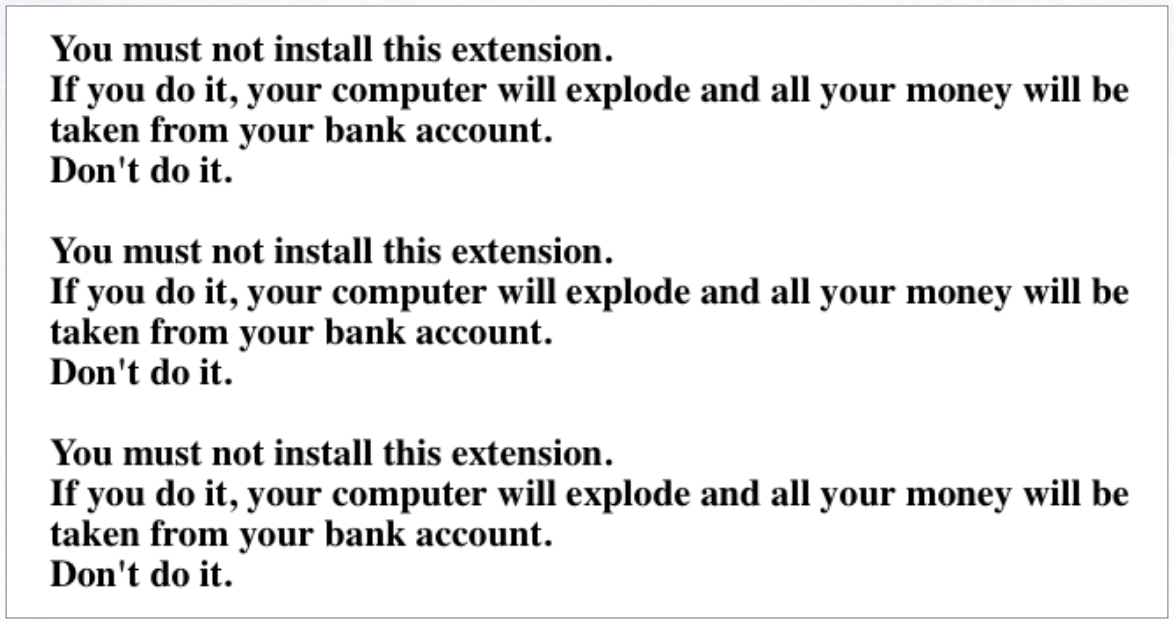
Member FDIC © 2005 TrustedBank, Inc.

In the digital world, people are less knowledgable about how to evaluate trust.

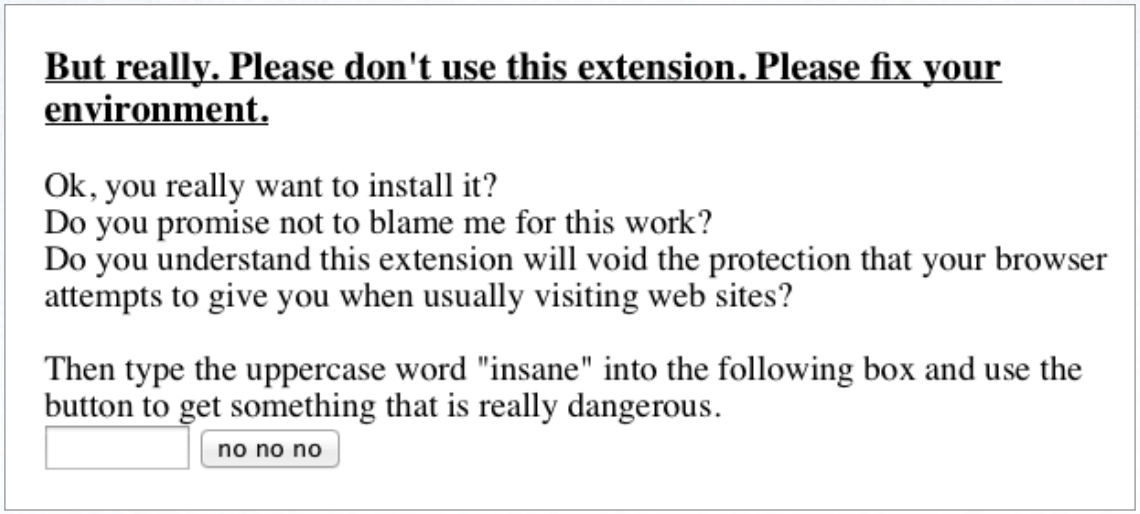
And any design we create to covey trustworthiness can easily be turned against us.



Trust Goes Beyond Transparency



Pitfall 1: Crying Wolf (Overly Alarming Threats)



Pitfall 2: Seemingly Irrational Choices

1 Protect the user upfront

Keeping the user safe shouldn't require his permission

2 Minimize scare tactics

Provide balanced, helpful conclusions based on the facts instead

3 Look legitimate, polished, and personal

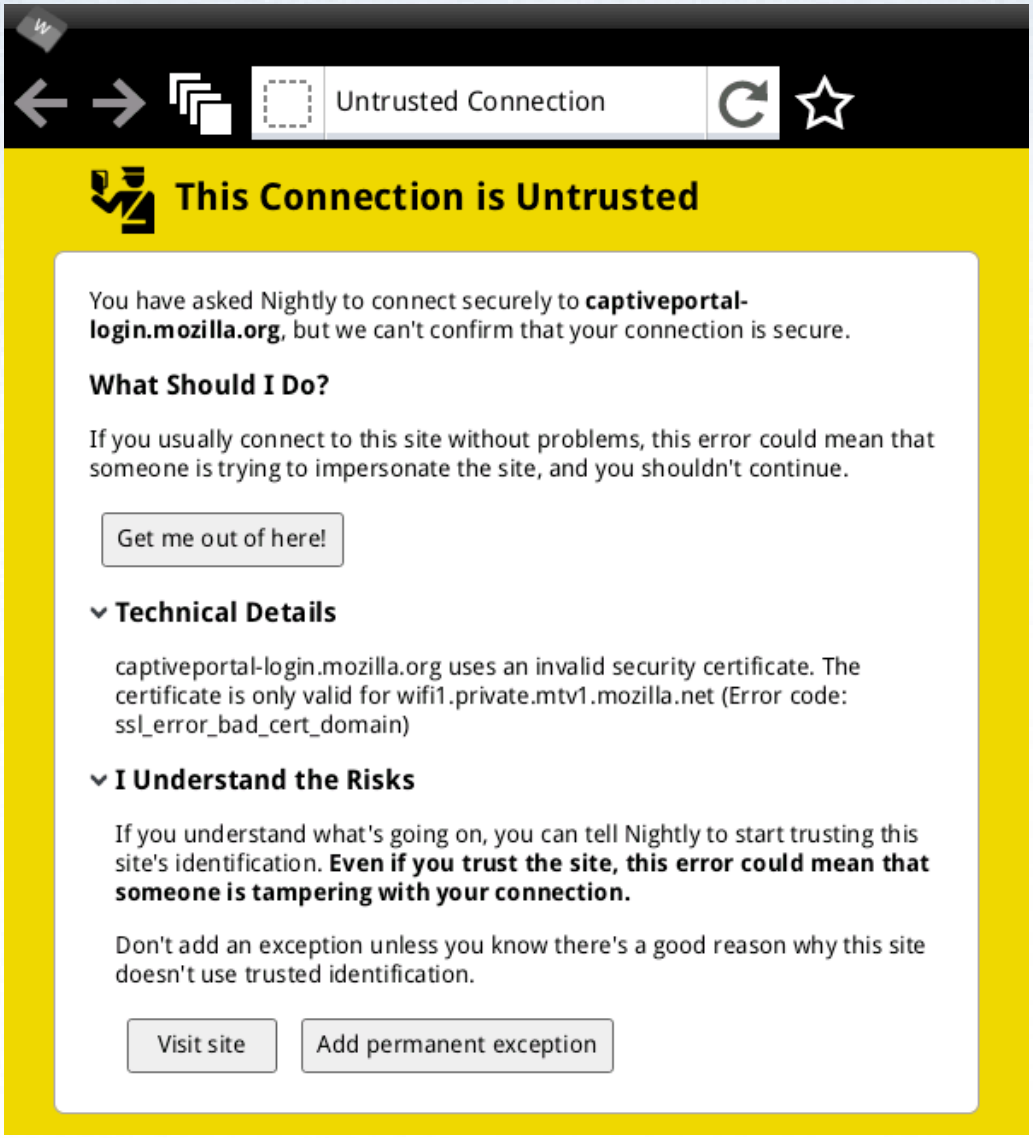
Take inspiration from clever scammers; perceived safety is just as important as true safety

How can we earn and keep the user's trust?

Respect My Time and Task

Design Imperative 2

A common coffee shop decision: When people are forced to choose between their task and "being safe"…

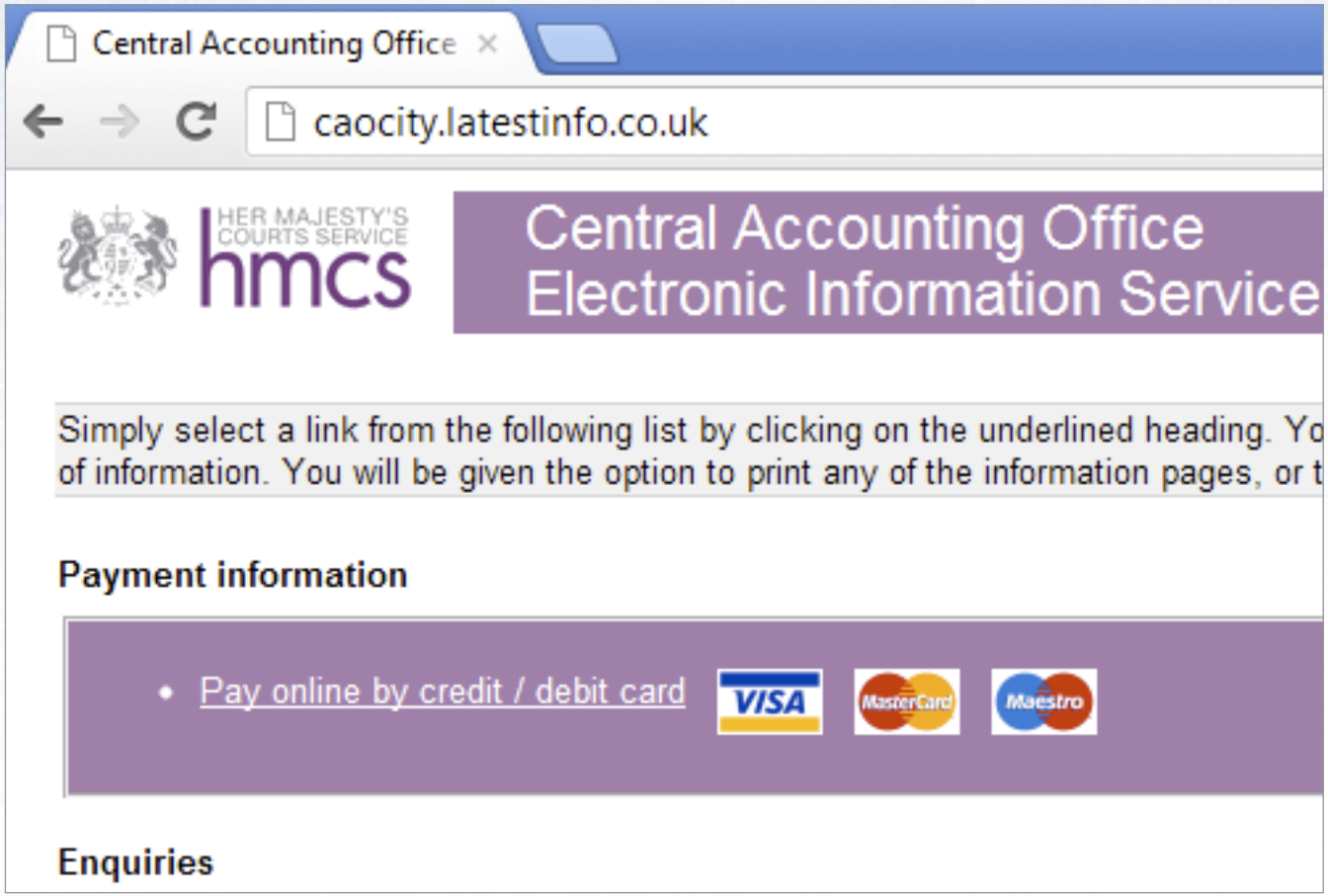


...they choose their task, especially if "being safe" is difficult or impractical.

If you want users to listen to what you have to say, respect their time and task.

The Golden Rule of Security and Privacy Messages

Pitfall 1: "Why is this relevant to me?"



Pitfall 2: LGTM! (a.k.a. Task-Blindness)

We don't pay attention to positive / neutral indicators as much as negative ones.

1 Focus on the impact to the user's task

Instead of on the security/privacy risk

2 Flag threats that the user cares about

Don't rely on the absence of positive indicators to tell the user that something's wrong

3 Don't interrupt a task when an immediate response (or any at all) isn't necessary.

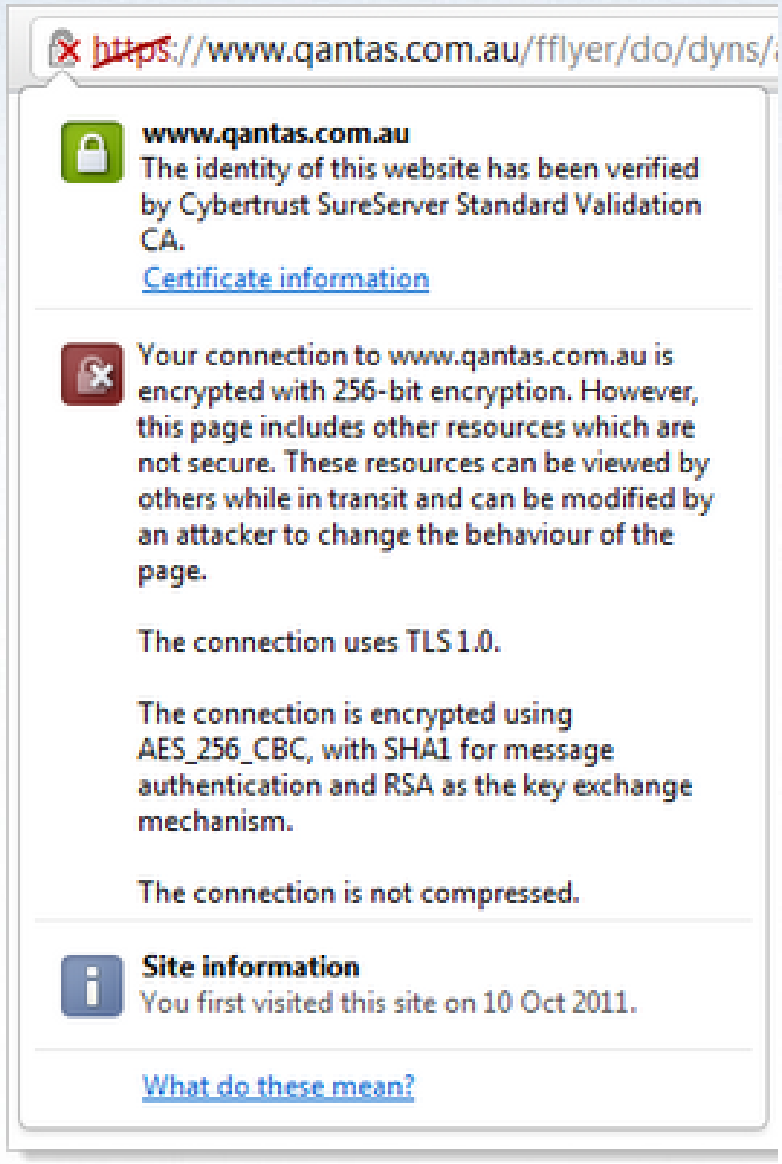
Wait until the user's done, or be smart enough to raise the issue before he starts

How can we respect the user's time and task?

Help Me Make a Thoughtful Decision

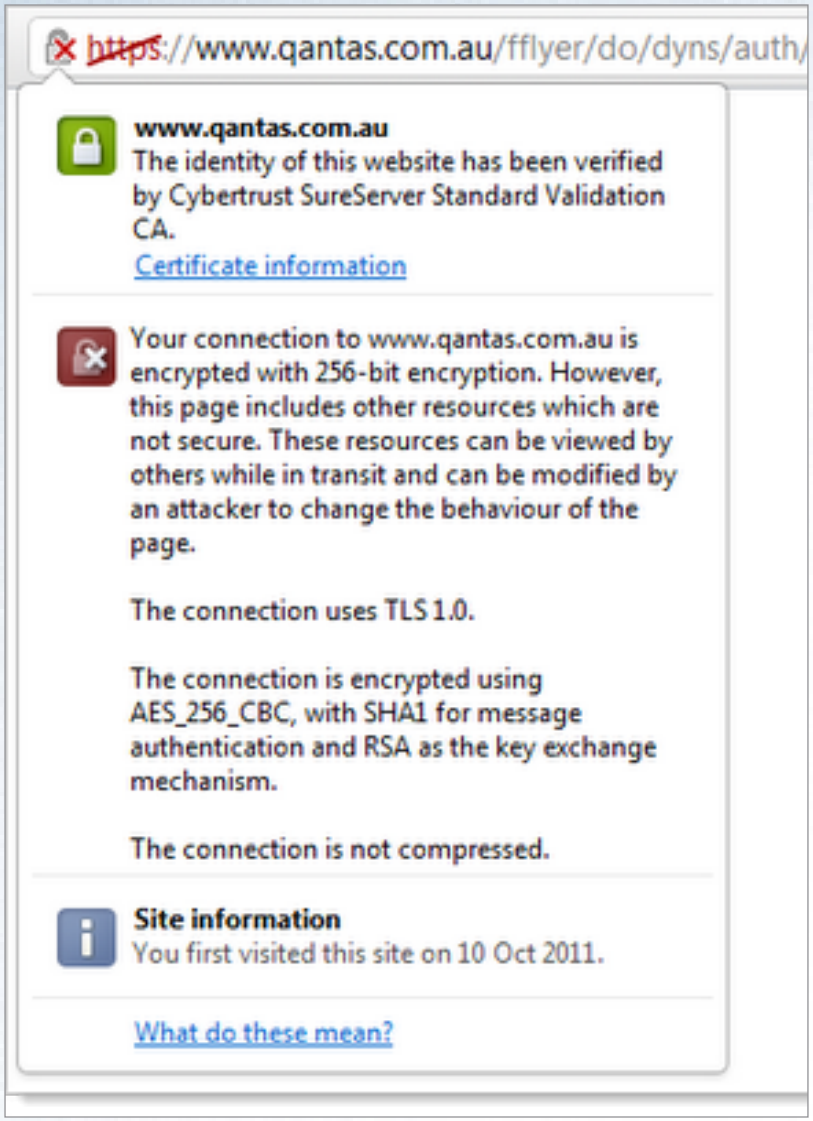
Design Imperative 3

Pitfall 1: Generic / Vague Messages

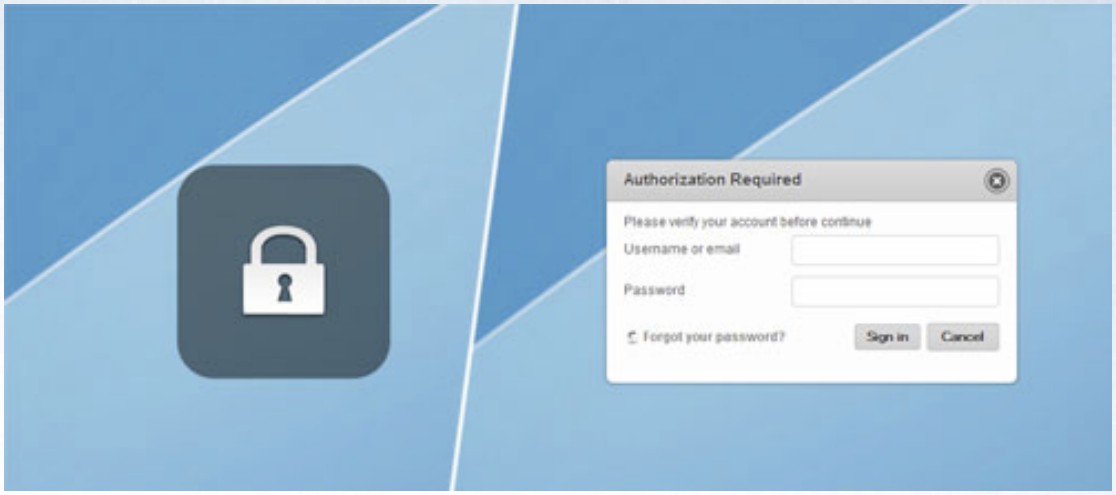


Pitfall 2: Sending Mixed Signals

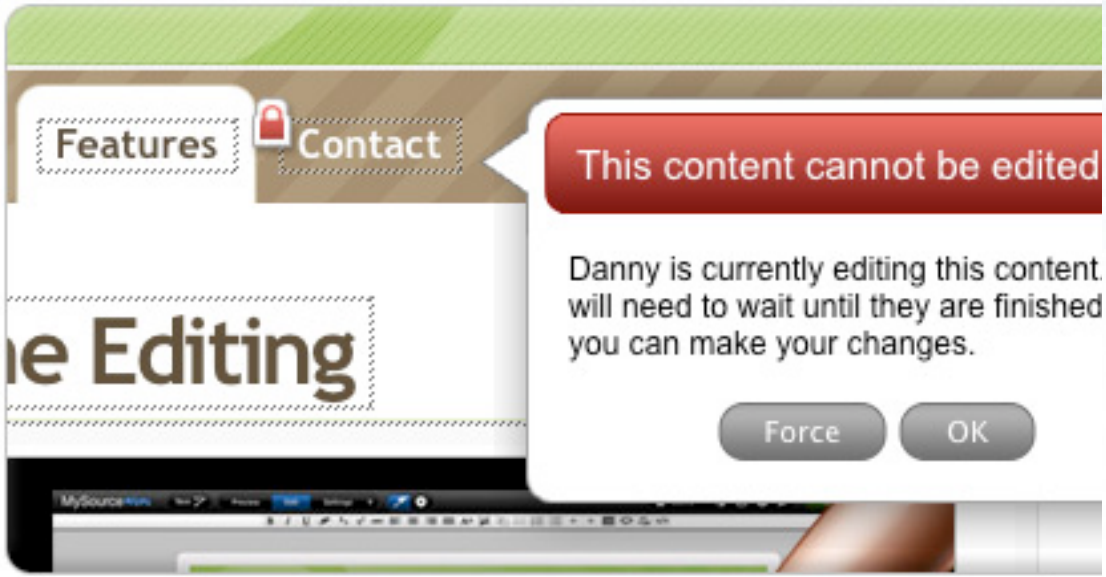
Pitfall 3: Abusing Metaphors



Lock == Trustworthiness



Lock == Protection



Lock == Preservation

Pitfall 3: Abusing Metaphors

1 Use consistent emotional cues

Positive for safe outcomes, negative for risky ones

2 Make safe choices easier to select

And less ideal ones harder to enable

3 Make it easy for the user to change his mind

Reduce the pressure of making the “right” choice right now

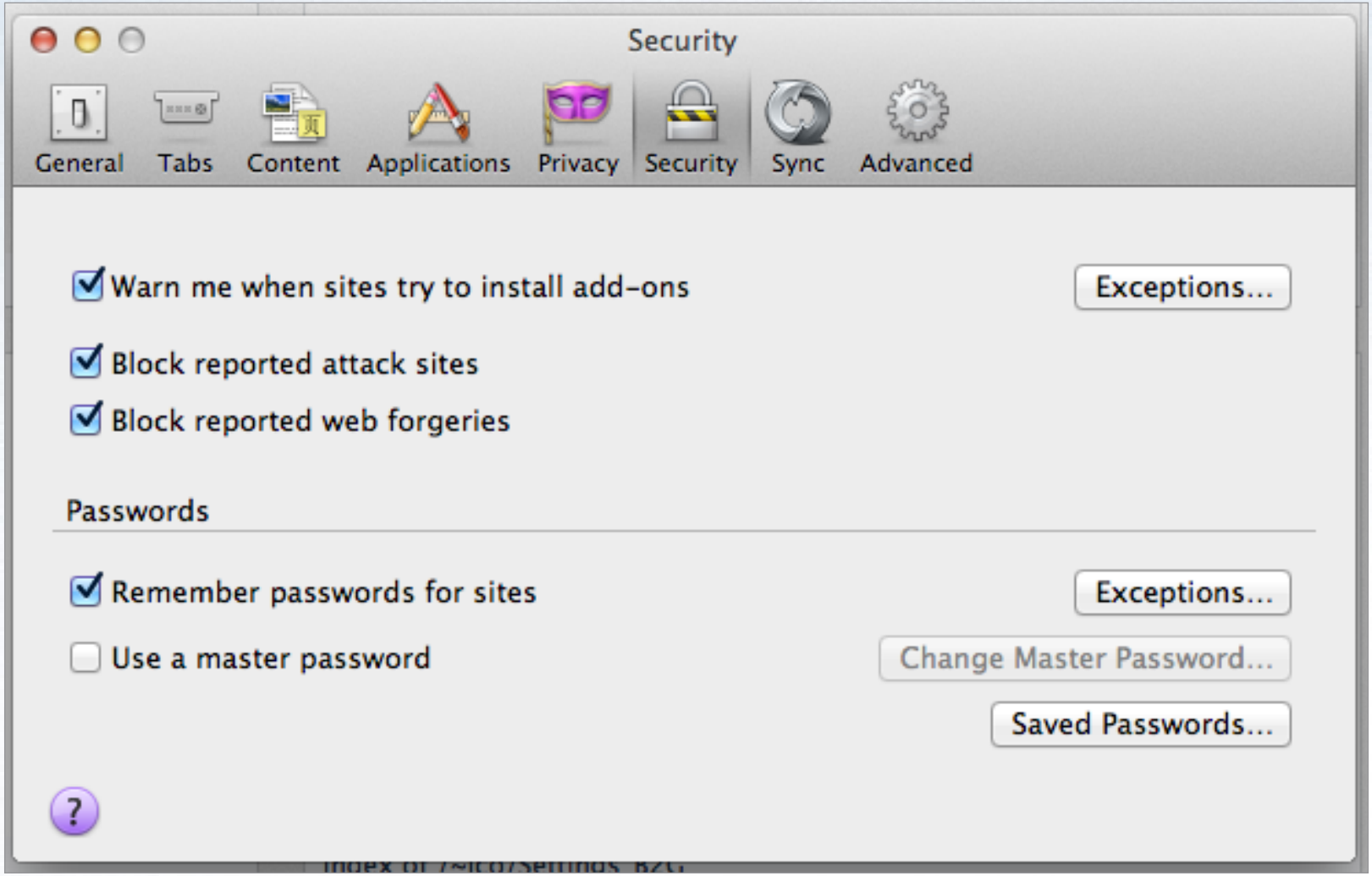
How can we help the user make a thoughtful decision?

Offer Control Without Harming Me

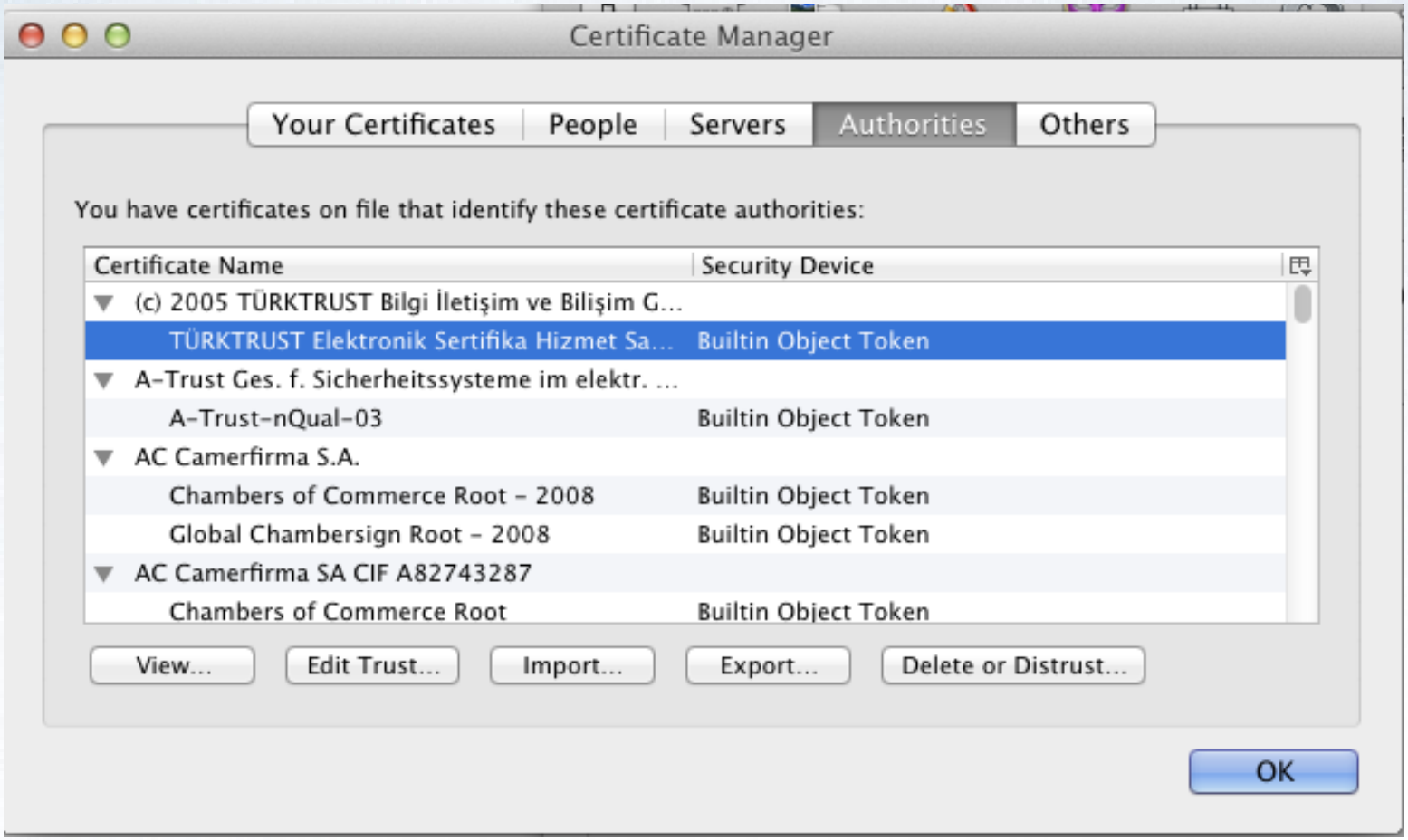
Design Imperative 4

A Tale of Two Cities: Novices vs. Experts

To feel in control, Novices want guidance; Experts want to draw their own conclusions.



Pitfall 1: Being all things to everyone



Pitfall 2: Being useful to no one

1 Set advanced options apart

So that novices won't use these features accidentally

2 Expose raw data to advanced users

Jargon is ok if it's precise and targets a technical audience

3 Provide details in the absence of choice

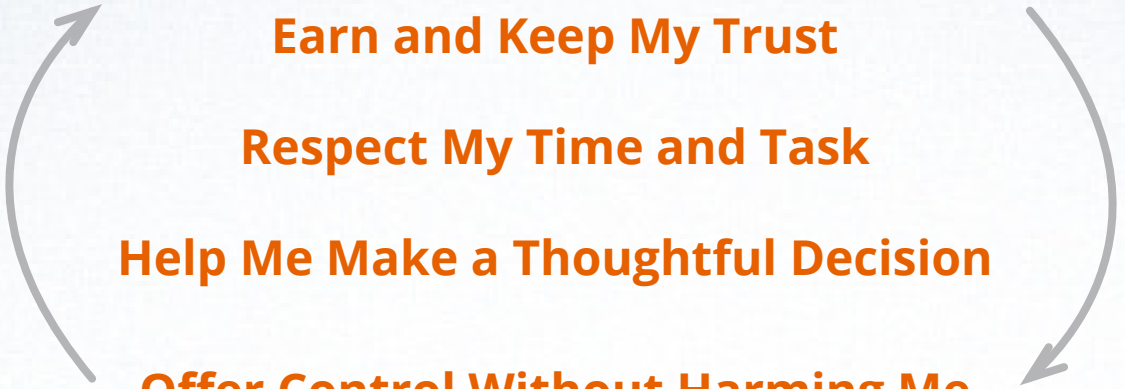
Control doesn't always mean offering choice; being able to understand the problem can still make the user feel in control

How can we offer control without harming expert or novice users?

Review + Case Study

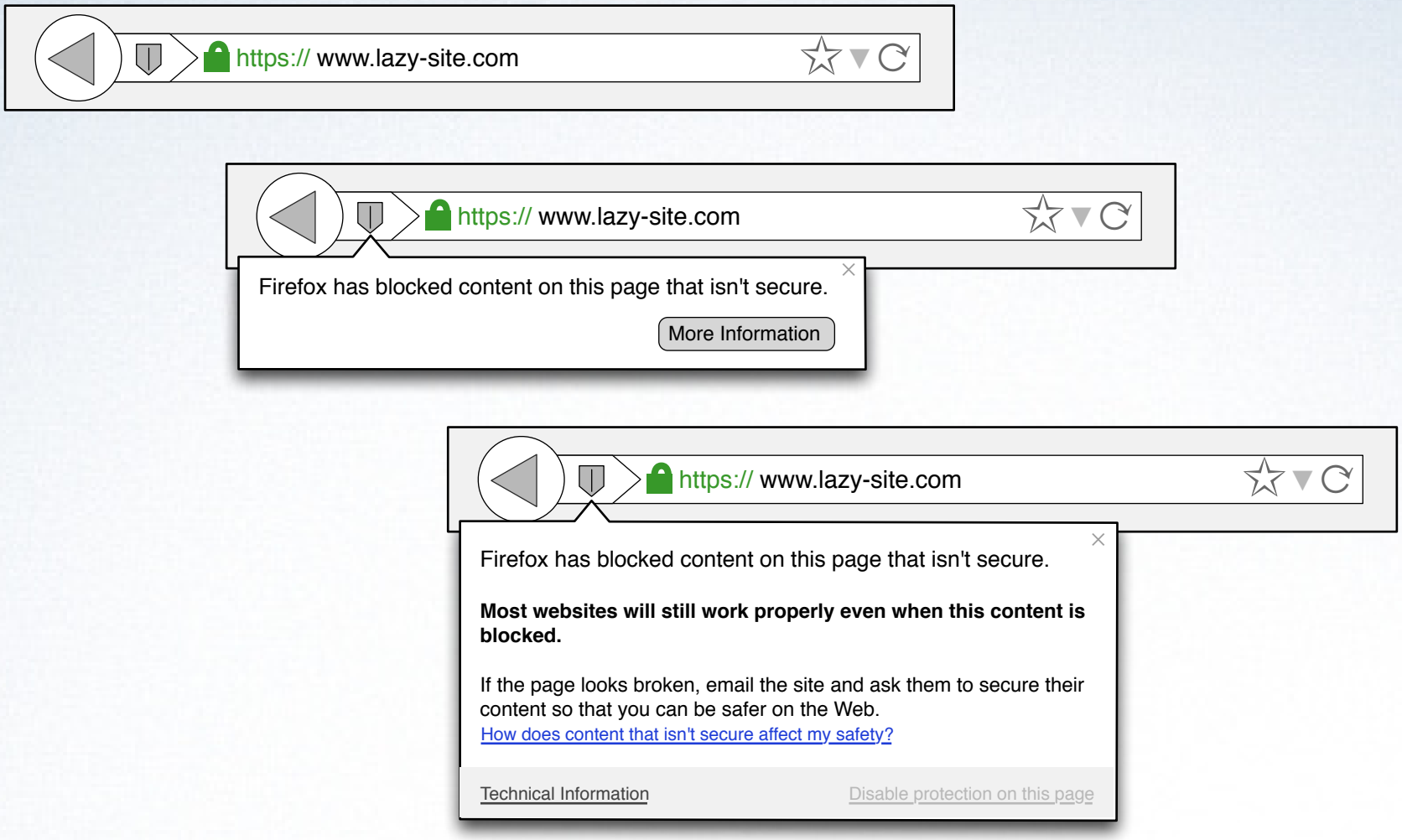
Mixed Content UI

Need to Trust

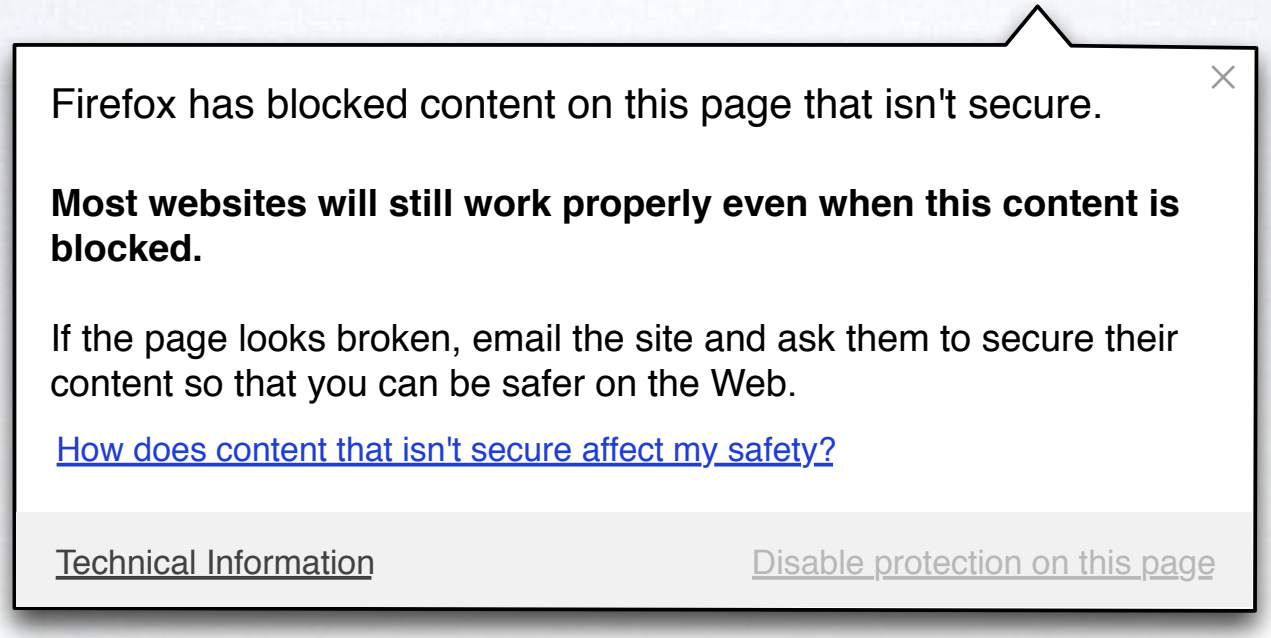


Need to Have Control

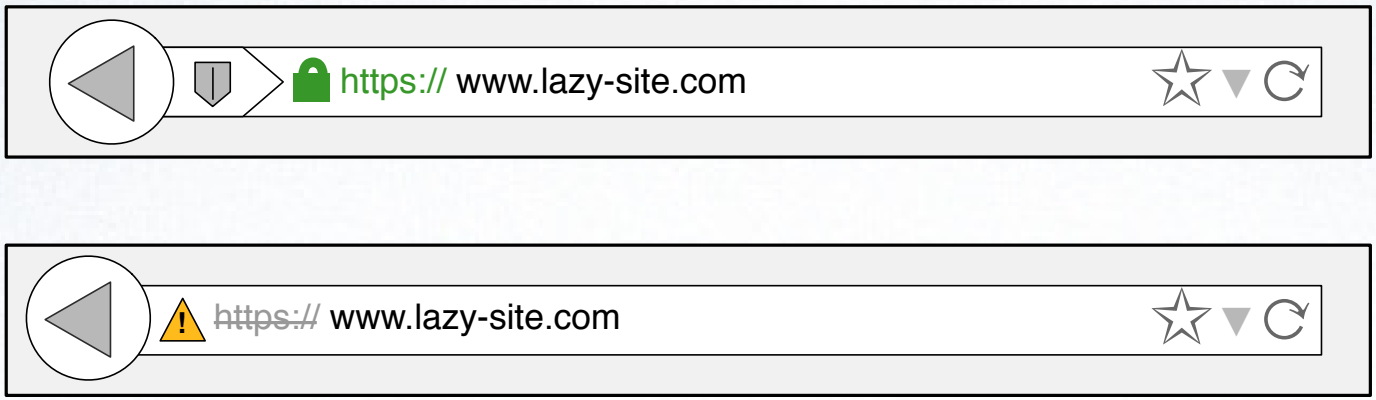
Together, these design imperatives create a cycle of Trust and Control



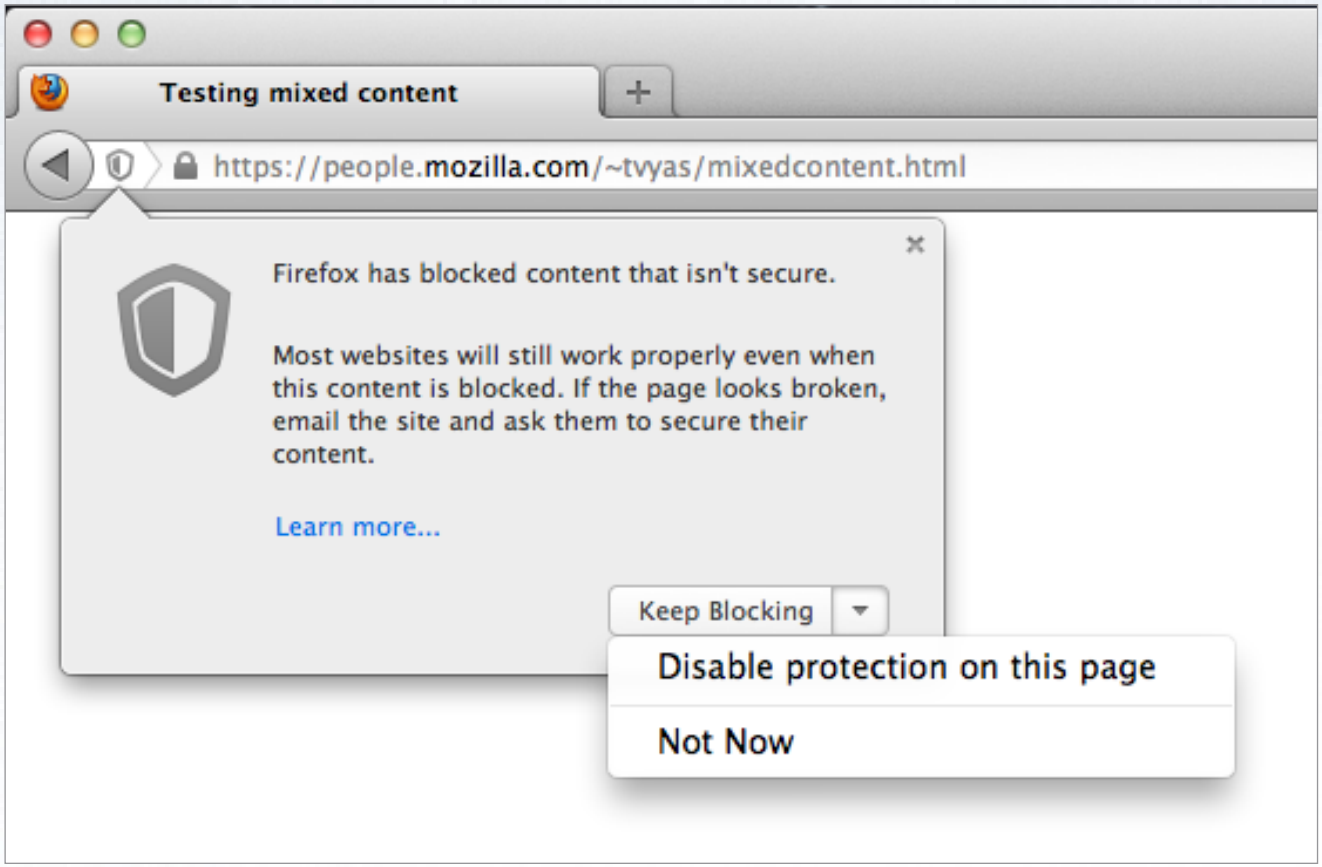
Principle 1: Gradually reveal information and functionality to accommodate user's time and varying levels of technical understanding.



Principle 2: Help the user complete his task within a security mindset so that security and usability are not seen in opposition to each other.



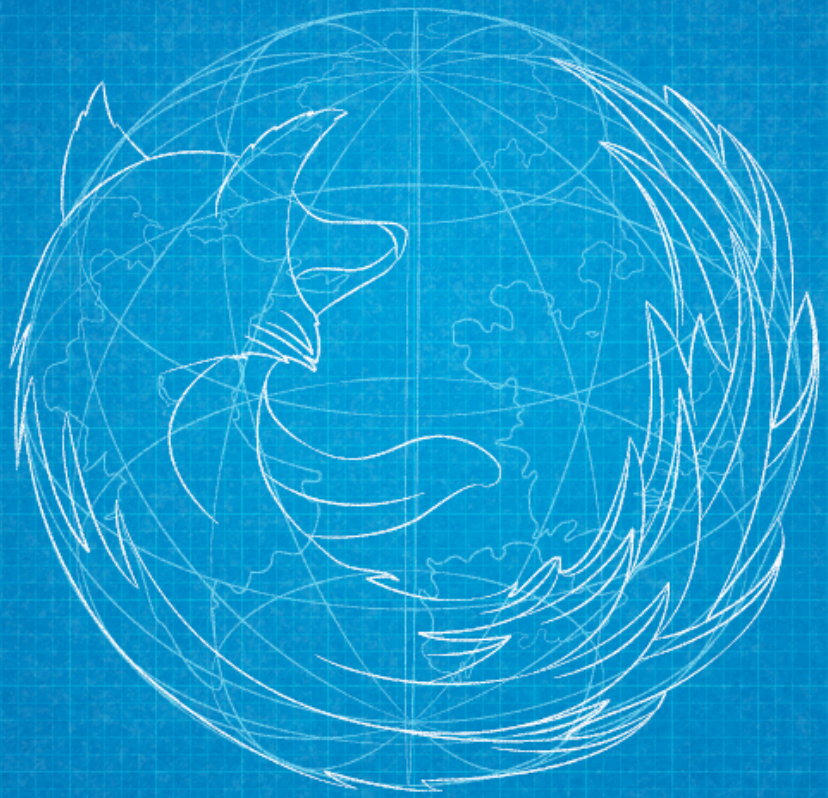
Principle 3: Communicate security messages using consistent emotional cues to help the user make intentional actions.



Lesson from current implementation:
Interface may change, Imperatives must stay the same.

Again: Do people even care about security and privacy?

*People care about being **safe** online. Mozilla can help by making security and privacy meaningful for them.*



Thank you!

Larissa Co | lco@mozilla.com | Jan 16, 2012

Different strategies for different security needs

- Maintain a reputation for security by letting the user know what the browser has already done to protect him from threats.
- Perceived security is just as important as actual security. Inspire confidence in the browser's intentions by crafting a polished user experience.
- Give warnings more weight by interrupting the user's task only when it's truly necessary for him to make a security choice.
- **Reinforce the idea that security is the browser's top priority by choosing messages and symbols that support, not dilute, the significance of the security risk.**
- Foster confidence in the legitimacy of the security feature's source by displaying personalized cues that the user can recognize.
- Create a consistent system that addresses each security concern based on the gravity of the threat, not a one-size-fits-all model for communicating security.
- Reduce user cynicism by minimizing scare tactics; provide balanced, helpful conclusions based on the facts instead.

How can we earn and keep the user's trust?

- Suggest ways for the user complete his task securely so that security and usability are not seen in opposition to each other.
- Eliminate unnecessary interruptions by making the secure choice for the user, as long as it's one that has minimal impact on his task.
- **Make security messages relevant to the user by focusing on the details that affect the his task right now; save lengthy, nuanced descriptions of the problem for users who want more information.**
- Shorten interruption time by explaining the user's choices concisely and displaying them prominently.
- Alleviate interruptions to the user's task by rewarding him for making more secure choices.

How can we respect the user's time and task?

- Help the user understand the nature of the security issue by using clear language that he understands, not technical jargon.
- Guide the user in making a more secure choice by breaking down facets of the decision into smaller, concrete touchpoints.
- Simplify the user's choice by making more secure choices easy to select, less secure ones harder to enable.
- **Communicate security messages using consistent positive or negative emotional cues to help the user make intentional choices.**
- Place the user in a security mindset by framing choices as security decisions instead of task-enabling ones.
- Reduce confusion by explaining apparent contradictions between what the user perceives and the nature of the threat.
- Minimize the fear of making the "right" choice by allowing the user to revert previous decisions.

How can we help the user make a thoughtful decision?

- Gradually reveal information and functionality to accommodate users' time and varying levels of technical understanding.
- Prevent accidental discovery and thoughtless use of advanced controls by distancing its access point from the basic controls.
- **Balance simplicity and power by providing cues that distinguish and set apart advanced options from everyone else's view.**
- Expose raw data to advanced users. Avoid misrepresenting or oversimplifying information that can lead to incorrect inferences.
- Maintain the user's perception of control by providing detailed information about the threat even when the user doesn't have the option to disable the browser's protection.
- Within the advanced controls section, encourage thoughtful decisions by making technical information more prominent than the options to disable the browser's protective measures.

How can we offer control without harming expert or novice users?