What do they think they are doing?

When Security meets Usability…
Do you use Webmail?
Do you use E-Mail for private stuff?
Do you use Social Networking sites?
Have you ever downloaded your address book to a Social Networking site?
Check your contacts and see who is LinkedIn

TIP
Want to see other ways to find your contacts?

1. Select your email provider
   - Yahoo!
   - Gmail
   - America Online
   - Hotmail

2. Login to your Webmail
   - Username: [Your Username]@yahoo.com
   - Password: [Your Password]

Your privacy is our top concern. Your contacts are your private information. LinkedIn will not store your username and password and any information you upload will be securely imported for your own use. LinkedIn will not send your contacts any e-mail. For more information please see the LinkedIn Privacy Policy.
Connect with Friends

The whole point of Flixster is to share movie ratings with friends. See which of your friends may already be on Flixster.

(Of course, you don't have to invite any friends, but don't blame us if you get bored and lonely.)

Which address book would you like to check? You will be able to choose which friends to invite on the following pages.

Hotmail®

Yahoo! Mail

gmail

AOL Mail™

Select >

Select >

Select >

Select >

---- OR ----

Copy and paste the text below into an email. Send the email to friends to invite them.

Hi,

I just took a movie quiz at Flixster.com. If you come take it too we can see if we like the same movies.

http://www.flixster.com/servlet/invite/693013361wnjABCm

Test
Get Address Book
Enter your Yahoo details below. On the next page you will be able to select who to connect with.

Yahoo Email Address: testflixster@mail.yahoo.com
Yahoo Password: [blank]

Note: Flixster does not store this information in any way.
unexpected invitations
Spamming in plain sight!
Get Address Book

Enter your Yahoo details below. On the next page you will be able to select who to connect with.

Yahoo Email Address: testflixter@mail.yahoo.com
Yahoo Password: [field]

Note: Flixster does not store this information in any way.
Phishing in plain sight!
“But hey, it's common practice!”
Check your contacts and see who is LinkedIn

1. Select your email provider

   - Yahoo!
   - Gmail
   - America Online
   - Hotmail

2. Login to your Webmail

   Username: [your_username]@yahoo.com
   Password: [your_password]

TIP: Want to see other ways to find your contacts?

Your privacy is our top concern. Your contacts are your private information. LinkedIn will not store your username and password and any information you upload will be securely imported for your own use. LinkedIn will not send your contacts any e-mail. For more information please see the LinkedIn Privacy Policy.
It's all about trust.
It's about what people think is happening.
“Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.”

(Kim Cameron, The Laws Of Identity)
“Nor were users clamoring for a single Microsoft identity service to be aware of all their Internet activities. As a result, Passport failed in its mission of being an identity system for the Internet.”

(Kim Cameron, The Laws Of Identity)
Flixster and LinkedIn?
justifiable!
engineer user trust
Get Address Book
Enter your Yahoo details below. On the next page you will be able to select who to connect with.

Yahoo Email Address: testflixster@mail.yahoo.com
Yahoo Password: 

Note: Flixster does not store this information in any way.
Concern

Will Flixster store my credentials?

End Concern
Get Address Book

Enter your Yahoo details below. On the next page you will be able to select who to connect with.

Yahoo Email Address: testflixster@mail.yahoo.com

Yahoo Password: 

Note: Flixster does not store this information in any way.
Get Address Book

Enter your Yahoo details below. On the next page you will be able to select who to connect with.

**Yahoo Email Address:** testflixtser@mail.yahoo.com

**Yahoo Password:**

[Continue >]

*Note:* Flixster does not store this information in any way.
Demandez la Carte Personnelle

Par mesure de sécurité, aucune des données que vous introduirez dans ces formulaires ne sera transmise sur Internet.

Renseignements personnels

Titre:
Nom:
Prénom:
Adresse:
N° / Boîte:
Code Postal:
Localité:
Adresse e-mail:
Téléphone privé:
Date de naissance:
État Civil:
Nombre de personnes à charge:
Habitation:
Depuis :
Nom agence bancaire:
Depuis (approximativement):
Adresse:
N° de compte personnel:
Prénom de votre mère:

M.  Mme

Célibataire  Marié(e)  Cohabitant
Divorcé(e)  Veuf/Veuve

Propriétaire  Locataire (mois/année)

(par mesure de sécurité)
That's a lot of financial information. Do I trust the Internet with it?
“For security reasons, the information you enter into this Web form will never be transmitted over the Internet.”
http://
users trust content
reputable sites teach
even if the content is implausible
“For security reasons, the information you enter into this Web form will never be transmitted over the Internet.”
idea
can content be an indicator?
personalize your bank's appearance!
<teaching>
“If it's your photo, then it's safe to enter your password!”
WRONG
Schechter, Dhamija, Ozment, Fischer (2007): *The Emperor's New Security Indicators*
reputable sites teach
disregard other indicators
users trust content
“The photo server will be back up shortly. We're sorry for the inconvenience.”
attack successful
Browsers
Downs, Holbrook, Cranor (2006): *Decision Strategies and Susceptibility to Phishing*
mental models meet security indicators
“Huh, I'm really not certain, but I'm intrigued by it.”
“Well, I mean, I'm figuring like, based off what it seemed like an encrypted page kind of, I don't know, like walks out or crypts into the circle so that it can't be read.”
<wisdom>
Unable to verify the identity of people.w3.org 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 people.w3.org, 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 accept this certificate for the purpose of identifying the web site people.w3.org?

Examine Certificate...

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this web site
“Possible Reasons for this Error”
Certification Authority ... Certificate
<jargon>server misconfiguration</jargon>
there might be an attack, and it is possibly malicious
(This dialogue might be the last line of defense against an attack.)
<impossible>
Please contact the site's webmaster
</impossible>
you should examine this certificate carefully
Unable to verify the identity of people.w3.org 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 people.w3.org, 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 accept this certificate for the purpose of identifying the web site people.w3.org?

Examine Certificate...

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this web site
Could not verify this certificate because the issuer is unknown.

Issued To
- Common Name (CN): people.w3.org
- Organization (O): <Not Part Of Certificate>
- Organizational Unit (OU): <Not Part Of Certificate>
- Serial Number: 01:E3:F6

Issued By
- Common Name (CN): CA Cert Signing Authority
- Organization (O): Root CA
- Organizational Unit (OU): http://www.cacert.org

Validity
- Issued On: 05/02/06
- Expires On: 04/08/06

Fingerprints
“Could not verify this certificate because the issuer is unknown.”
“Issued By”
Downs, Holbrook, Cranor (2006): *Decision Strategies and Susceptibility to Phishing*
“Basically that it’s kind of like the **elevator certificate**. For whatever reason, they don’t have it. But at that point sometimes when you go into the elevators you can see if their certificate is up to date or if it’s not current. And that’s kind of what that meant for me.”
Elevator Certificate: The writing on the wall that you read while your elevator is in free fall.
users trust content
useless security indicators teach
disregard advice
<attack>
You have attempted to establish a connection with "northwestairlines.112.207.net". However, the security certificate presented belongs to "*.concoursecommunications.com". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "northwestairlines.112.207.net", please cancel the connection and notify the site administrator.
You have attempted to establish a connection with "northwestairlines.112.2o7.net".

However, the security certificate presented belongs to "*.concoursecommunications.com". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
“possible, though unlikely”
WRONG
If you suspect the certificate shown does not belong to “northwestairlines.112.2o7.net”, please cancel the connection and notify the site administrator.
good advice!
WRONG
In this case: “attacked” by a hotspot
“legitimate” attack
“legitimate” attacks teach
users trust content
disregard advice
but they shouldn't need to
there is often good information available
there is often good advice to be given
Web Security Context Working Group
What can we tell users to help them make the right decisions?
how?
hard problems
security usability: much research to be done
What decisions should users make at all?
What decisions should we keep away from them?
web user agents are infrastructure
Whose Web do we change?
Whose Web might we break?
future
platform
applications
local

(Widgets)
remote

(mash-ups)
ubiquitous
scan
print
find your kids
open your safe
turn off the fridge
divorce
been there
done that
e.g.,
same-origin policy
so
Flixster won't get at your Webmail!
but Flixster got the password!
technical defense
attack the human!
people want convenience
features
the unexpected
and they'll get it!
help, don't hinder
usability
mental models
metaphors
indicators
best practice
enable flexibility
author
explain
exchange
read
use
strategies
policies
<http://www.w3.org/TR/access-control/>
punching holes into the sandbox
allow https://*.w3.org
read the address book
not the inbox
first steps!
<challenges>
If TLS confuses people, what will policies do to them?
How do we give flexibility to users?
What does all this really mean to users?