

The Secure Modern Desktop

Keeping the Phish in the Sea




New Challenges

- Security problems – not just about buffer overflows and rootkits anymore
- We need to prevent:
 - Identity theft
 - Phishing
 - More sophisticated spyware, malware
- We need to facilitate encryption
- Most of these issues: KIO, KHTML, Konqueror

What is Wrong With This?

aircanada.com check-in - Konqueror

AIR CANADA  aircanada.com check-in

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**

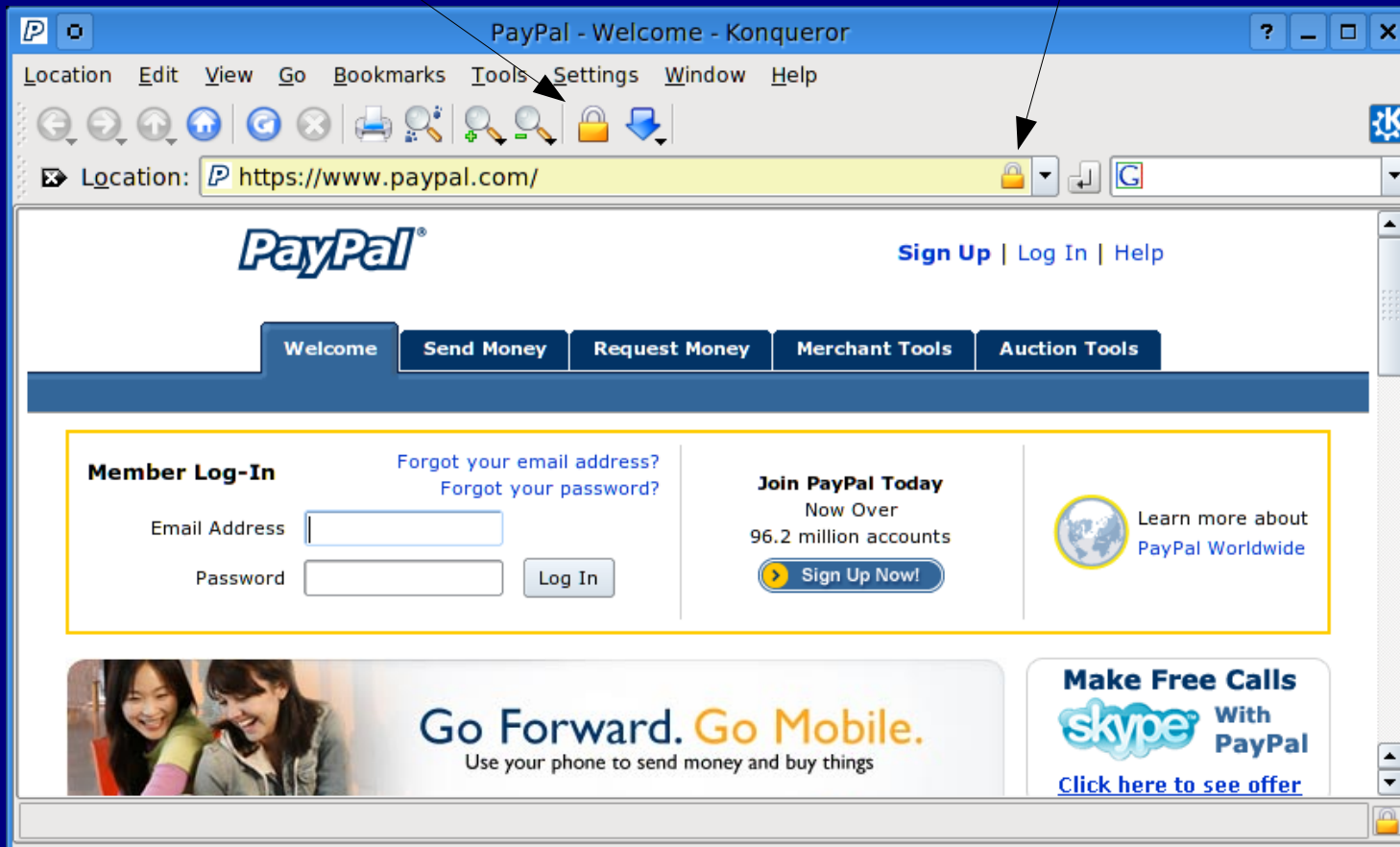
Where to Begin?

- 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!

The Browser Today



Konqueror



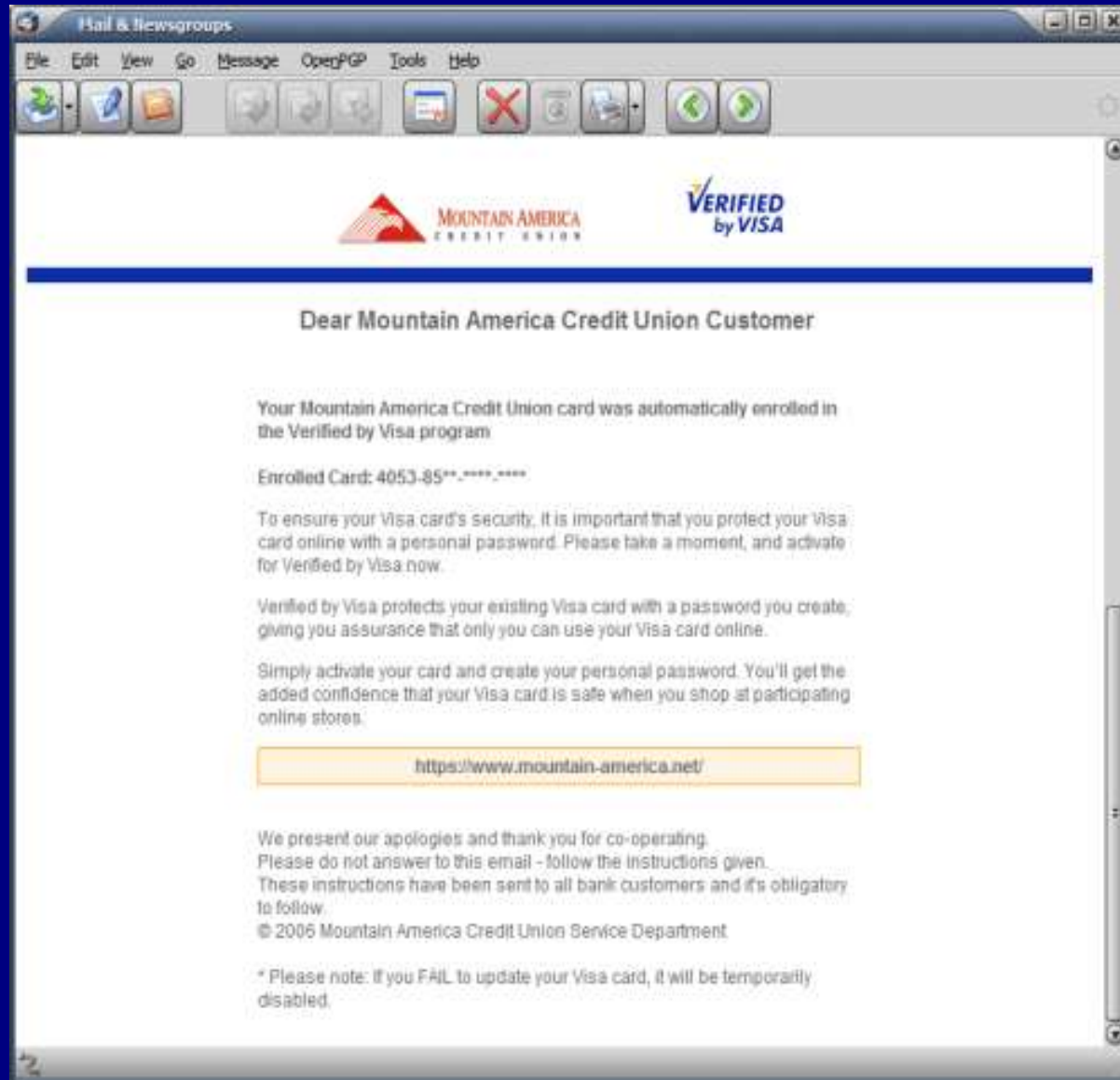
Flaws in Browsers

- 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?



Some Phishers Go To Great Lengths!

The image shows a screenshot of a web browser displaying a phishing website for Mountain America Credit Union. The browser's address bar shows a URL that appears to be a legitimate site, but the page content is a phishing page designed to steal user credentials. The page features the Mountain America Credit Union logo and the slogan "It's Just Too Easy!". A prominent "Online Services" section is titled "Verified by VISA" and includes a form for users to "Activate Now for Verified by Visa" by entering their card number. The form includes a "SUBMIT" button. Below the form, there are links for "Privacy & Security" and "Terms & Conditions". The page also includes a navigation menu with options like "Products & Services", "Business Services", "Our Company", "Online Services", "Advice & Planning", and "Apply Now". A sidebar on the left lists various services such as "Credit Cards", "Signature Awards", "Credit Card Application", "Consumer Tips", and "Consumer Education". At the bottom of the page, there are logos for NCUA and Digital Incentive, along with links to privacy statements and disclosures. A JavaScript error message is visible in the bottom status bar: "JavaScript Currently Forbidden [<script>: 6] [3+F+P: 0]".

Mountain America Credit Union | Online Services | Verified by VISA - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://www.mountain-america.net/step1.php?ad=9270682a1f7754b1a6a3be40c213273c

Netcraft Services | Back to Top | New Site Rank: | Site Report [US] | Transform Internet, Inc.

New user? | Demo | Get more Info | Rates | Branch Locations | ATM Locations | FAQs | Careers | Press Site | Contact Us

Online Branch
LOGIN

SEARCH

Products & Services | Business Services | Our Company | Online Services | Advice & Planning | Apply Now

Online Services
Verified by VISA

We use advanced SSL encryption technology to ensure confidential information cannot be viewed, intercepted or altered.

Activate Now for Verified by Visa
Enter your card number (without spaces).
SUBMIT

Privacy & Security | Terms & Conditions

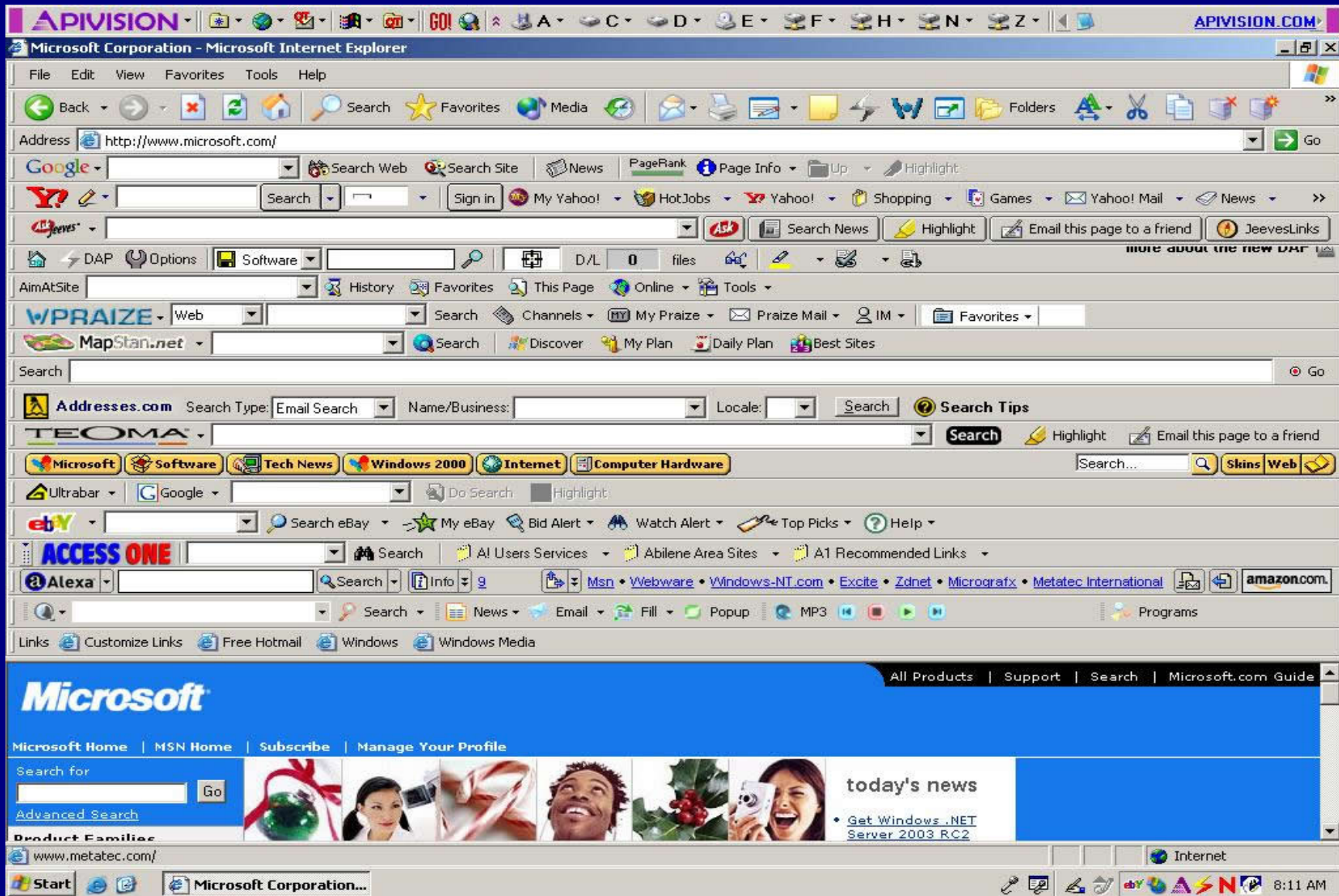
NCUA
DIGITAL INCENTIVE

Mountain America Privacy Statement
Mountain America Financial Services, LLC Privacy Statement
USA Patriot Act Disclosure

JavaScript Currently Forbidden [<script>: 6] [3+F+P: 0]

Done | www.mountain-america.net

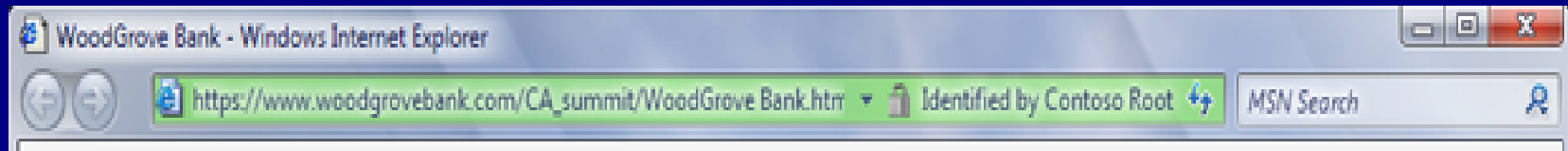
This is Not A Solution!



Security Initiatives

- Microsoft: CardSpace (formerly 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

A Safer KDE Desktop

- Konqueror:
 - Status bar, location bar become permanent
 - JavaScript popups become more easily distinguished from system popups
 - Personalization features (petnames?)
- More robust SSL and more pervasive encryption
- Extended wallet system
- Anti-phishing system
 - SafeSite



SafeSite

- Think of it as SpamAssassin for anti-phishing:
 - Check URLs against a phishing database (APWG or other), even before the user clicks
- High-impact tool, especially for KMail, KNode, Konqueror
- Configurable backends to address privacy concerns

KDE 4

- Let's make KDE 4 the most secure desktop yet
 - Built-in anti-phishing database support
 - Leadership in removing bad browser features
 - Better usability of encryption in KMail and other applications
 - KWallet NG and/or CardSpace support
 - Be active, participate!
- Remember: KDE is a *networked desktop environment*

George Staikos <staikos@kde.org>

aKademy Sep 23, 2006