



High Validation SSL Certificates

Tim Callan
Group Product Marketing Manager
VeriSign Inc.



Where it all comes together:

Online business has a problem

- + Phishing growing rampant
 - 9715 new phishing sites in January 2006 alone¹
 - 100 brands hijacked
- + Consumer distrust growing as a result
 - 84% believe businesses not doing enough to protect them
 - 24% don't purchase online at all²
- + Users need help distinguishing legitimate sites from crafty phishing sites
 - 90% fooled in April 2006 Harvard/UC Berkeley study³

1. Anti-Phishing Working Group, March 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf

2. Forrester Research, December 2005. <http://www.internetretailer.com/article.asp?id=17763>

3. "Why Phishing Works," April 2006. http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf

We need a new solution

+ For consumers

- Easy
- No barrier
- Broad reach
- Reliable and accurate

+ For site owners

- Easy
- No barrier
- Broad reach
- Reliable and accurate

Agenda

- + The problem today
 - Phishing's chilling effect on online business
 - Requirements for an effective solution
- + The coming solution: High Validation SSL
 - AKA "High Assurance"
 - What it is
 - What it looks like in the browser
 - How it works
 - Who will support it
 - How (and when) you can take advantage of it

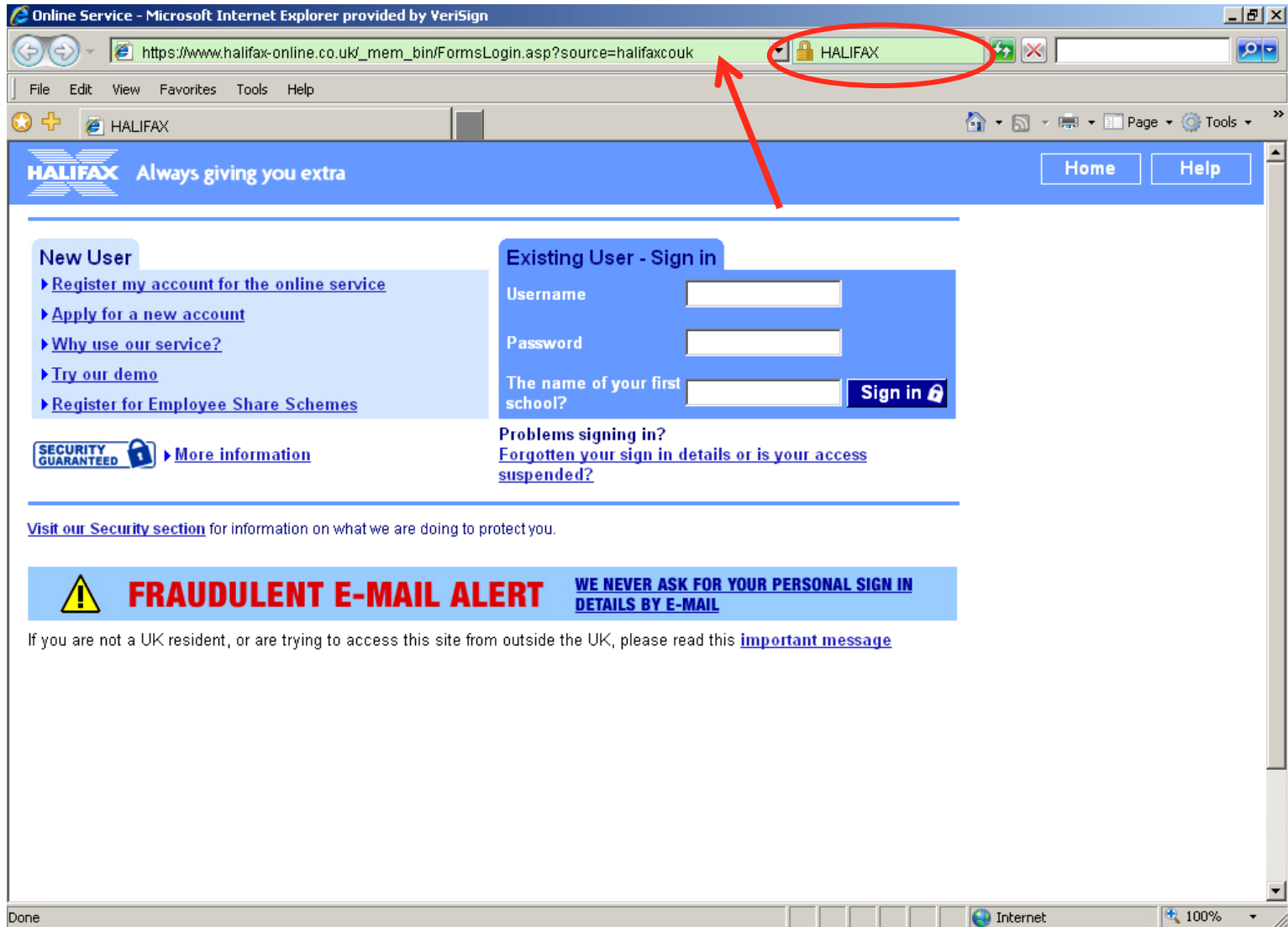
What is High Validation?

- + The biggest improvement in online trust infrastructure since 1995
- + A new way for users to identify online entities
- + A new kind of SSL/TLS certificate
- + A major blow to phishing
- + A paradigm shift in secure online transactions

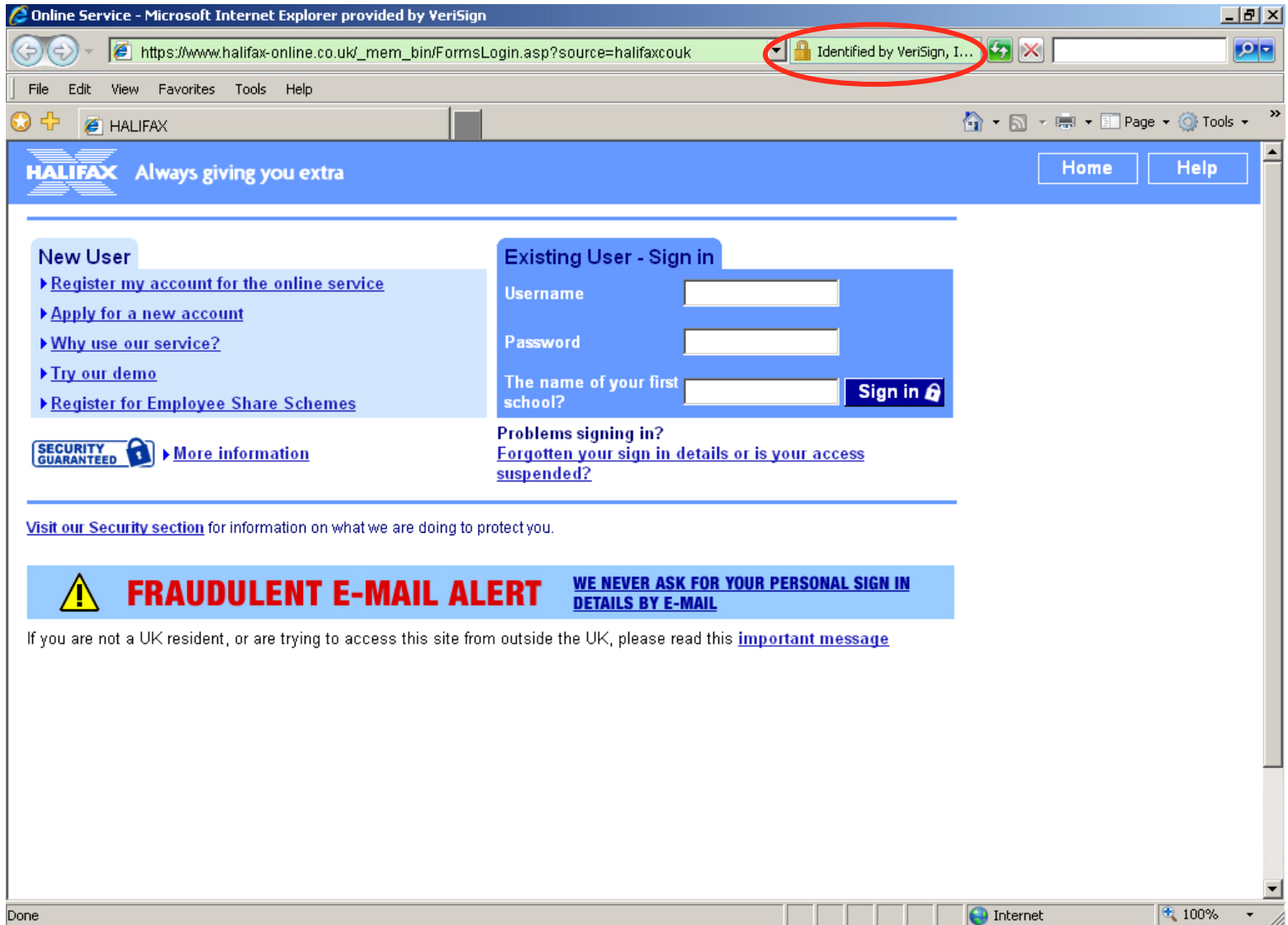
Industry leaders answer the call

- + CA-Browser Forum establish to create High Validation standard
- + SSL Certificates can be issued with High Validation status
- + Backward compatible
 - Older browsers display certificates just as they do today

Internet Explorer 7 user experience



Internet Explorer 7 user experience



How will it work?

- + Site owners undergo uniformly high level of validation
- + CAs undergo more stringent audit
- + Browser set OID to display High Validation status
- + Same High Validation procedure for standard encryption and strongest-encryption SGC certificates
 - Regular – new display in IE 7
 - SGC – new display in IE 7 and strongest encryption

Market adoption

+ Browsers

- IE 7 expected in public beta summer 2006
- Other browsers
 - Likely to adopt new display architecture

+ CAs

- Leading CAs expected to roll out new certificates

+ Site Owners

- New authentication procedure
 - Almost identical to VeriSign's existing procedure
- Plan for 12-, 24-, or 36-month certificate lifespan

Next steps

- + Update organization info with data providers
- + Keep domain registration information updated
- + Implement High Validation certificates for all new public-facing sites
- + Contact your SSL provider to plan migration of existing certificates
- + Accept the IE7 beta version on your Web site
- + Stay up to date
 - Microsoft IE blog, <http://blogs.msdn.com/ie/>
 - SSL Blog, www.verisign.com/sslblog