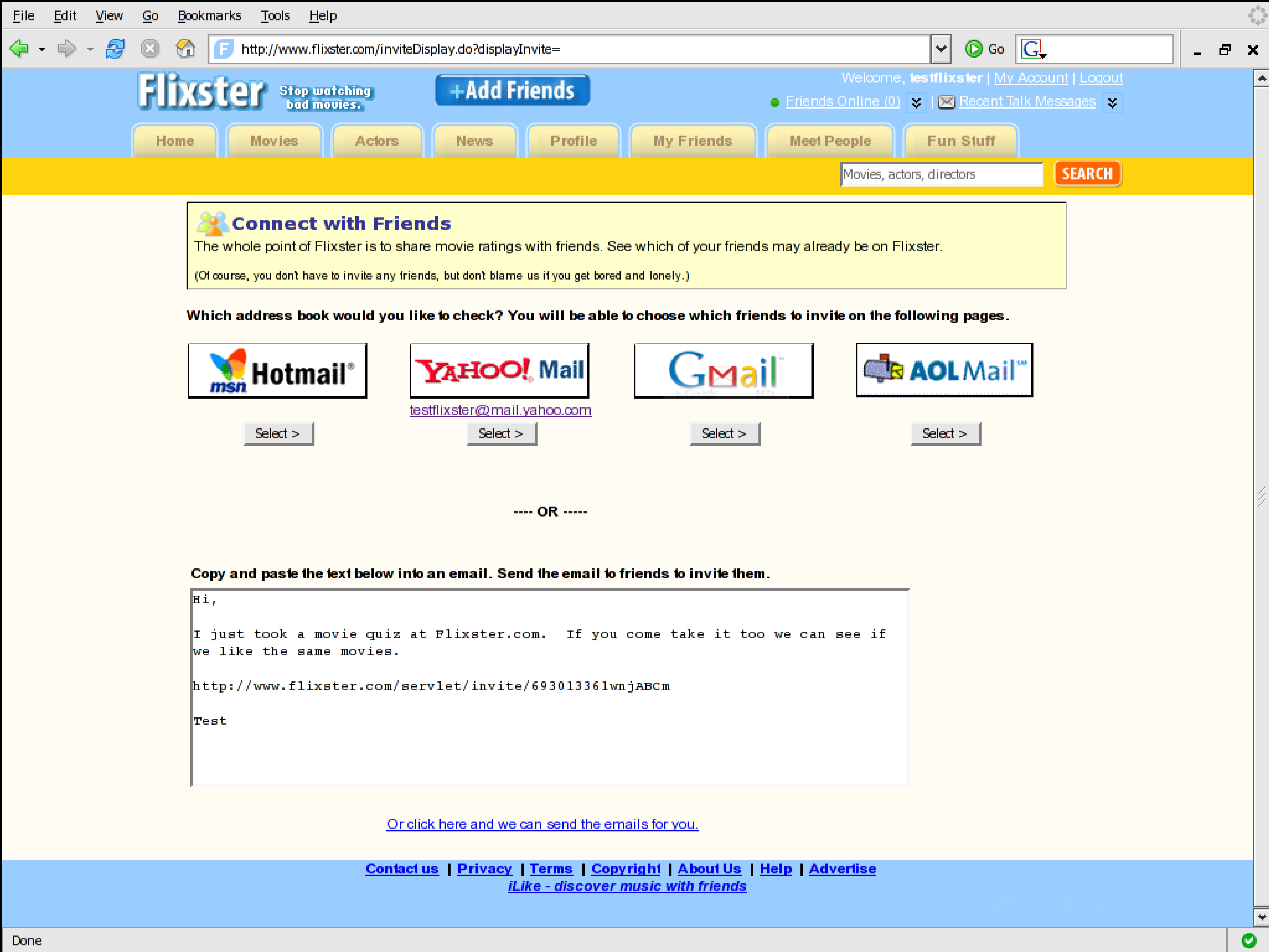
What do they think they are doing?

When Security meets Usability...


File
Edit
View
Go
Bookmarks
Tools
Help
http://www.flixster.com/inviteDisplay.do?displayInvite=
Go
Flixster
Stop watching bad movies.
+Add Friends
Welcome, testflixster | My Account | Logout
Friends Online (0) | Recent Talk Messages
Home
Movies
Actors
News
Profile
My Friends
Meet People
Fun Stuff
Movies, actors, directors
SEARCH
Hotmail
msn
YAHOO! Mail
GMail
AOL Mail
Select >
Select >
Select >
Select >
Done

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 dont have to invite any friends, but dont 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.

testflixster@mail.yahoo.com

---- OR -----

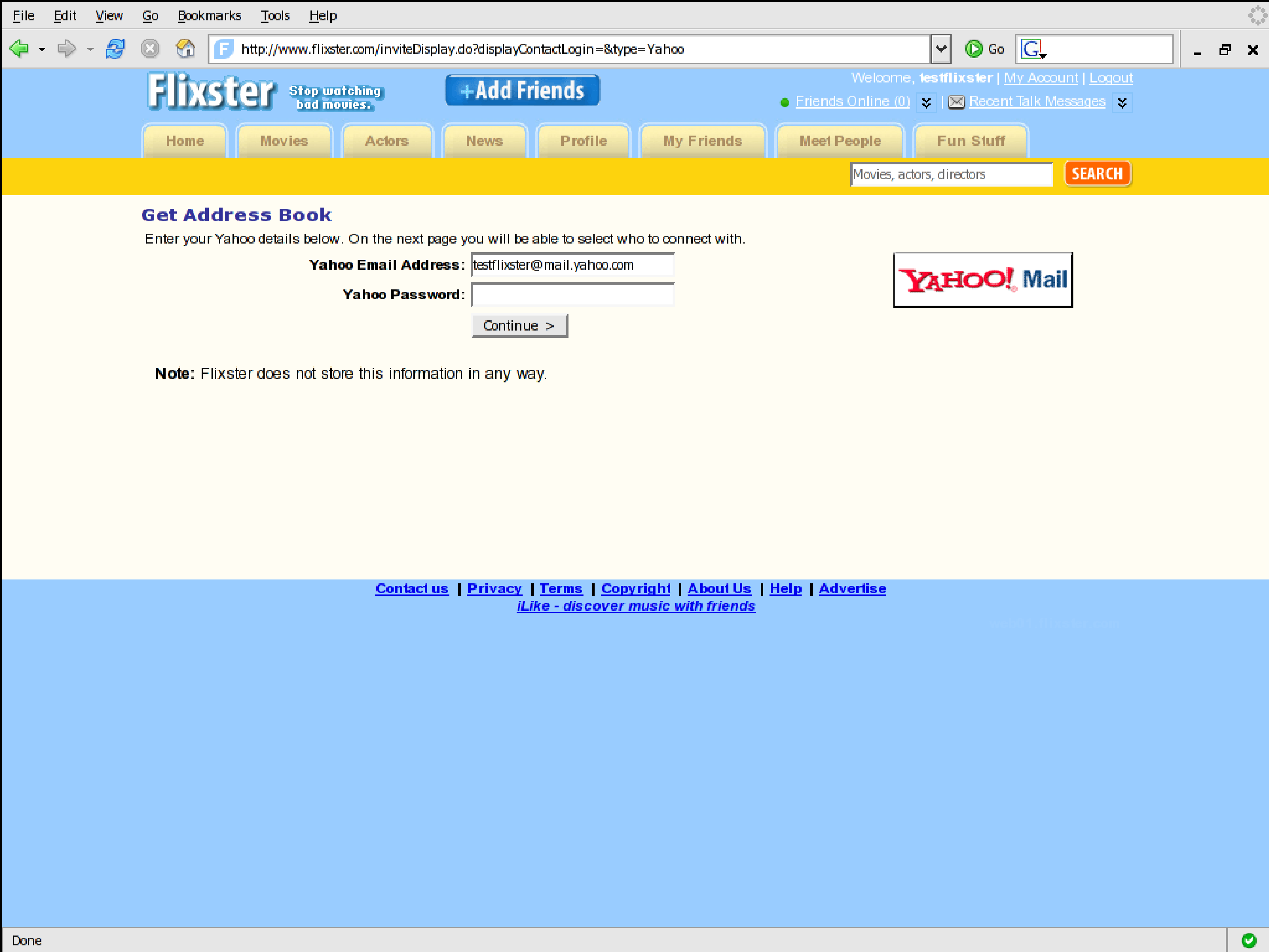
Copy and paste the text below into an email. Send the email to friends to invite them.

```
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/69301336lwnjABCm

Test
```

Or click here and we can send the emails for you.

Contact us | Privacy | Terms | Copyright | About Us | Help | Advertise

iLike - discover music with friends



http://www.flixster.com/inviteDisplay.do?displayContactLogin=&type=Yahoo

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.

Contact us | Privacy | Terms | Copyright | About Us | Help | Advertise

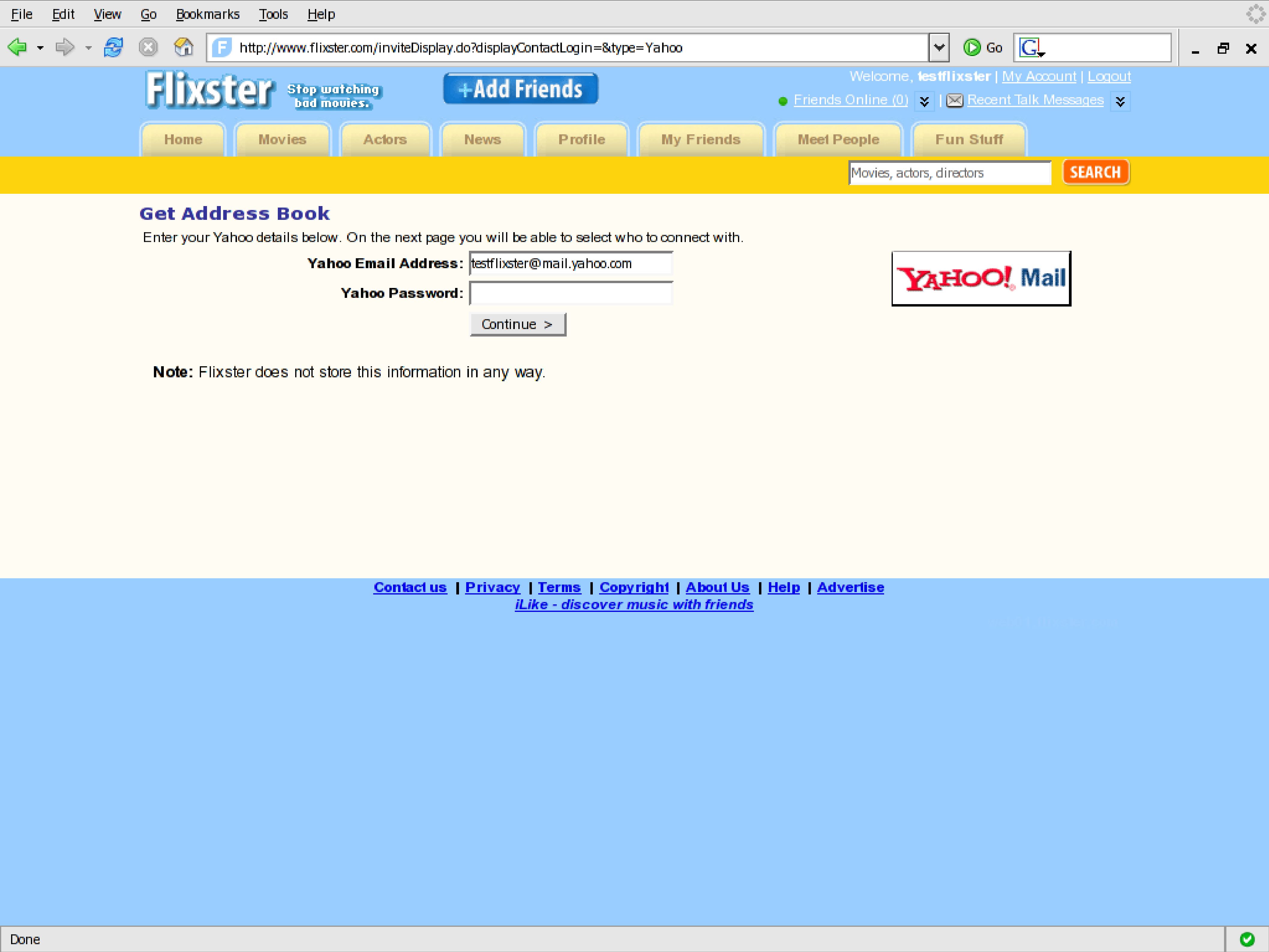
iLike - discover music with friends

unexpected invitations

/.

<slashdot>

Spamming in plain sight!


File
Edit
View
Go
Bookmarks
Tools
Help
http://www.flixster.com/inviteDisplay.do?displayContactLogin=&type=Yahoo
Go
Flixster
Stop watching bad movies.
+Add Friends
Welcome, testflixster | My Account | Logout
Friends Online (0) | Recent Talk Messages
Home
Movies
Actors
News
Profile
My Friends
Meet People
Fun Stuff
Movies, actors, directors
SEARCH
YAHOO! Mail

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

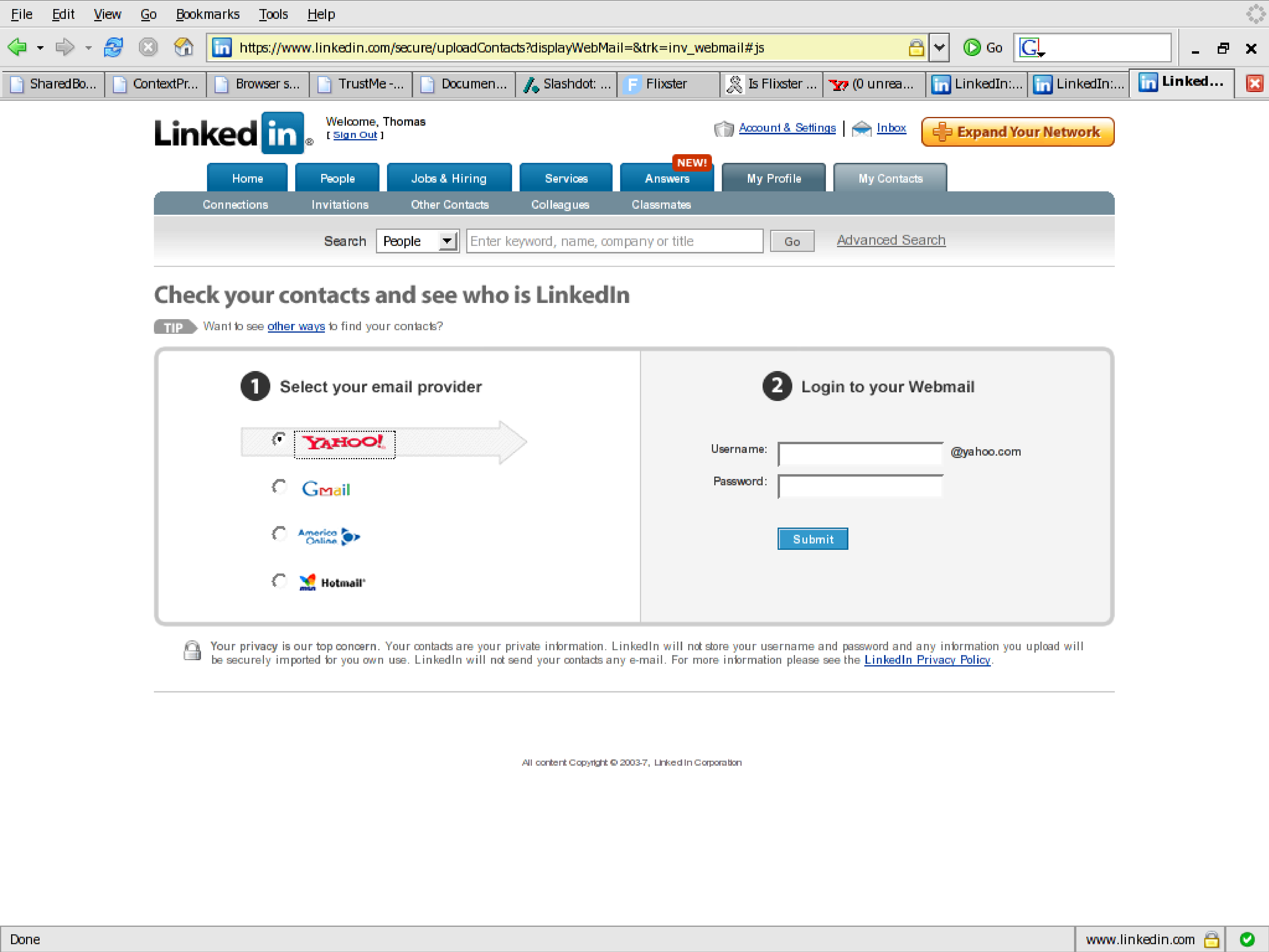
Yahoo Password:

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

Contact us | Privacy | Terms | Copyright | About Us | Help | Advertise
iLike - discover music with friends
Done

Phishing in plain sight!

“But hey, it's **common** practice!”



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: @yahoo.com

Password:

Submit

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 you own use. LinkedIn will not send your contacts any e-mail. For more information please see the LinkedIn Privacy Policy.

All content Copyright © 2003-7, LinkedIn Corporation

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)

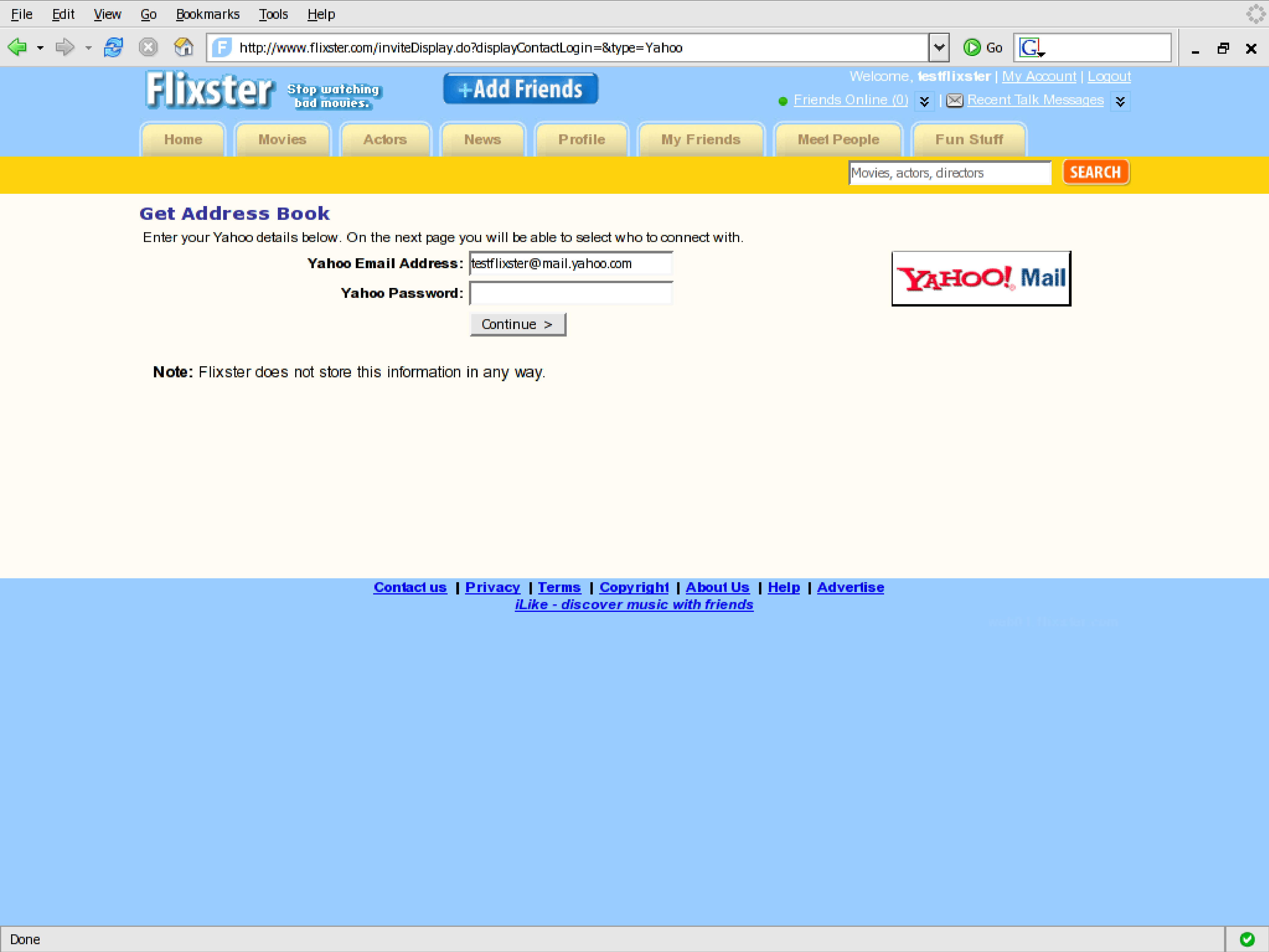
“Nor were users clamoring for a single Microsoft identity service to be aware of all their Internet activities. As a result, Passport failed in its mission of being an identity system for the Internet.”

(Kim Cameron, The Laws Of Identity)

Flixster and LinkedIn?

justifiable!

engineer user **trust**


File
Edit
View
Go
Bookmarks
Tools
Help
http://www.flixster.com/inviteDisplay.do?displayContactLogin=&type=Yahoo
Go
Flixster
Stop watching bad movies.
+Add Friends
Welcome, testflixster | My Account | Logout
Friends Online (0) | Recent Talk Messages
Home
Movies
Actors
News
Profile
My Friends
Meet People
Fun Stuff
Movies, actors, directors
SEARCH
YAHOO! Mail
Contact us | Privacy | Terms | Copyright | About Us | Help | Advertise
iLike - discover music with friends
Done

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:

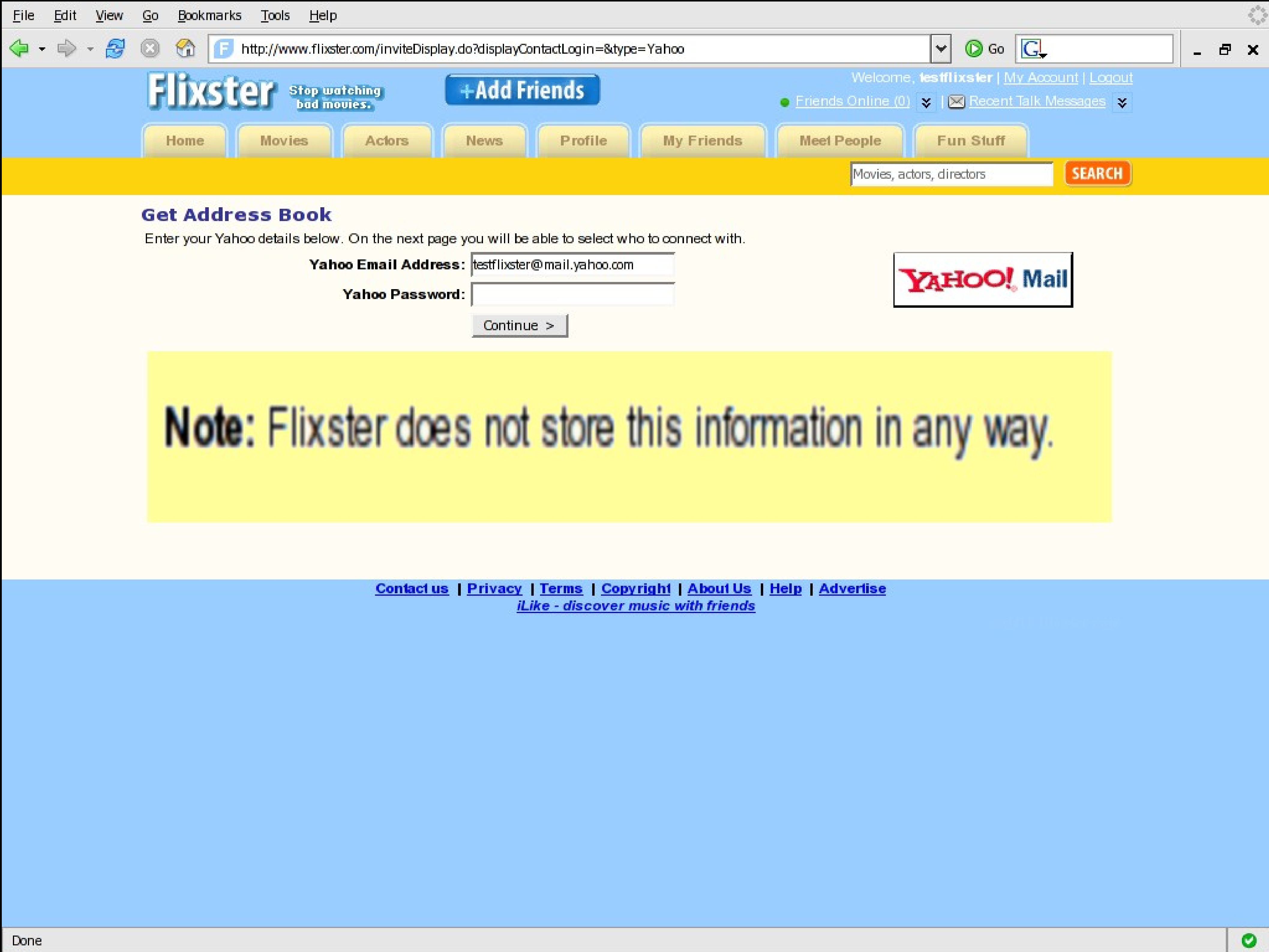
Continue >

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

<concern>

Will Flixster store my credentials?

</concern>



File Edit View Go Bookmarks Tools Help
http://www.flixster.com/inviteDisplay.do?displayContactLogin=&type=Yahoo
Go
Flixster Stop watching bad movies.
+Add Friends
Welcome, testflixster | My Account | Logout
Friends Online (0) | Recent Talk Messages
Home
Movies
Actors
News
Profile
My Friends
Meet People
Fun Stuff
Movies, actors, directors
SEARCH

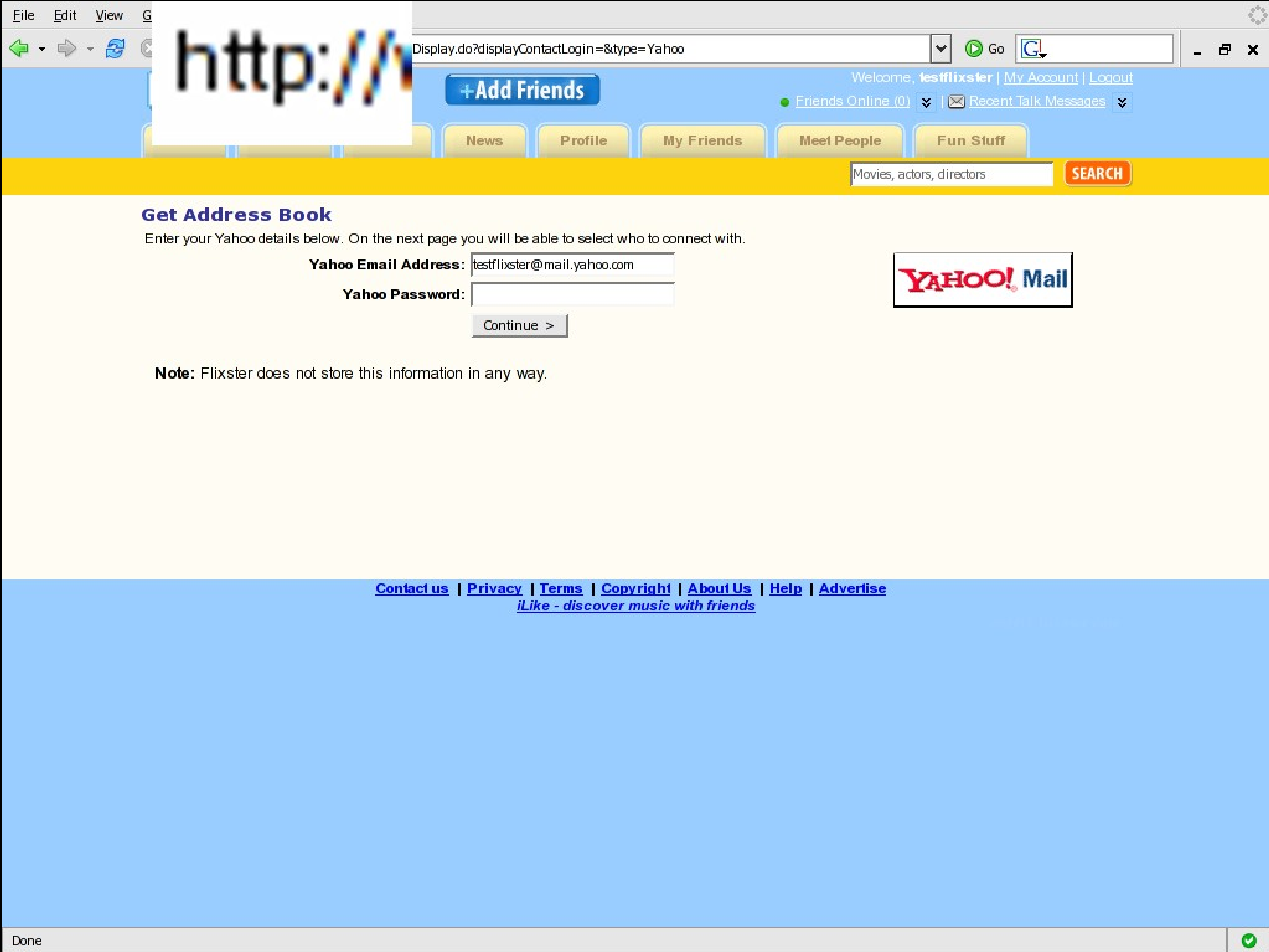
Get Address Book

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.

Contact us | Privacy | Terms | Copyright | About Us | Help | Advertise
iLike - discover music with friends
Done


File
Edit
View
G
http://
Display.do?displayContactLogin=&type=Yahoo
Go
+Add Friends
Welcome, testflixster | My Account | Logout
Friends Online (0) | Recent Talk Messages
News
Profile
My Friends
Meet People
Fun Stuff
Movies, actors, directors
SEARCH
YAHOO! Mail
Done

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:

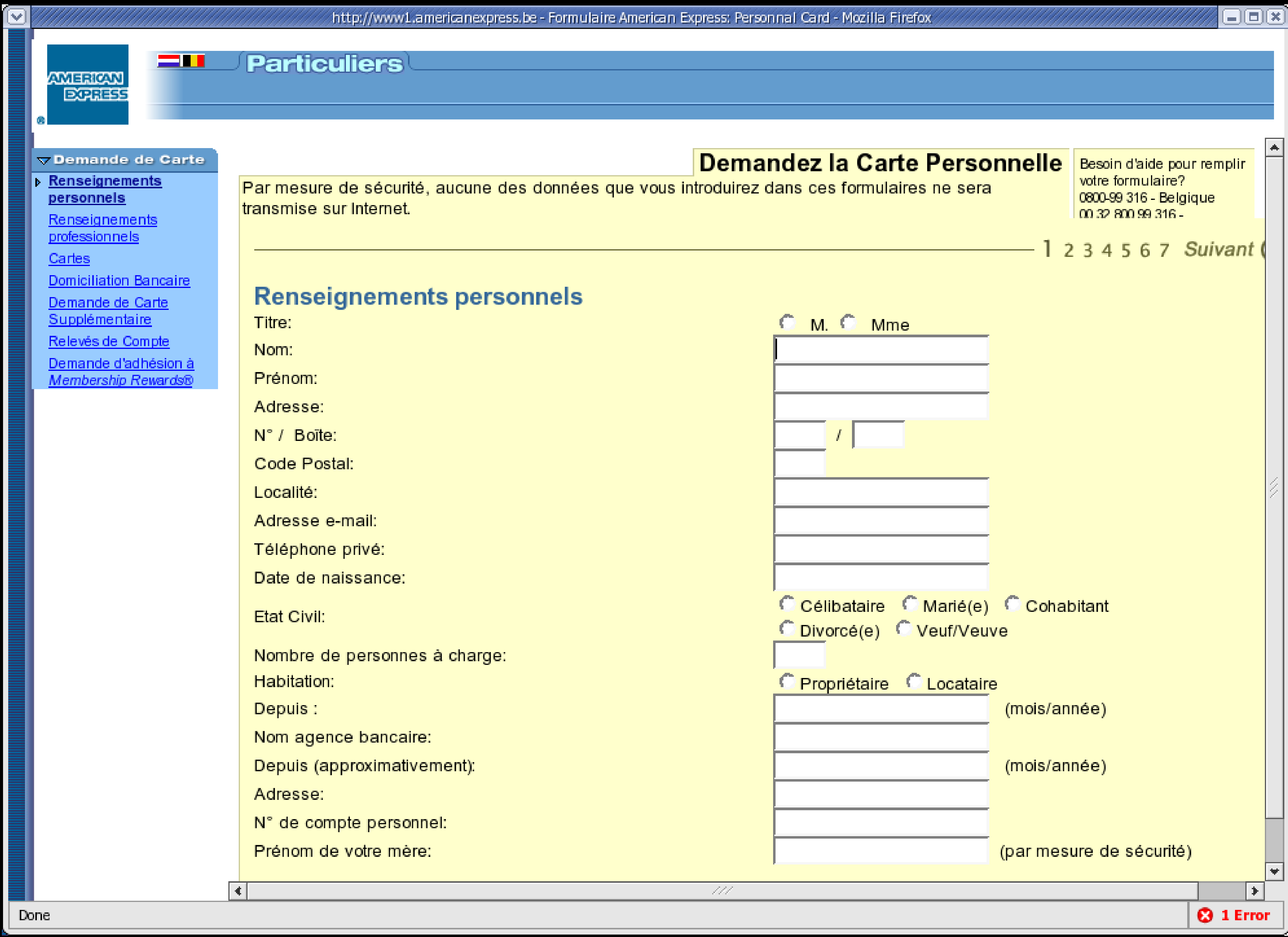
Continue >

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

Contact us | Privacy | Terms | Copyright | About Us | Help | Advertise

iLike - discover music with friends

http://


http://www1.americanexpress.be - Formulaire American Express: Personnal Card - Mozilla Firefox
AMERICAN EXPRESS
Particuliers
Demande de Carte
Renseignements personnels
Renseignements professionnels
Cartes
Domiciliation Bancaire
Demande de Carte Supplémentaire
Relevés de Compte
Demande d'adhésion à *Membership Rewards®*
Done
1 Error

Demandez la Carte Personnelle

Besoin d'aide pour remplir votre formulaire?
0800-99 316 - Belgique
00 32 800 99 316 -

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

1 2 3 4 5 6 7 *Suivant*

Renseignements personnels

Titre: ○ M. ○ Mme

Nom:

Prénom:

Adresse:

N° / Boîte: /

Code Postal:

Localité:

Adresse e-mail:

Téléphone privé:

Date de naissance:

Etat Civil: ○ Célibataire ○ Marié(e) ○ Cohabitant ○ Divorcé(e) ○ Veuf/Veuve

Nombre de personnes à charge:

Habitation: ○ Propriétaire ○ Locataire

Depuis : (mois/année)

Nom agence bancaire:

Depuis (approximativement): (mois/année)

Adresse:

N° de compte personnel:

Prénom de votre mère: (par mesure de sécurité)

<concern>

That's a lot of private information. Do I trust the Internet with it?

</concern>

"For security reasons, the information you enter into this Web form will never be transmitted over the Internet."

http://

reputable sites **teach**

users trust **content**

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>

if users trust content

...

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**

users trust **content**

disregard **other**

indicators

users trust **content**

“The photo server will be back up shortly. We're sorry for the inconvenience.”

password: _

password: * _

password: * * _

password: * * * * * *

attack **successful**

<Browsers>

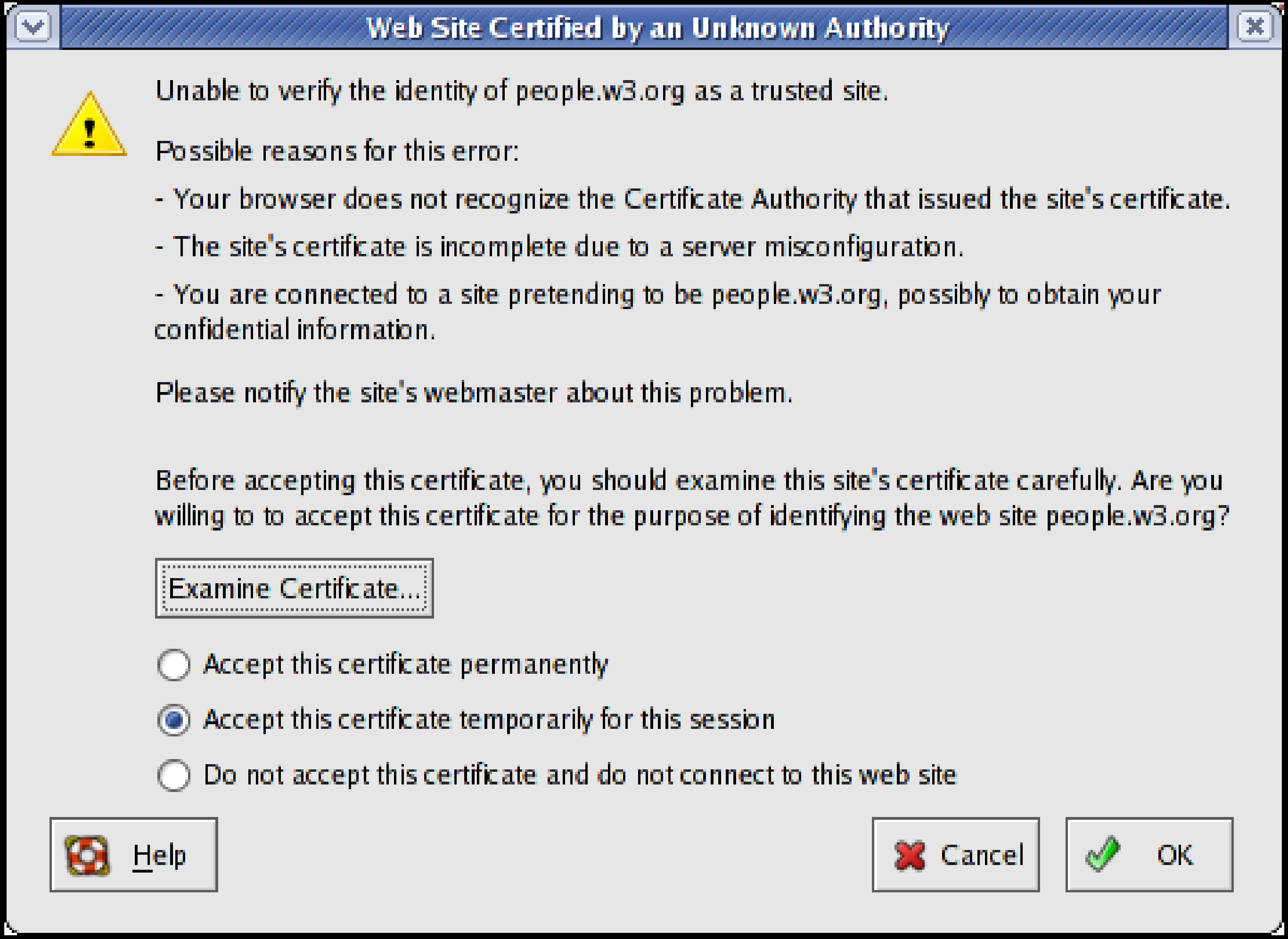
Downs, Holbrook, Cranor (2006): *Decision Strategies and Susceptibility to Phishing*

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>



Web Site Certified by an Unknown Authority

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 to accept this certificate for the purpose of identifying the web site people.w3.org?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

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

<speculation>

“Possible Reasons for this Error”

</speculation>

<jargon>

Certification Authority … Certificate

</jargon>

<jargon>

server misconfiguration

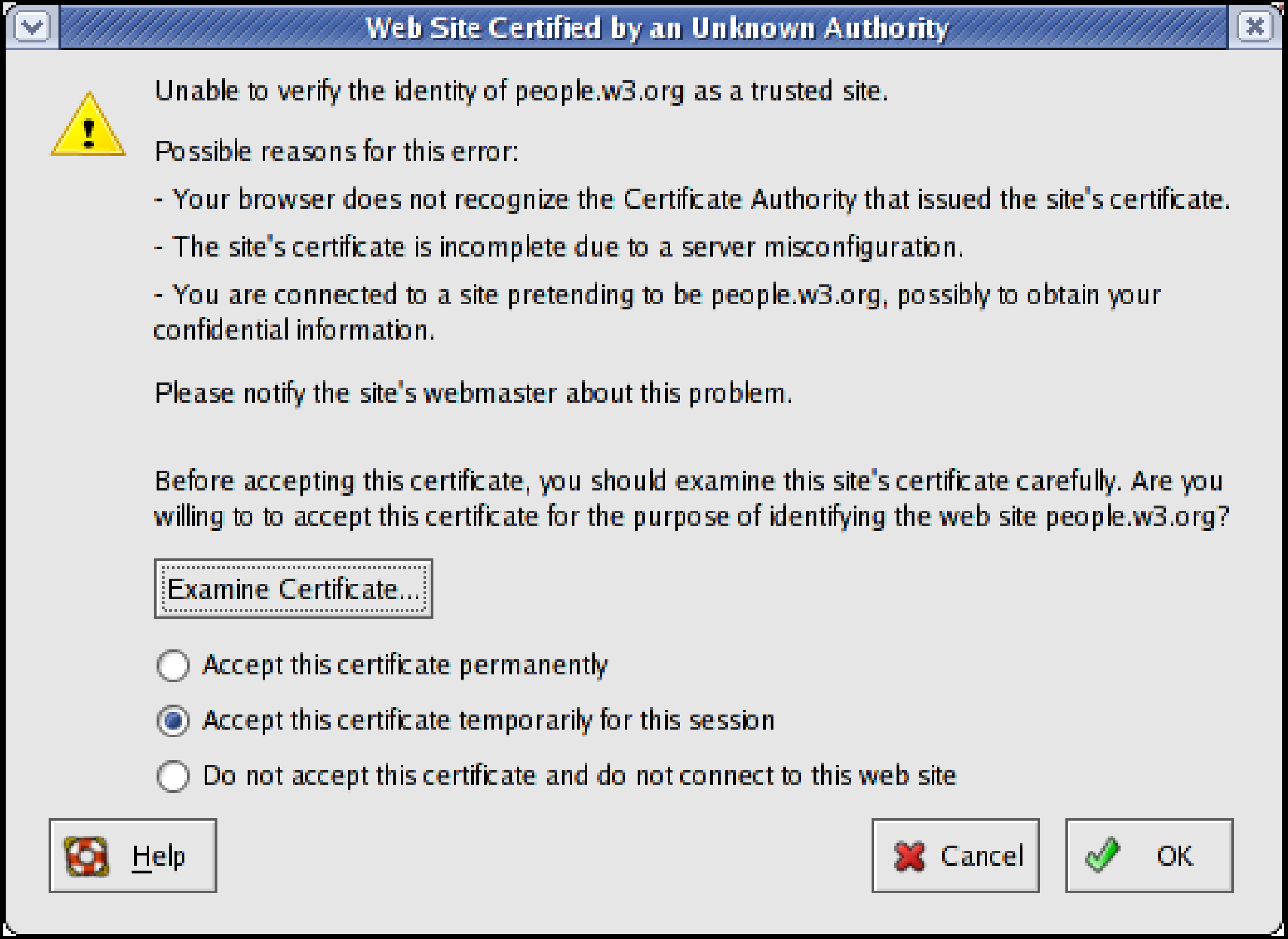
</jargon>

<oops>

there ***might*** be an attack, and it is ***possibly*** malicious

</oops>

This is your last line of defense against the guy running **ettercap** right now.



Web Site Certified by an Unknown Authority

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 to accept this certificate for the purpose of identifying the web site people.w3.org?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

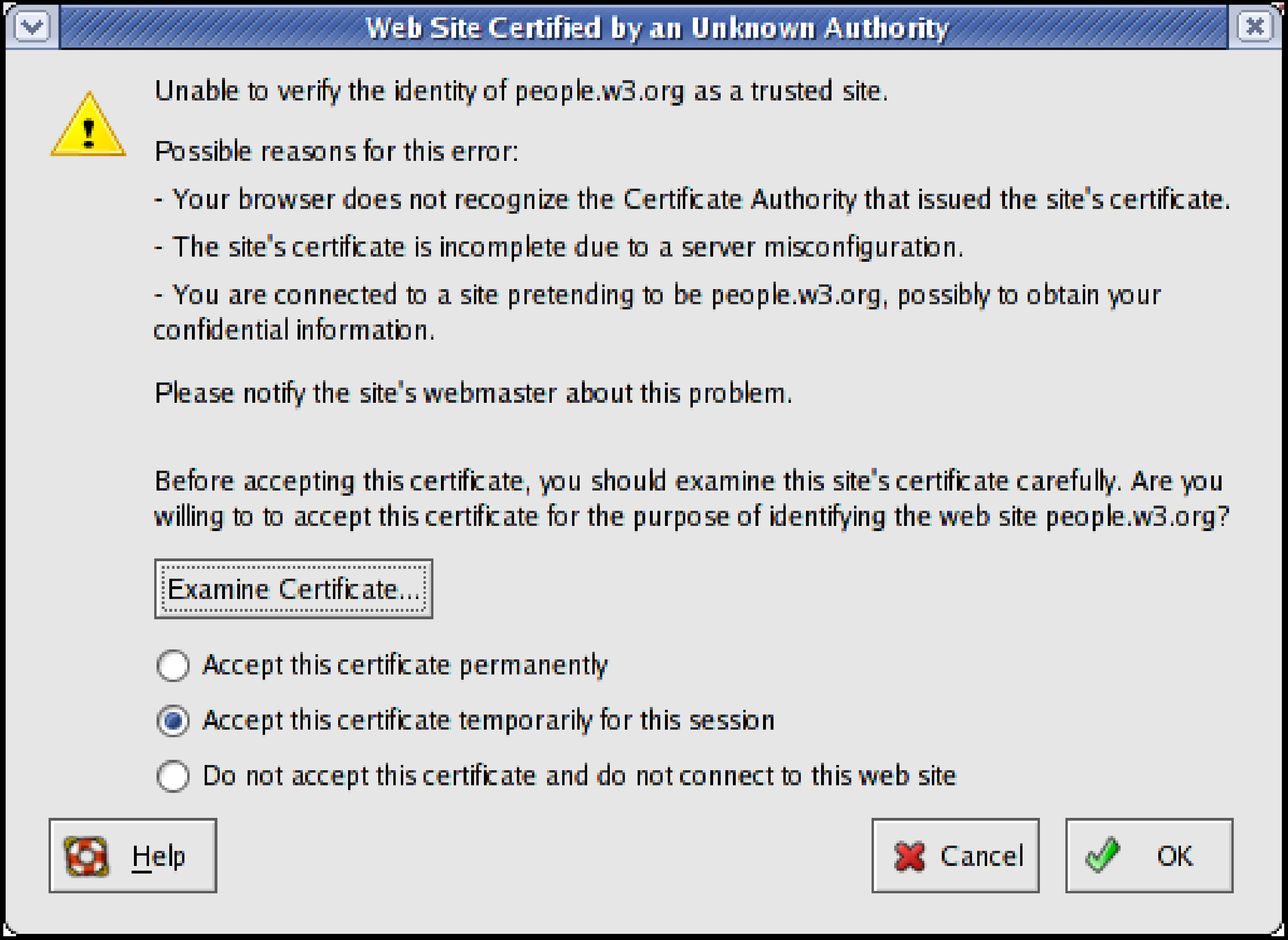
○ Do not accept this certificate and do not connect to this web site

<impossible>
Please contact the
site's webmaster
</impossible>

<impossible>

you should examine
this certificate
carefully

</impossible>



Web Site Certified by an Unknown Authority

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.

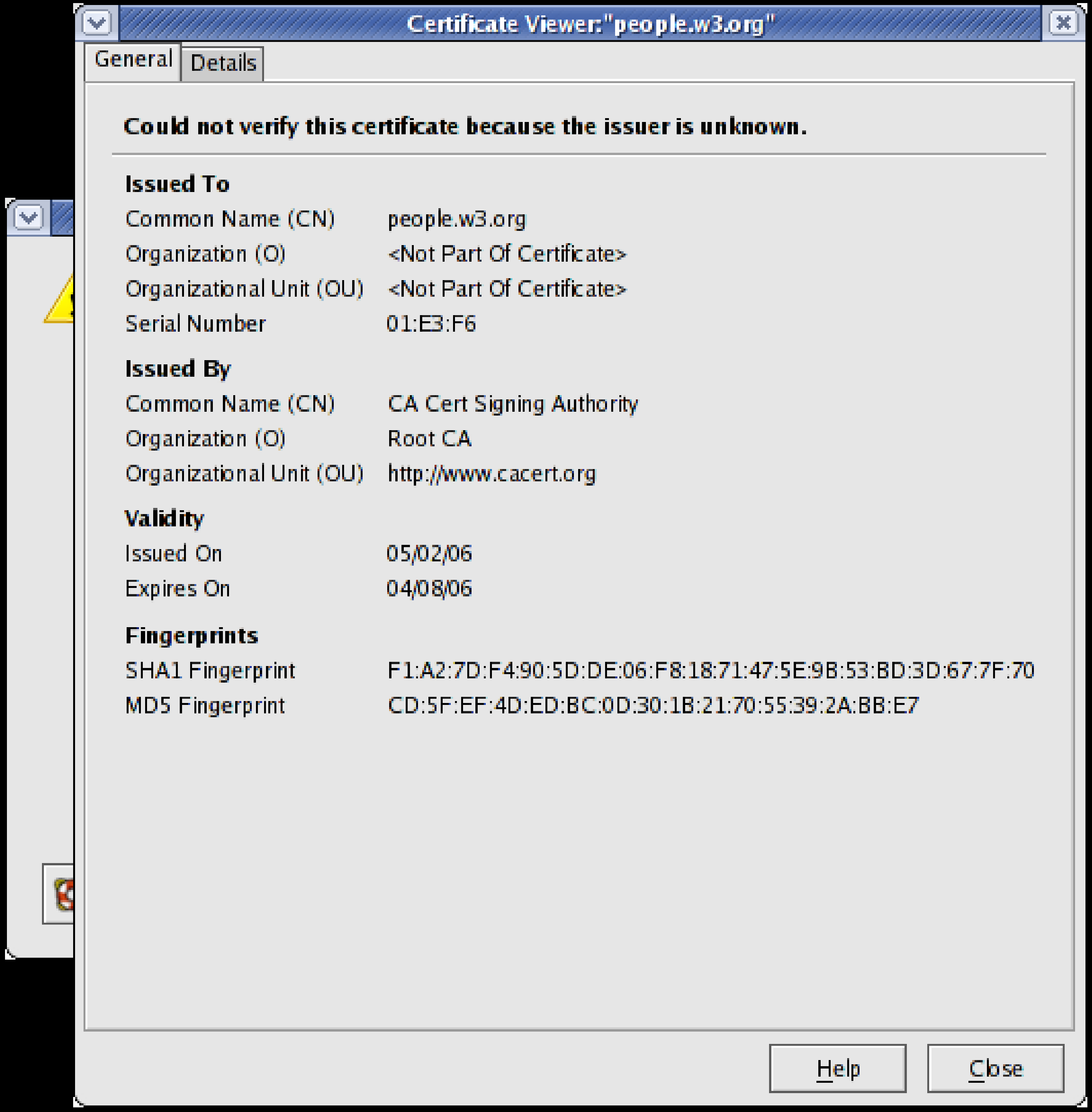
Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site people.w3.org?

○ 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

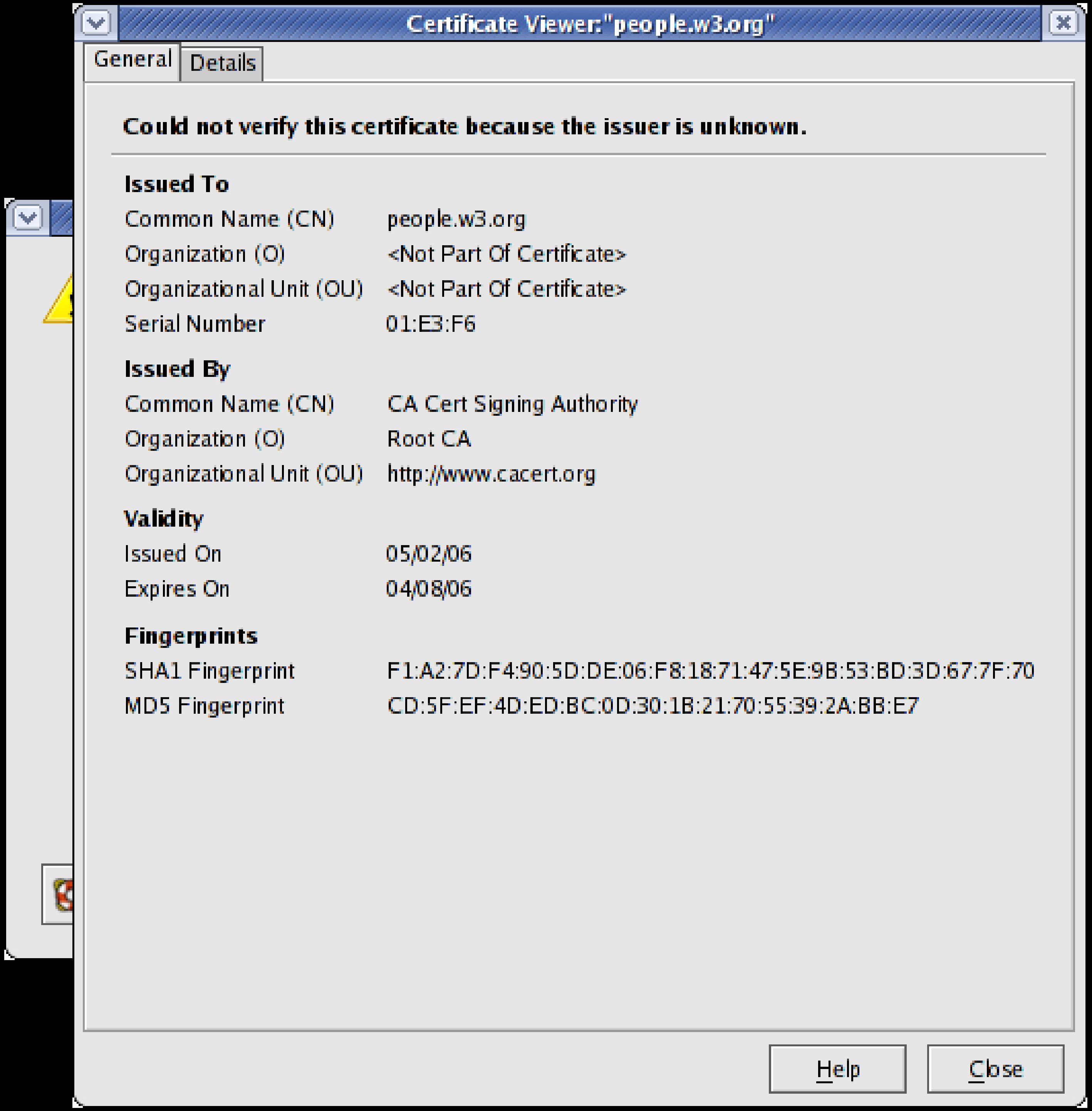
Issued On 05/02/06
Expires On 04/08/06

Fingerprints

SHA1 Fingerprint F1:A2:7D:F4:90:5D:DE:06:F8:18:71:47:5E:9B:53:BD:3D:67:7F:70
MD5 Fingerprint CD:5F:EF:4D:ED:BC:0D:30:1B:21:70:55:39:2A:BB:E7

“Could not verify this certificate because the issuer is ***unknown***.”

“Issued By”



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

SHA1 Fingerprint	F1:A2:7D:F4:90:5D:DE:06:F8:18:71:47:5E:9B:53:BD:3D:67:7F:70
MD5 Fingerprint	CD:5F:EF:4D:ED:BC:0D:30:1B:21:70:55:39:2A:BB:E7

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.”

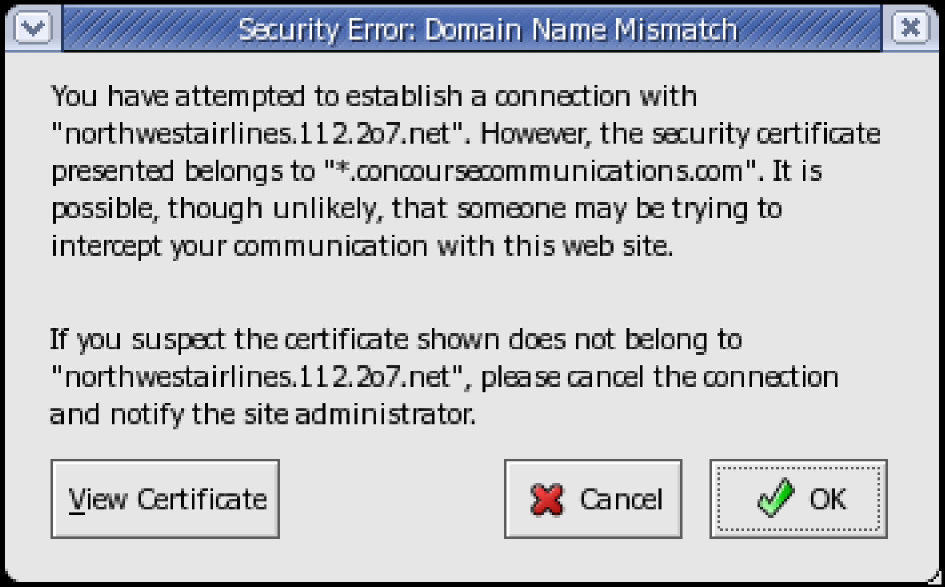
Elevator Certificate: The writing on the wall that you read while your elevator is in free fall.

users trust **content**

useless security indicators **teach**

disregard advice

<attack>



You have attempted to establish a connection with "northwestairlines.112.2o7.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.

If you suspect the certificate shown does not belong to "northwestairlines.112.2o7.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

<http://www.w3.org/2006/WSC/>

W3C Web Security Context Working Group

What can we tell users to help them make the right decisions?

how?

hard problems

DANGEROUS
CLIFF EDGE
DANGEROUS
CLIFF EDGE
CHILDREN MUST BE SUPERVISED
AT ALL TIMES
SURVEILLEZ VOS ENFANTS
EN P

security usability: much research to be done

What decisions should users make at all?

What decisions should we keep away from them?

Key continuity management for TLS?

Don't let the attacker control your security UI.

Steer users toward known sites when they interact with forms?

<future>

ALKIN

platform

applications

local

(Widgets)

remote

(mash-ups)

ubiquitous

scan
print
find your kids
open your safe
turn off the fridge
listen to your spouse
(if using a VOIP phone)
file for divorce

Google™

<security>

RESTRICT!

</security>

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!

think about it…

<?>

Thomas Roessler

tlr@w3.org