Securing The Web Browser
Keeping the Phish in the Sea
What is Wrong With This?

Welcome

Personal identification

Enter last name*  First name*

Select your departure city*

Select one of the following for identification*

- Aeroplan Number
- Credit Card number
- Booking Reference

Please note that fields marked * are mandatory entries.

Your personal information is encrypted securely when sent between your computer and Air Canada.

Use aircanada.com check-in:

- from any Canadian city and from select international cities (with electronic or paper ticket)
- from select US cities (with electronic ticket only)
- to any destination
- at least one hour prior to departure for all flights within Canada
- at least 1.5 hours prior for flights between Canada and the USA
- at least 2 hours prior for flights between Canada and other countries
- up to 12 hours prior to departure

Is it safe to input my credit card online for identification purposes?

QUIT  CONTINUE
Where to Begin?

- Security indicator only in the *content region*
  - Notice that it is used for personal data that should be secure
- No access to the location or *identity* indicators
- Site was able to remove all *chrome*
- **This looks like a **phishing** site!**
  - Can phishing *really* be that easy? YES!
What is Wrong With This?
Nothing!!
Konqueror

PayPal - Welcome - Konqueror

Location: https://www.paypal.com/

Member Log-In

Forgot your email address?
Forgot your password?

Email Address
Password
Log In

Join PayPal Today
Now Over 96.2 million accounts

Mandate Tools
Auction Tools

Welcome
Send Money
Request Money

Go Forward. Go Mobile.
Use your phone to send money and buy things

Make Free Calls With PayPal
Click here to see offer

Learn more about PayPal Worldwide
Firefox Chrome
Internet Explorer Chrome
The Browser Today
Flaws in Browsers

- Sites have too much control over chrome
  - Can spoof system windows
- Chrome is inconsistent across platforms
  - Inconsistent user experience – think phones, kiosks, PCs
- Users trust content as much as chrome
- Identity and encryption concepts are mixed, indicated only with a boolean (the padlock)
... and more flaws

• Certificate issuance is a black-box, inconsistent
  • What does it even mean? My data is encrypted? I'm talking specifically to *my* bank? Will my bank handle my data properly?

• International domain names can confuse users
  • For that matter, even simple .COM ones do!

• Keystrokes can be stolen with XmlHttpRequest, iframes

• Scripting and active content are far too powerful

• Very vulnerable to click-through syndrome
You Don't Believe It?

Dear Mountain America Credit Union Customer

Your Mountain America Credit Union card was automatically enrolled in the Verified by Visa program.

Enrolled Card: 4053-85**-****

To ensure your Visa card's security, it is important that you protect your Visa card online with a personal password. Please take a moment, and activate for Verified by Visa now.

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You’ll get the added confidence that your Visa card is safe when you shop at participating online stores.

https://www.mountain-americ.net/

We present our apologies and thank you for cooperating. Please do not answer to this email - follow the instructions given. These instructions have been sent to all bank customers and it’s obligatory to follow.

© 2006 Mountain America Credit Union Service Department

* Please note: If you FAIL to update your Visa card, it will be temporarily disabled.
Some Phishers Go To Great Lengths!
Why Are These Hard to Solve?

- In many cases, fixing these *breaks the Internet™*
  - Users won't upgrade, we end up worse off
  - Browsers need to do this together, or we need incentives
- There are too many sites that rely on misfeatures
- The concept of identity is not well understood or defined
- Business models are involved
This is Not A Solution!
Users use Web Browsers

- The web browser needs to be easy to use, safe, and powerful
- We need to provide solid, comprehensible chrome and rich content support
- Usability is key: users need to be able to understand the software on first use, but it must be optimally efficient to use years later
- Our current paradigms are failing
User Interface – Good or Bad?
Current Initiatives

- KDE: KWallet
- Microsoft: InfoCard
- CA-Browser forum: High Assurance
- Informal: UI, SSL synchronization between browser developers
- W3C: public-usable-authentication
- Anti-phishing plugins
High Assurance

- 110 certificate authority roots in KDE today
- No standards!
- High Assurance will finally begin to set standards for CAs
Spoof Proof Browser

- Status bar, location bar become permanent
- JavaScript popups become more easily distinguished from system popups
- Personalization features (petnames?)
- More robust SSL