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?
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

PayPal - Welcome - Konqueror

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

PayPal - Welcome - Konqueror

Member Log-In

Email Address

Forgot your email address?

Forgot your password?

Password

Log In

Join PayPal Today

Now Over 96.2 million accounts

Sign Up Now!

Learn more about PayPal Worldwide

Go Forward. Go Mobile.

Use your phone to send money and buy things

Make Free Calls

With PayPal

Click here to see offer
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
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-america.net/

We present our apologies and thank you for co-operating. 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.

© 2008 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!
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