Designing Trustworthy User-Agents for a Hostile Web

Usenix Security 2009

Eric Lawrence
Program Manager
Microsoft Corporation

About Eric…

- IE8 Program Manager - Security
- IE7 PM – Networking & Trust
- Developer of Fiddler, TamperIE, IEToys

IE 7 *significantly* reduced attack surface against the browser and local machine…

but…

- WebApp attacks (CSRF, XSS, ClickJacking, splitting) could become the next big vector of exploit.
- More high-value information is moving to the web.
- Social Engineering and exploitation of add-ons continues to grow.
- The Web platform itself is getting richer.
- and the next generation of attackers is coming out of grade school.

Worst of all, it turns out that crime *does* pay (quite well) after all.

Why is browser security so elusive?

Complexity.

The security architecture of the current web platform was largely an afterthought.

Maybe there’s a shortcut?

We could block nearly 100% of exploits by removing just one component from the system…

The Network cable

Or, we could block a majority of exploits by removing a different component from the system…

The user

So, if we re-architect everything, or get rid of the users, or get rid of the network, then security *might be* easy.

FAIL

Security is straightforward.

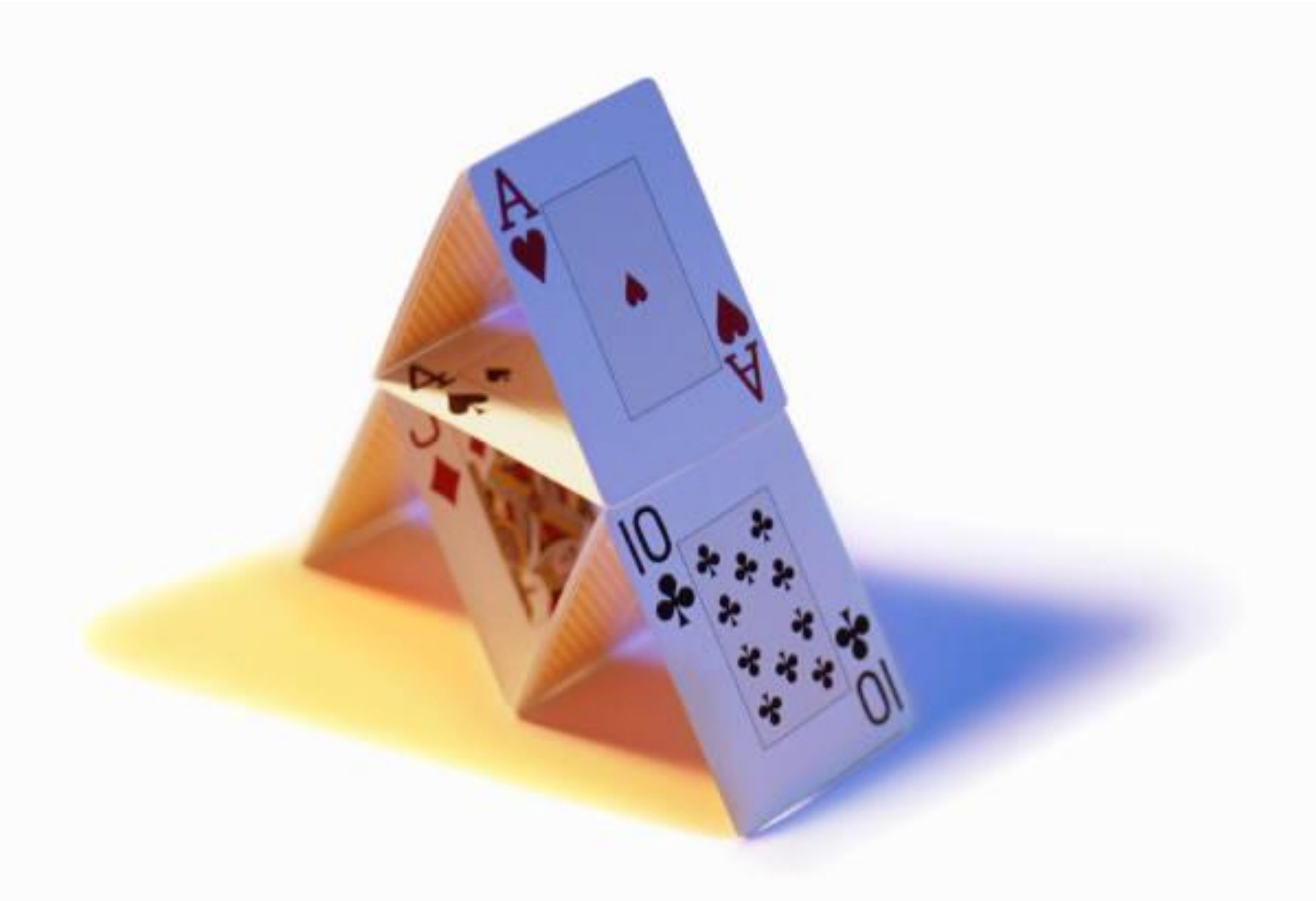
Tradeoffs are complicated.

Yes, Microsoft is a big, influential company...

…but the Internet is bigger.

- Many hundreds of millions of users…
- From all over the world…
- Visiting billions of web pages…
- And most don’t really even know what a “browser” is!

The Web is surprisingly fragile.



For most web users, it’s all about value.

The browser that most users will ask for…

Race car

The browser that meets users security expectations…

Amphibious assault tank

Bad guys only need to find *one* way in…

Security Team's Investments

- **Security Feature Improvements**
  - Create security features that address the top vulnerabilities today and in the future
- **Secure Features**
  - Reduce attack surface of existing code by closing legacy holes
  - Apply security-focused rigors against new code
- **Provide Security *and* Compatibility**
  - Users understand that improved security is a reason to upgrade

Threat Focus Areas

Address the evolving threat landscape

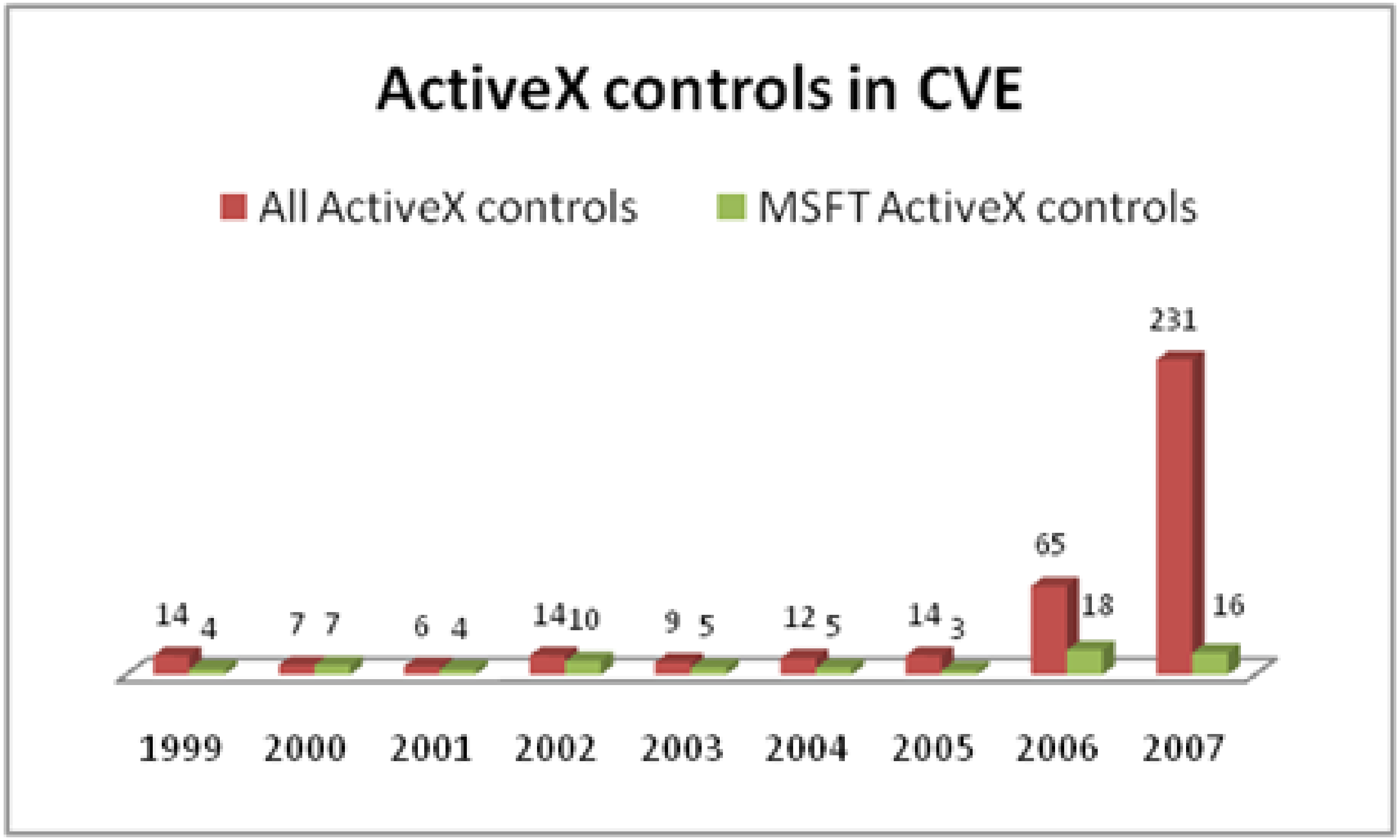
Browser & Add-on Vulnerabilities

Social Engineering

Web App Vulnerabilities

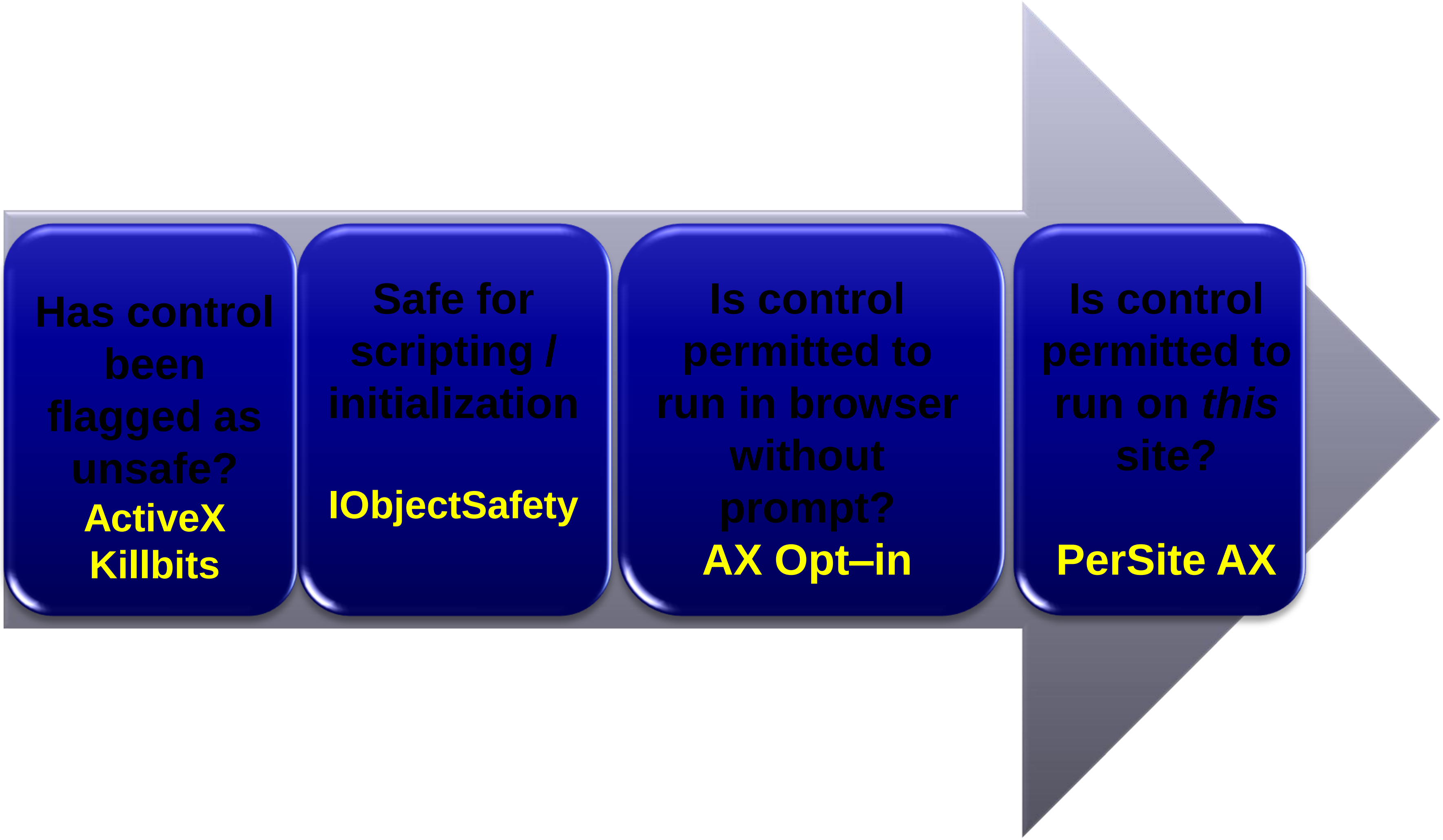
Browser/Add-on Vulnerabilities

ActiveX



Browser/Add-on Vulnerabilities

ActiveX Gauntlet



Has control been flagged as unsafe?

ActiveX Killbits

Safe for scripting / initialization

IObjectSafety

Is control permitted to run in browser without prompt?

AX Opt–in

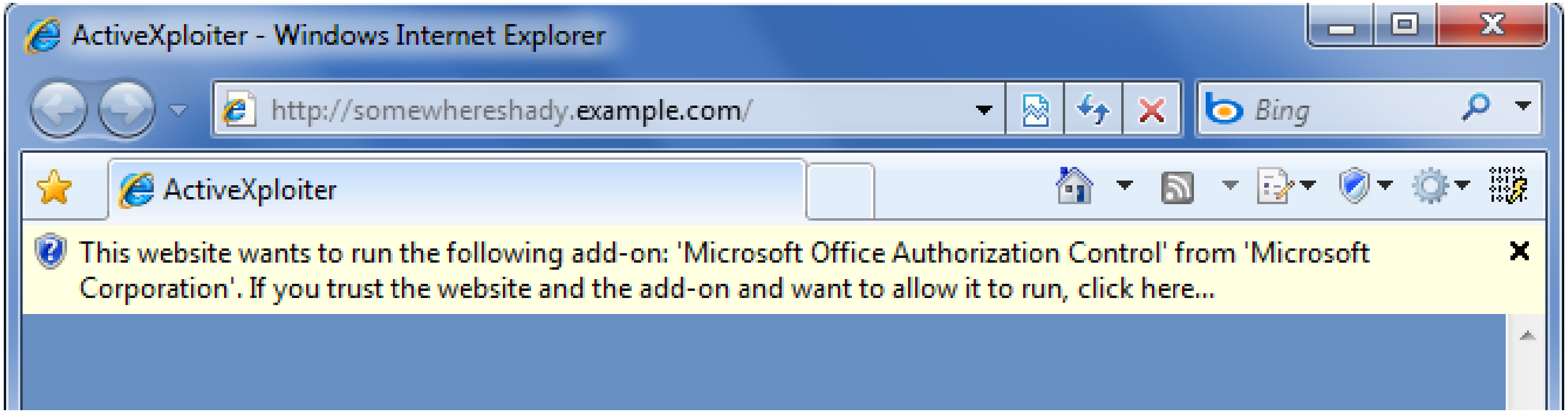
Is control permitted to run on *this* site?

PerSite AX

Browser/Add-on Vulnerabilities

Per-site ActiveX

- Helps prevent repurposing of ActiveX controls



ActiveXploiter - Windows Internet Explorer

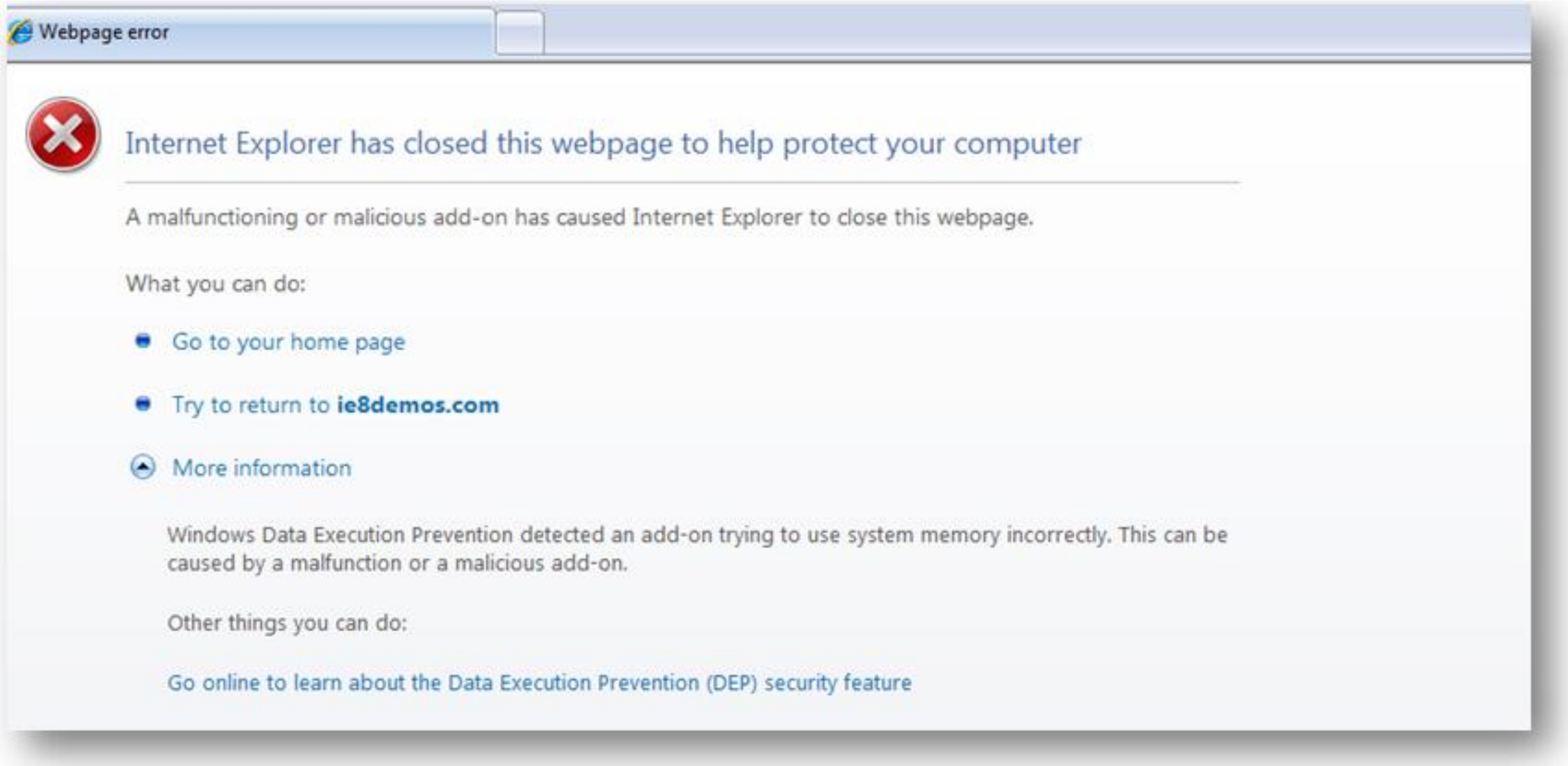
http://somewhereshady.example.com/

This website wants to run the following add-on: 'Microsoft Office Authorization Control' from 'Microsoft Corporation'. If you trust the website and the add-on and want to allow it to run, click here...

Browser/Add-on Vulnerabilities

Data Execution Prevention

- Mitigates many memory-related vulnerabilities by blocking code execution
- Other protections like ASLR, SAFESEH, GS, etc



Webpage error

Internet Explorer has closed this webpage to help protect your computer

A malfunctioning or malicious add-on has caused Internet Explorer to close this webpage.

What you can do:

- Go to your home page
- Try to return to **ie8demos.com**

More information

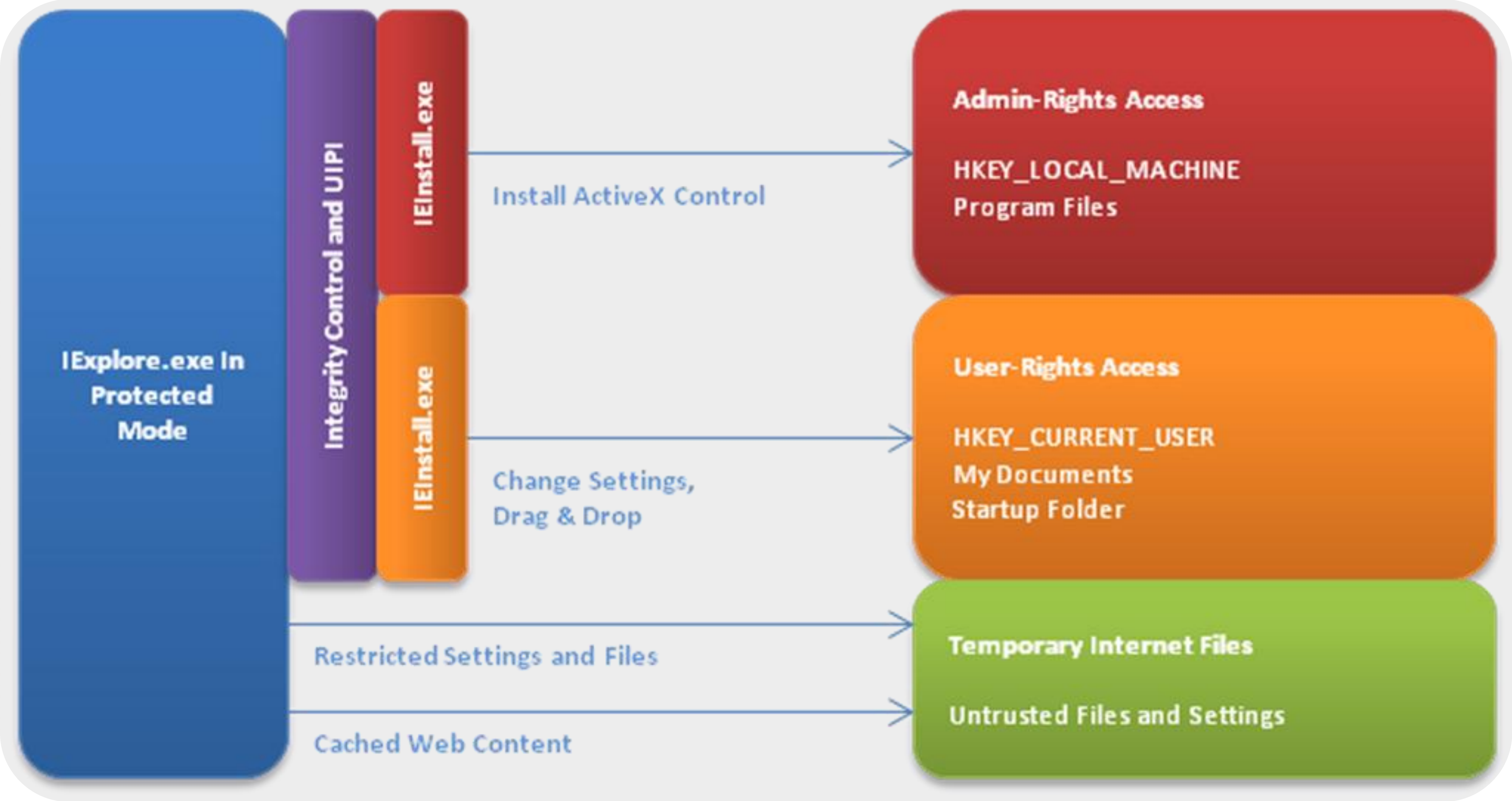
Windows Data Execution Prevention detected an add-on trying to use system memory incorrectly. This can be caused by a malfunction or a malicious add-on.

Other things you can do:

Go online to learn about the Data Execution Prevention (DEP) security feature

Browser/Add-on Vulnerabilities

Protected Mode



Protected Mode

- Loosely-coupled IE enables one frame to host both Low and Medium tabs
- Intranet Zone moved to Medium Integrity by default
- Silent Elevation List split
- Minor API improvements
  - DWebBrowserEvents2::NewProcess
  - IE[Get|Set]ProtectedModeCookie
  - IERefreshElevationPolicy (IE7 GDR)
  - *Other registry/filesystem helpers.*

Question

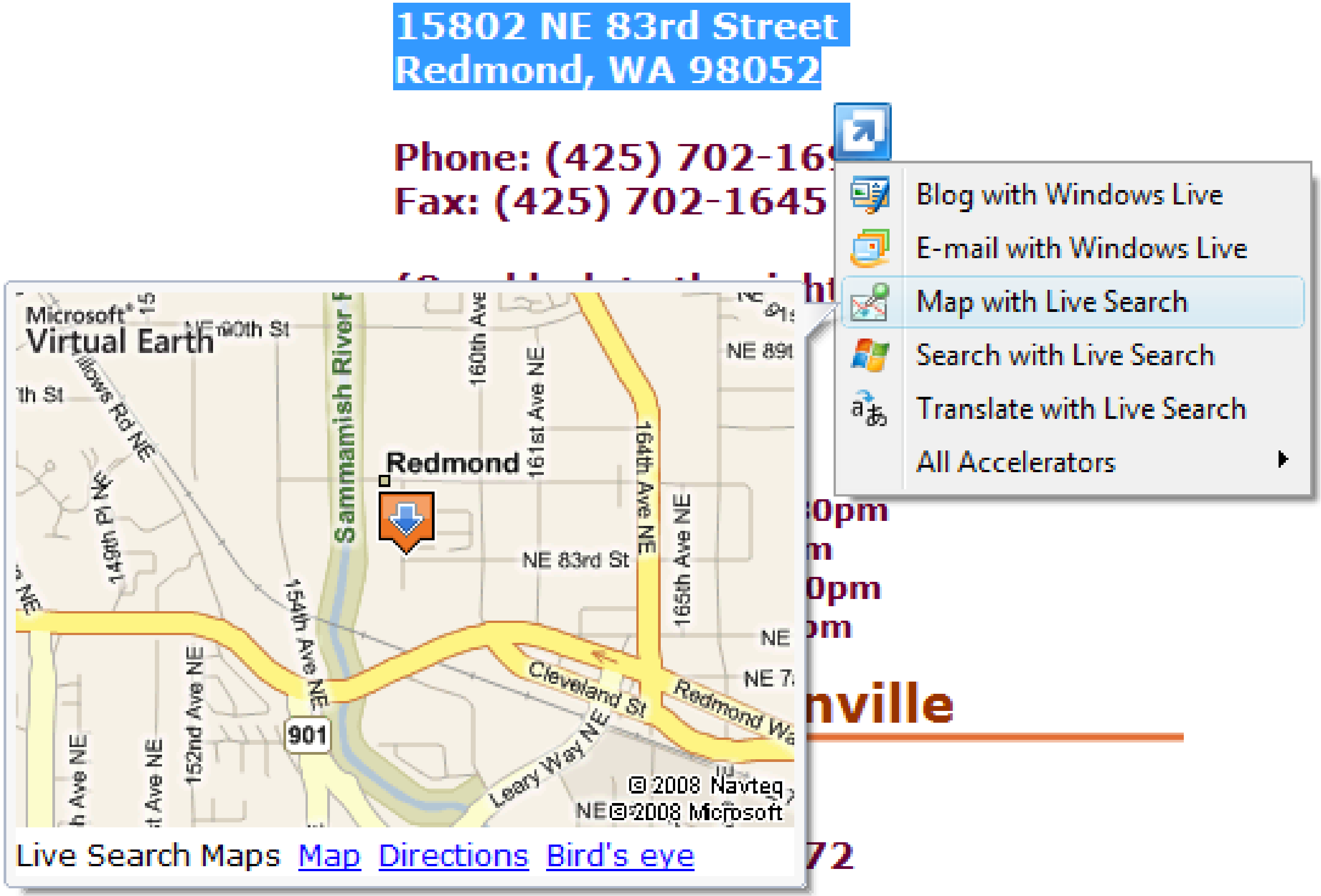
What’s the best way to develop secure, performant, and reliable C/C++ code?

Answer

Don’t.

Non-Binary Extensibility

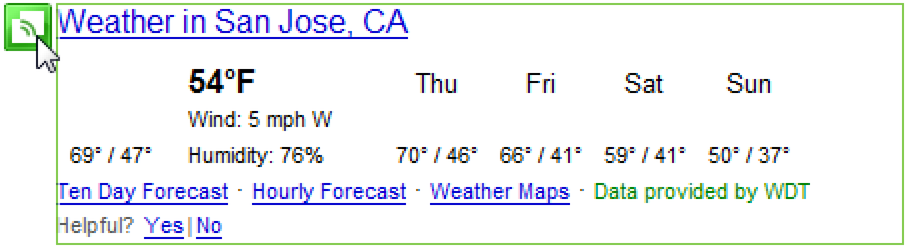
Accelerators



15802 NE 83rd Street
Redmond, WA 98052

Phone: (425) 702-16
Fax: (425) 702-1645

WebSlices

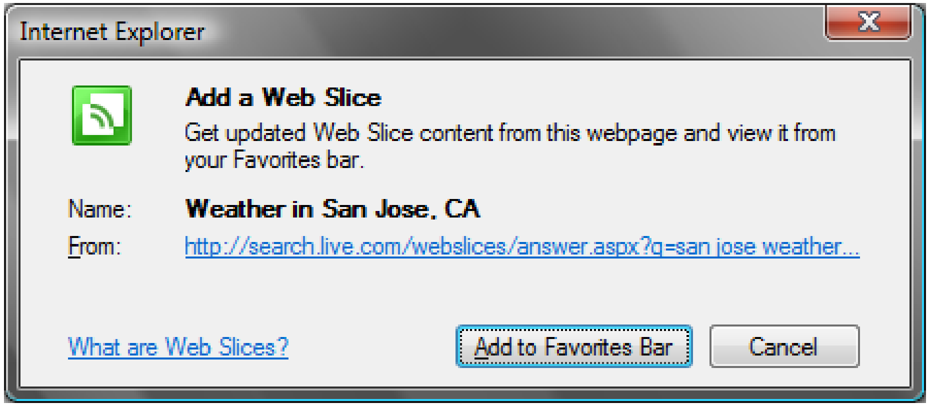


Weather in San Jose, CA

	54°F Wind: 5 mph W	Thu	Fri	Sat	Sun
69° / 47°	Humidity: 76%	70° / 46°	66° / 41°	59° / 41°	50° / 37°

Ten Day Forecast · Hourly Forecast · Weather Maps · Data provided by WDT

Helpful? Yes | No



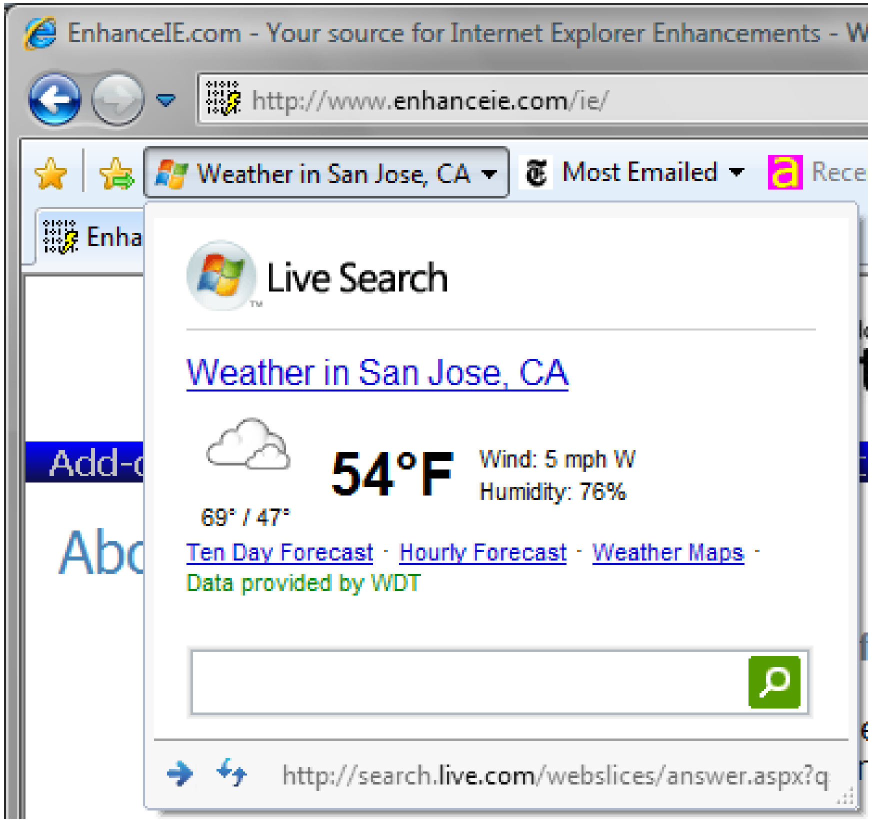
Internet Explorer

Add a Web Slice

Get updated Web Slice content from this webpage and view it from your Favorites bar.

Name: **Weather in San Jose, CA**

From: http://search.live.com/webslices/answer.aspx?q=san jose weather...



EnhanceIE.com - Your source for Internet Explorer Enhancements - W

http://www.enhanceie.com/ie/

Weather in San Jose, CA

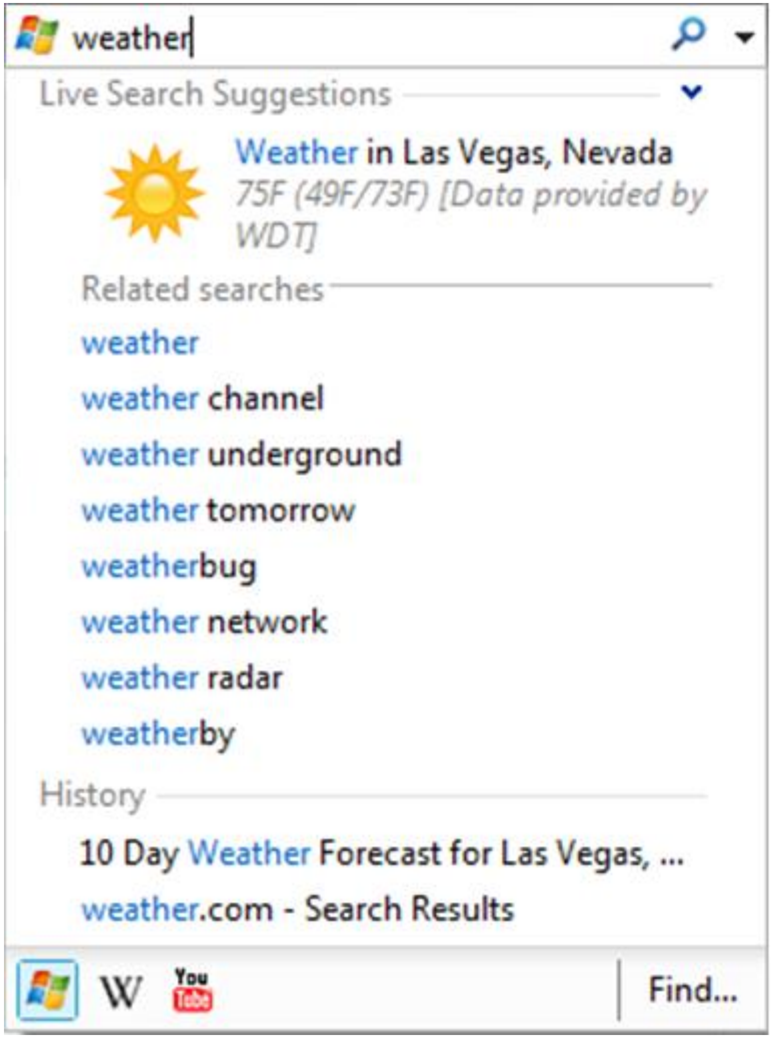
54°F Wind: 5 mph W Humidity: 76%

69° / 47°

Ten Day Forecast · Hourly Forecast · Weather Maps · Data provided by WDT

http://search.live.com/webslices/answer.aspx?q

Visual Search Suggestions



weather

Live Search Suggestions

Weather in Las Vegas, Nevada

75F (49F/73F) [Data provided by WDT]

Related searches

- weather
- weather channel
- weather underground
- weather tomorrow
- weatherbug
- weather network
- weather radar
- weatherby

History

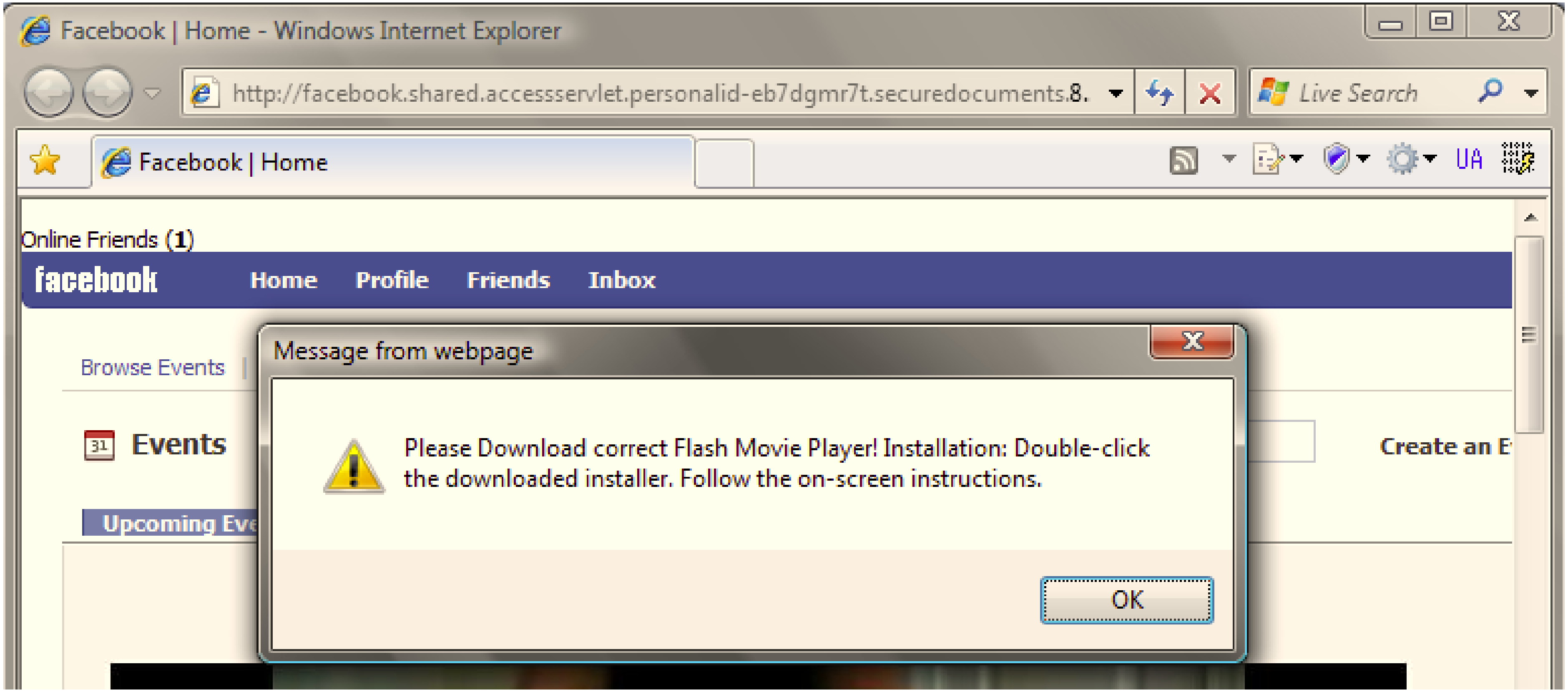
- 10 Day Weather Forecast for Las Vegas, ...
- weather.com - Search Results

L33t hax0r demo

Sometimes, threats are obvious…

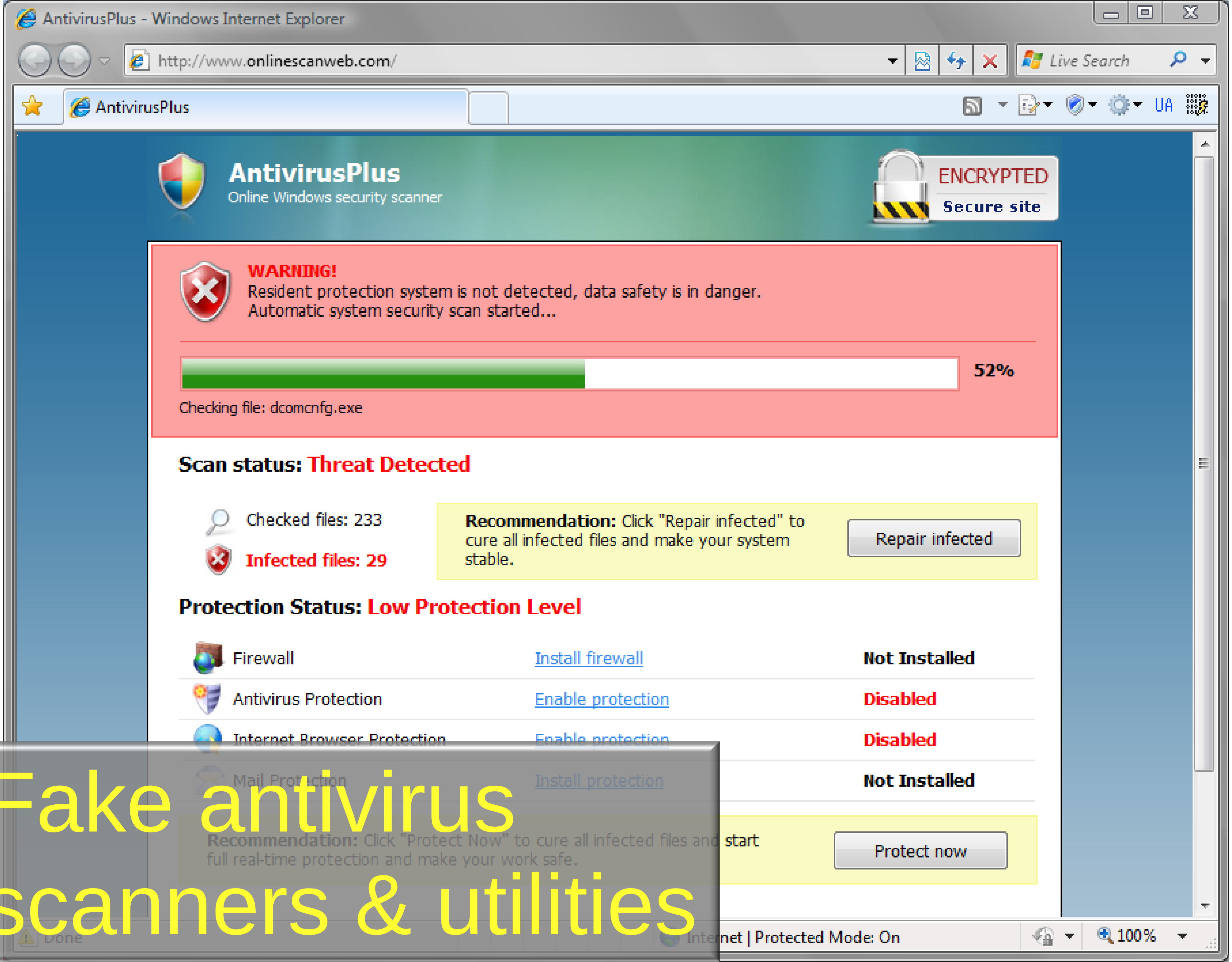
…but bad guys are getting smarter…

Fake codecs and add-ons



Message from webpage

Please Download correct Flash Movie Player! Installation: Double-click the downloaded installer. Follow the on-screen instructions.


AntivirusPlus - Windows Internet Explorer
http://www.onlinescanweb.com/
Live Search
AntivirusPlus
UA
ENCRYPTED
Secure site
Done
Internet | Protected Mode: On
100%

AntivirusPlus
Online Windows security scanner

WARNING!
Resident protection system is not detected, data safety is in danger.
Automatic system security scan started...

52%

Checking file: dcomcnfg.exe

Scan status: Threat Detected

Checked files: 233
Infected files: 29

Recommendation: Click "Repair infected" to cure all infected files and make your system stable.

Protection Status: Low Protection Level

Firewall	Install firewall	**Not Installed**
Antivirus Protection	Enable protection	**Disabled**
Internet Browser Protection	Enable protection	**Disabled**
Mail Protection	Install protection	**Not Installed**

Recommendation: Click "Protect Now" to cure all infected files and start full real-time protection and make your work safe.

Fake antivirus scanners & utilities

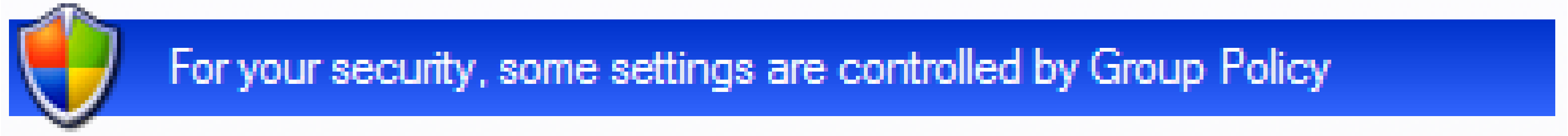
Try as we might…

…we haven’t
figured out how to
patch the user.

Social Engineering

Group Policy Controls

“Don’t ask my users to make security decisions.”



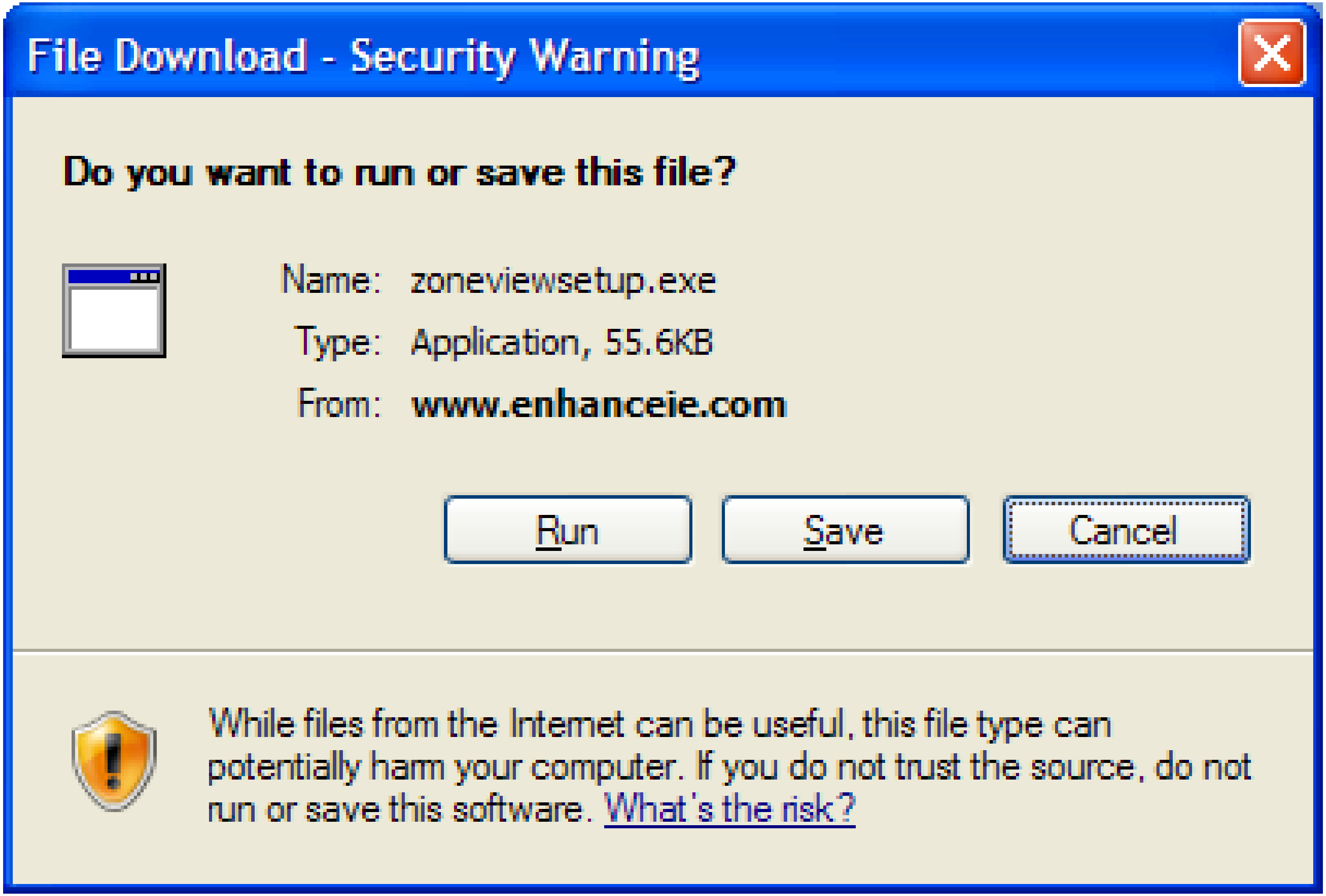
For your security, some settings are controlled by Group Policy

Policies include:

- Treat certificate errors as fatal
- Block insecure content
- Prevent bypass of SmartScreen Filter warnings
- Regulate ActiveX control install & availability

IE8 includes over 1400 group policy controls.

What if we can’t get rid of the user?



File Download - Security Warning

Do you want to run or save this file?

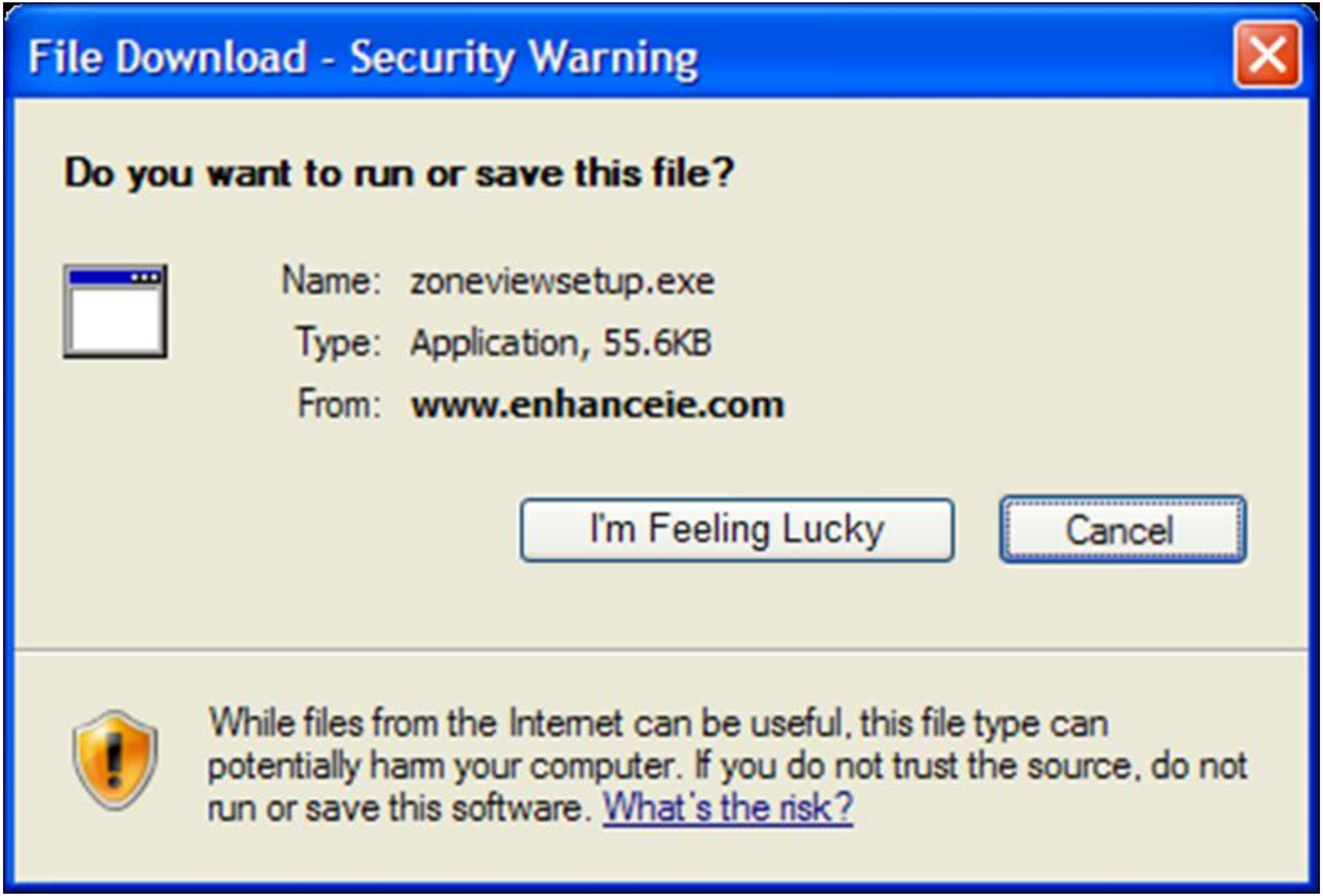
Name: zoneviewsetup.exe

Type: Application, 55.6KB

From: www.enhanceie.com

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

WARNING
STRONG CURRENT
IF IN DOUBT, DON'T GO OUT
DANGER
NO SWIMMING



File Download - Security Warning

Do you want to run or save this file?

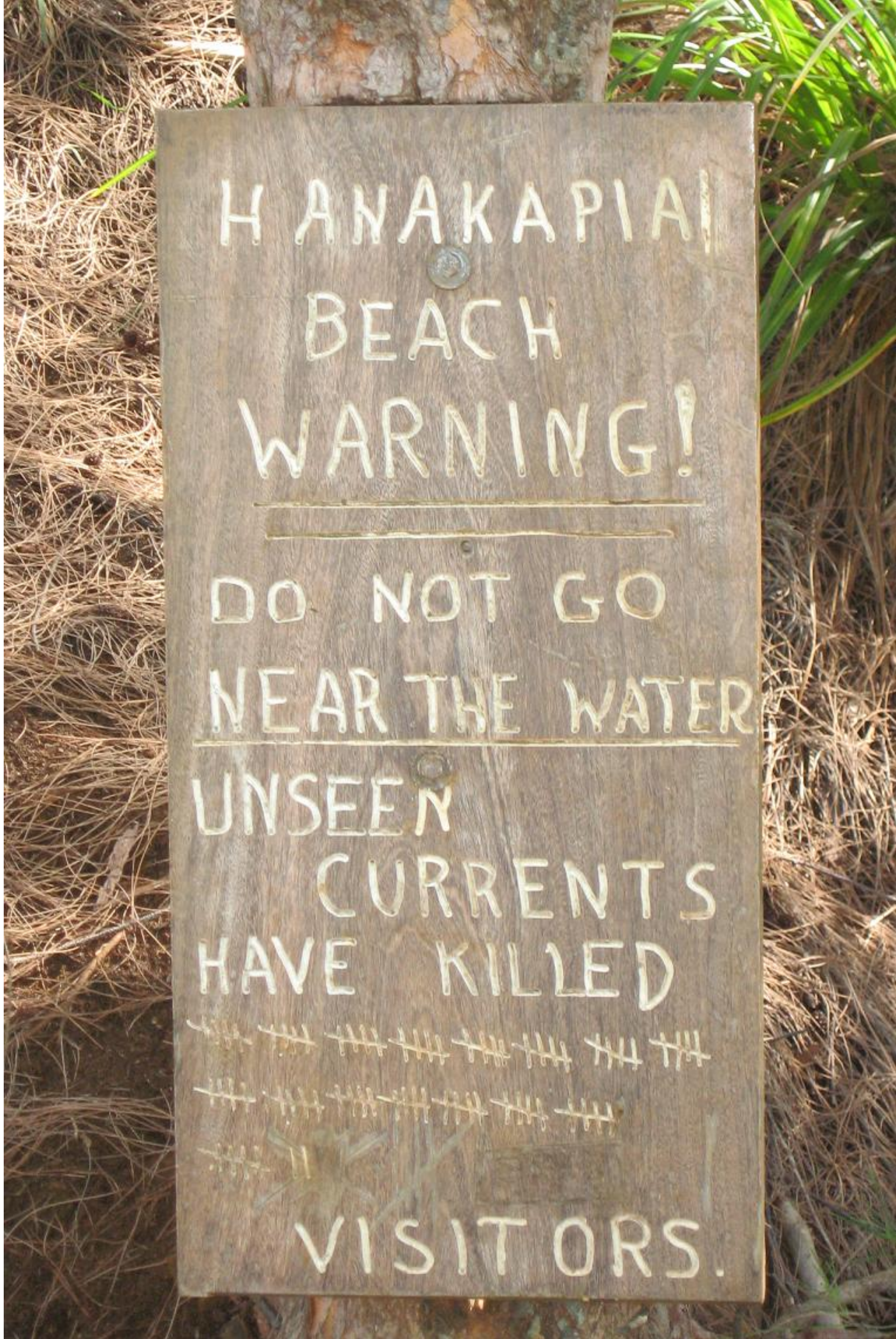
Name: zoneviewsetup.exe

Type: Application, 55.6KB

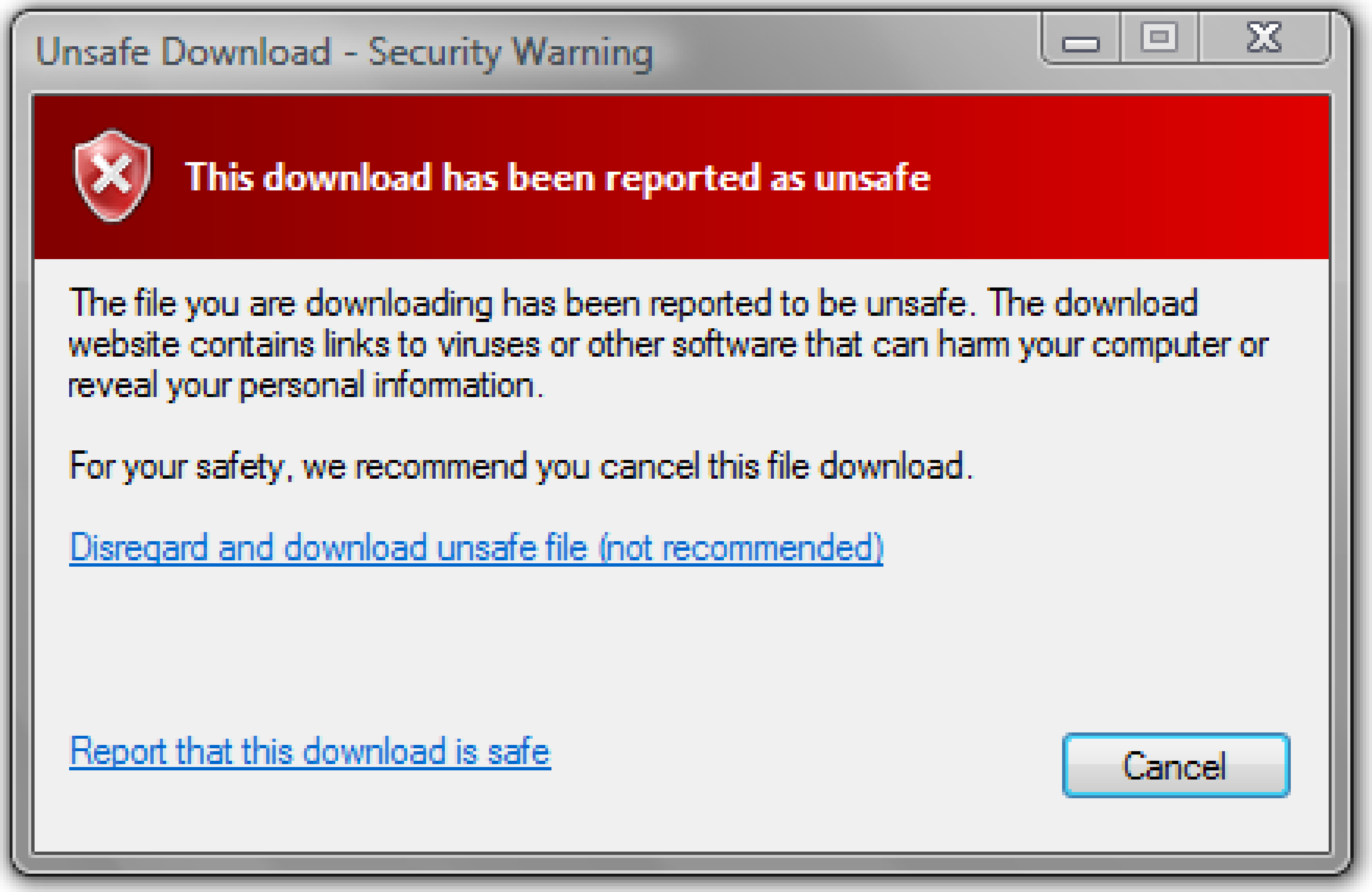
From: **www.enhanceie.com**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

A more effective warning?



SmartScreen Download Block



This download has been reported as unsafe

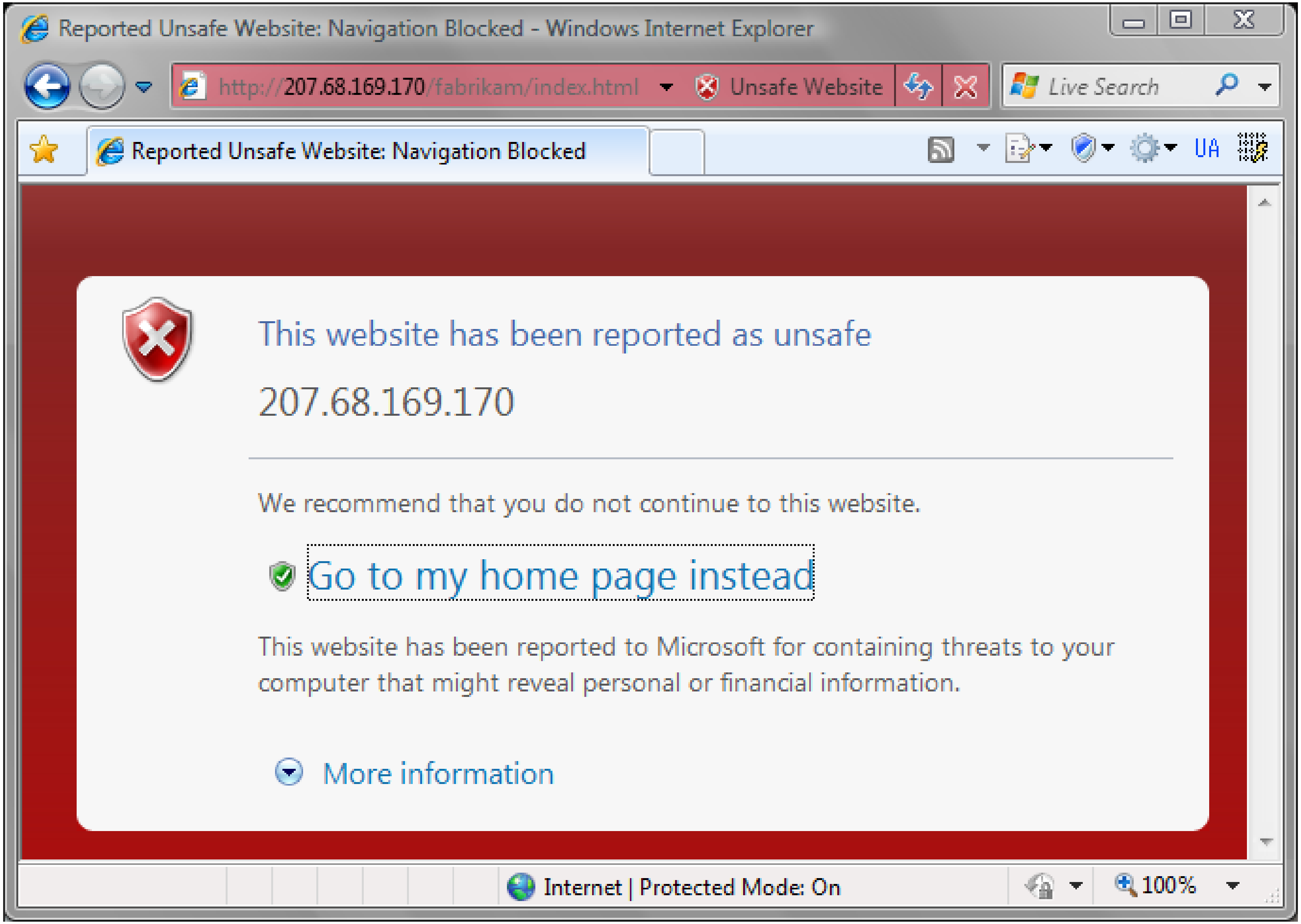
The file you are downloading has been reported to be unsafe. The download website contains links to viruses or other software that can harm your computer or reveal your personal information.

For your safety, we recommend you cancel this file download.

Disregard and download unsafe file (not recommended)

Report that this download is safe

SmartScreen Block Page



Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
http://207.68.169.170/fabrikam/index.html
Unsafe Website
Live Search
Reported Unsafe Website: Navigation Blocked
UA

This website has been reported as unsafe

207.68.169.170

We recommend that you do not continue to this website.

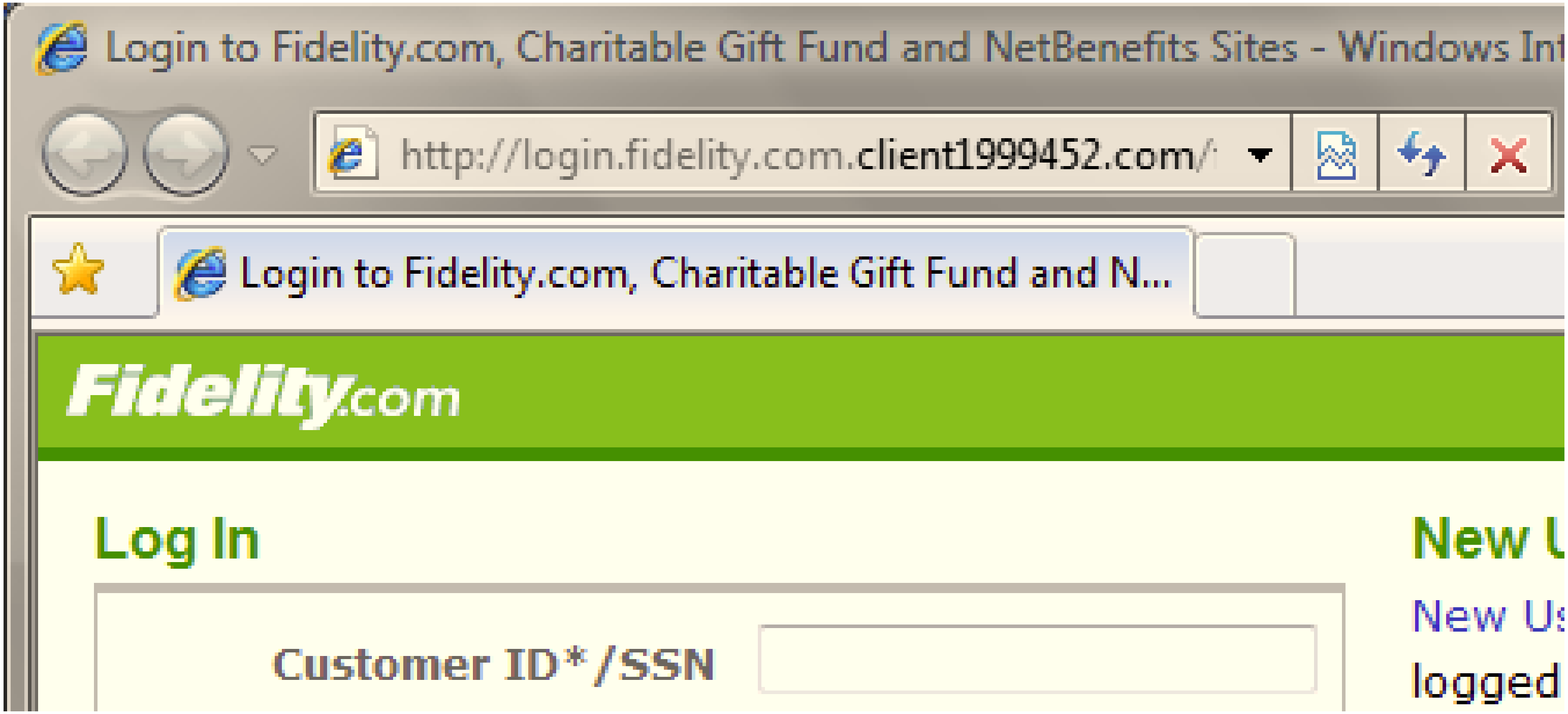
Go to my home page instead

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

More information

Internet | Protected Mode: On
100%

Domain Highlighting



Login to Fidelity.com, Charitable Gift Fund and NetBenefits Sites - Windows Int

http://login.fidelity.com.client1999452.com/

Login to Fidelity.com, Charitable Gift Fund and N...

Fidelity.com

Log In

Customer ID*/SSN

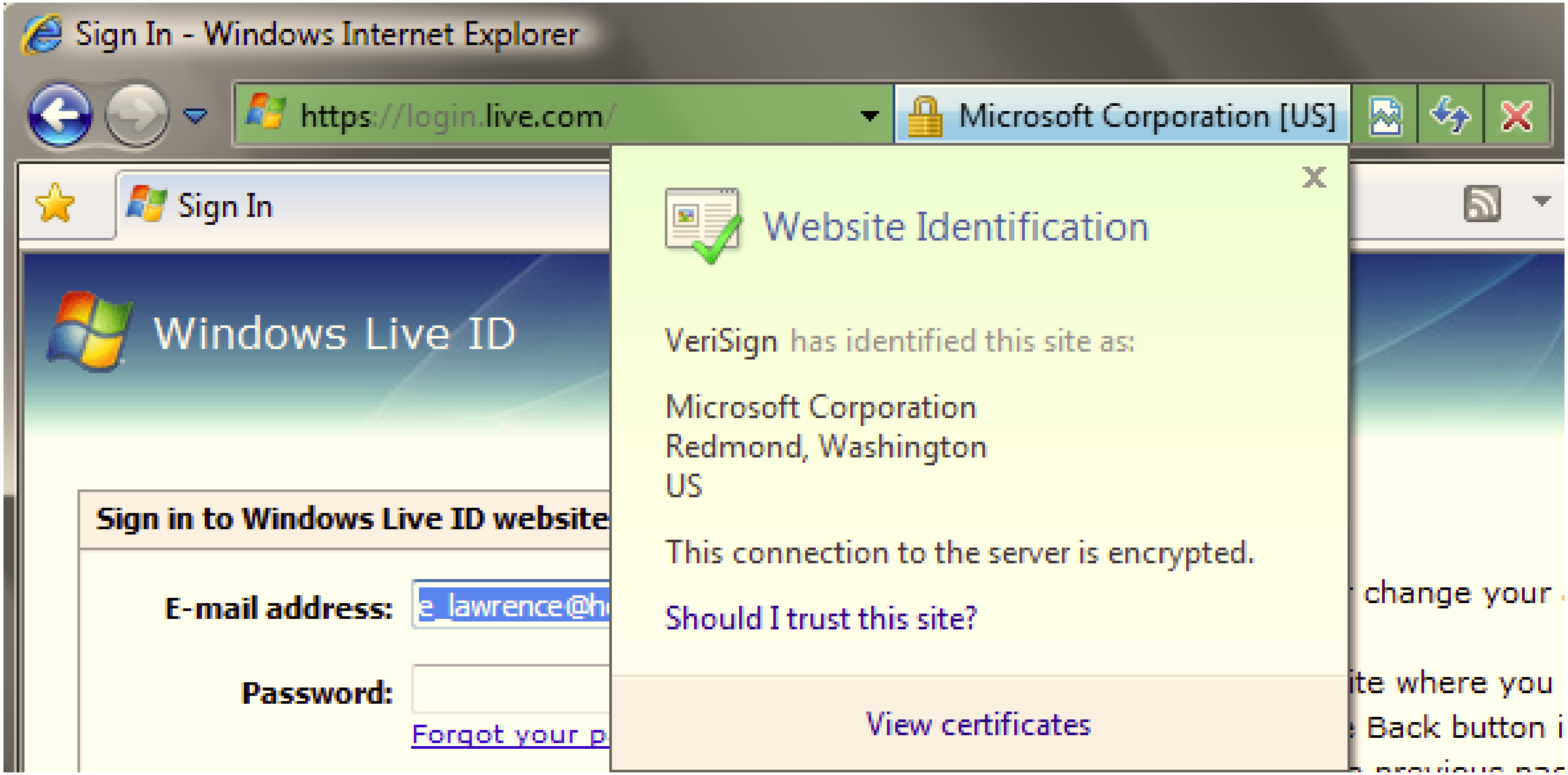
New U

New Us

logged

HTTPS - Extended Validation

- Supported by all modern browsers.
- Over 10,000 sites with extended validation certificates.



Website Identification

VeriSign has identified this site as:

Microsoft Corporation
Redmond, Washington
US

This connection to the server is encrypted.

Should I trust this site?

View certificates

Sign in to Windows Live ID website

E-mail address: e_lawrence@h

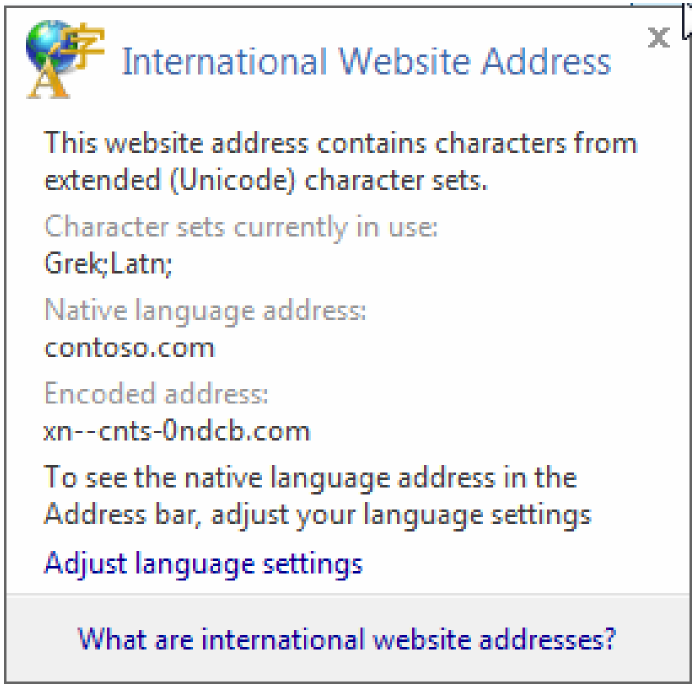
Password:

Forgot your p

Social Engineering

International Domain Names

- Protects against homograph style phishing attacks
- Unicode display restricted to user’s configured languages



International Website Address

This website address contains characters from extended (Unicode) character sets.

Character sets currently in use:
Grek;Latn;

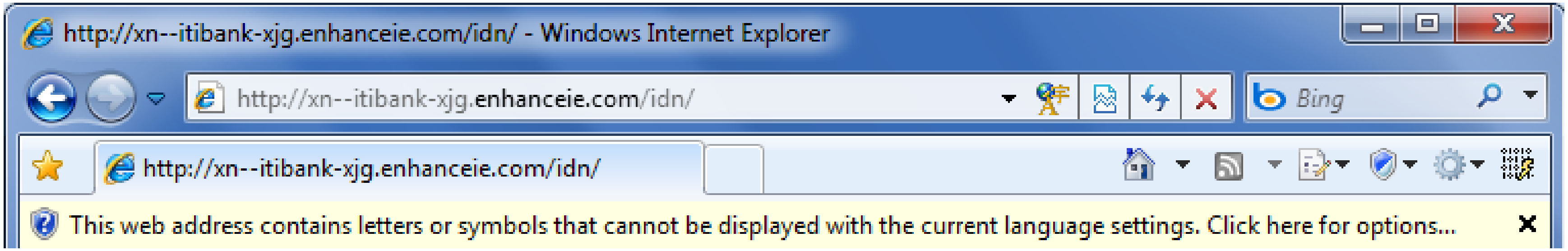
Native language address:
contoso.com

Encoded address:
xn--cnts-0ndcb.com

To see the native language address in the Address bar, adjust your language settings

Adjust language settings

What are international website addresses?



http://xn--itibank-xjg.enhanceie.com/idn/ - Windows Internet Explorer

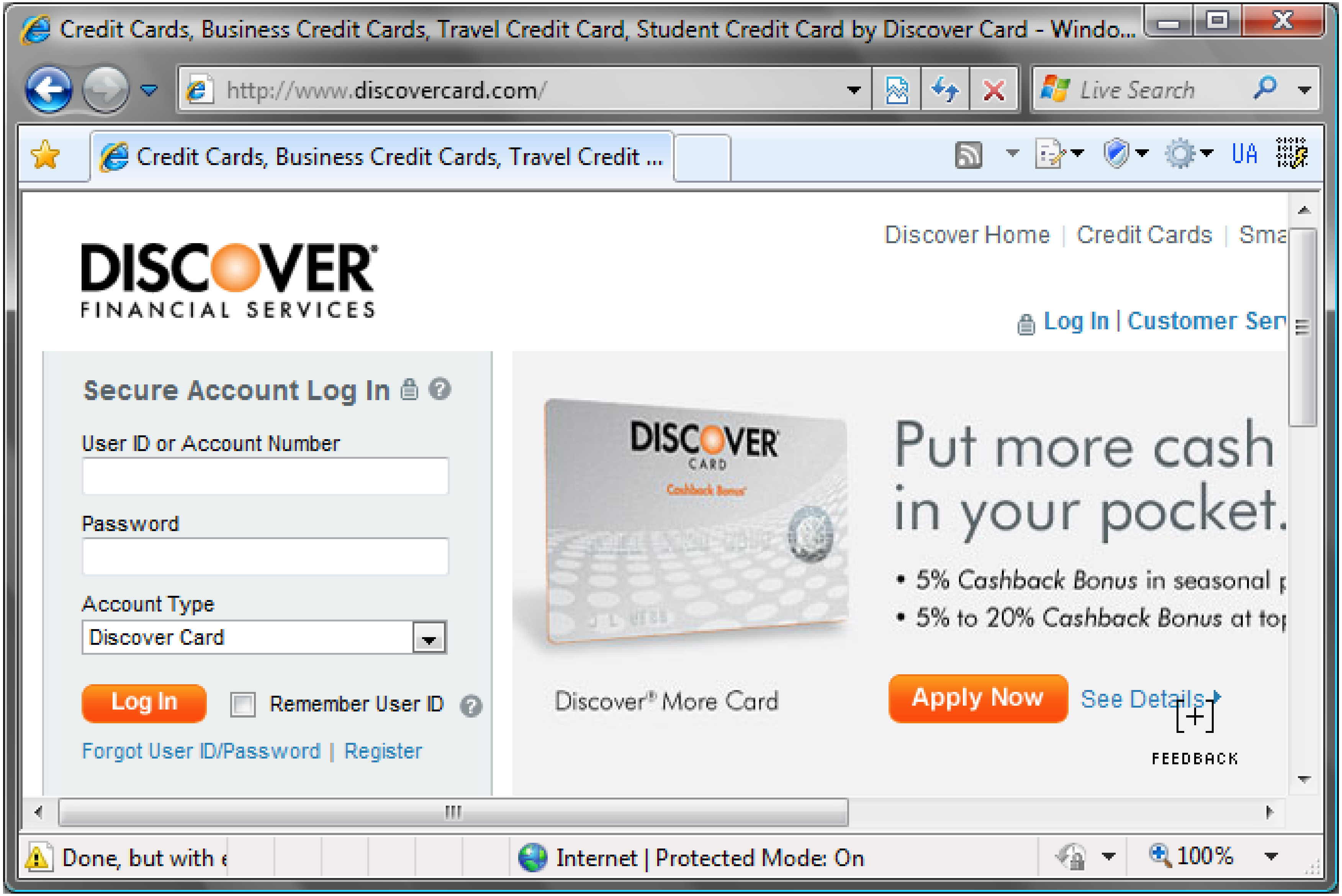
http://xn--itibank-xjg.enhanceie.com/idn/

http://xn--itibank-xjg.enhanceie.com/idn/

This web address contains letters or symbols that cannot be displayed with the current language settings. Click here for options...

HTTPS Mistakes

Insecure Login Form



Credit Cards, Business Credit Cards, Travel Credit Card, Student Credit Card by Discover Card - Windo...

http://www.discovercard.com/

Discover Home | Credit Cards | Sma

Log In | Customer Ser

Secure Account Log In

User ID or Account Number

Password

Account Type

Discover Card

Log In □ Remember User ID

Forgot User ID/Password | Register

Put more cash in your pocket.

- 5% Cashback Bonus in seasonal
- 5% to 20% Cashback Bonus at to

Discover® More Card

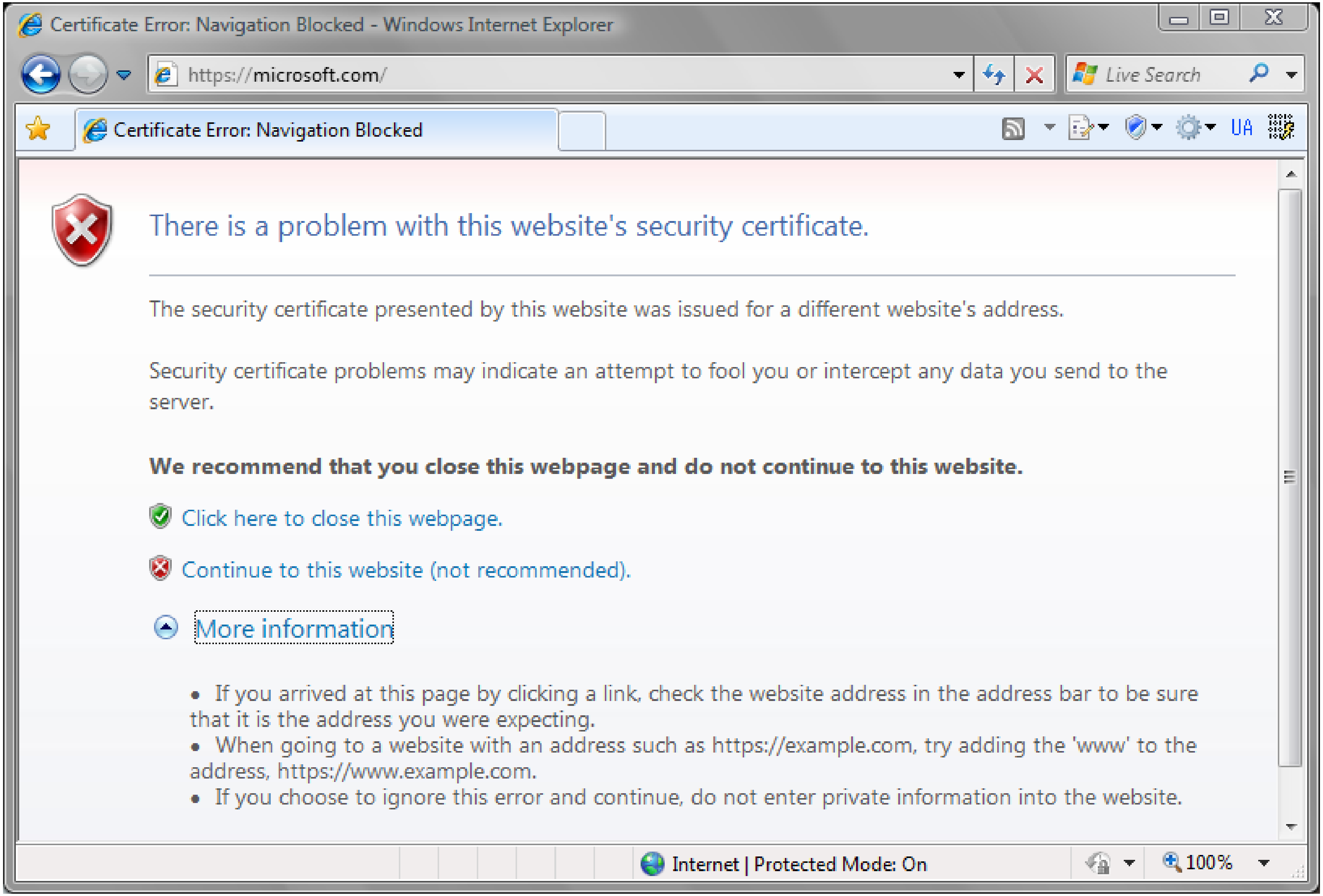
Apply Now See Details

Done, but with e

Internet | Protected Mode: On

Live Search
Credit Cards, Business Credit Cards, Travel Credit ...
DISCOVER FINANCIAL SERVICES
DISCOVER CARD
Cashback Bonus
FEEDBACK
100%

Certificate Mismatch



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://microsoft.com/
Live Search
Certificate Error: Navigation Blocked
UA

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

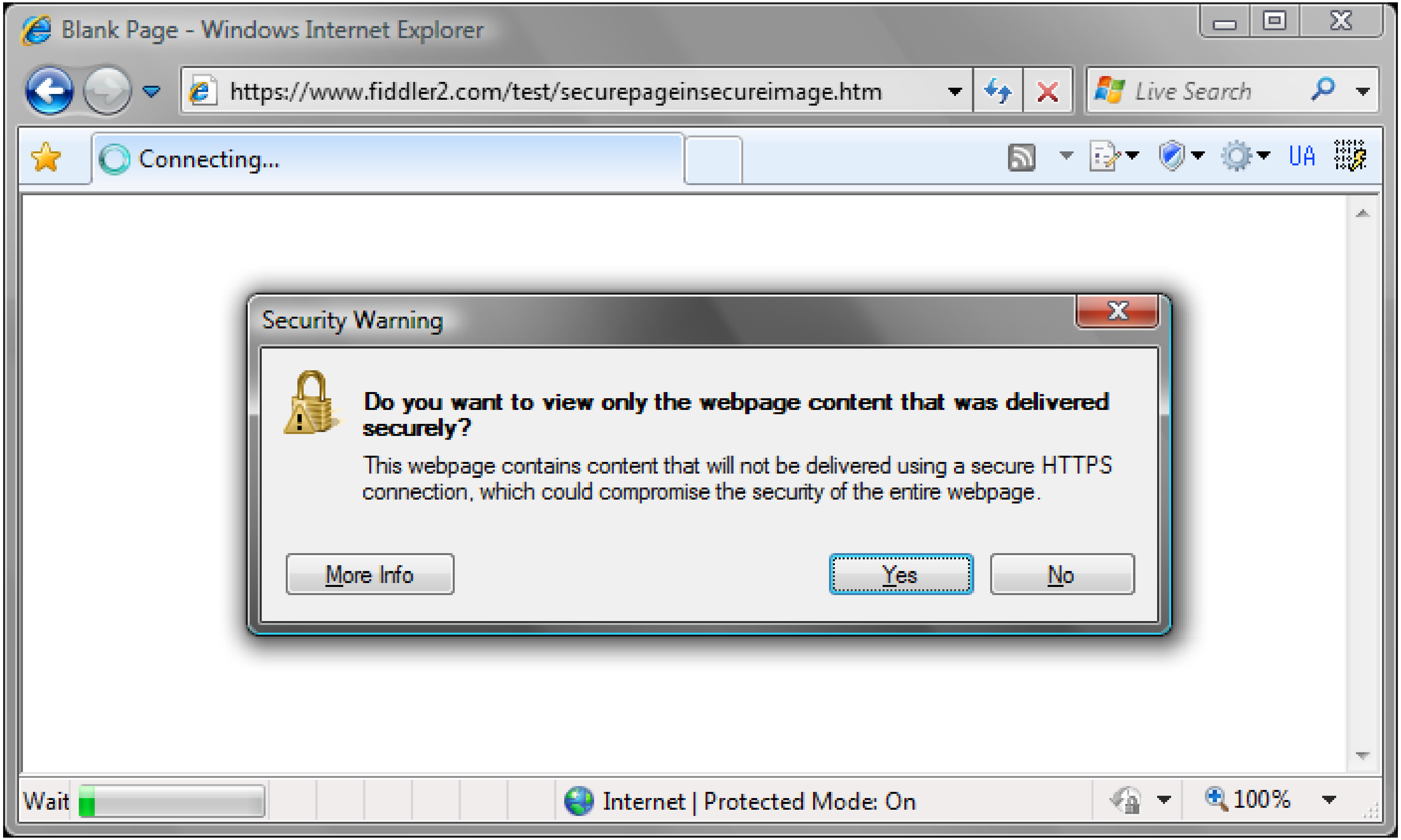
Click here to close this webpage.

Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

Mixed Content - Prompt



Blank Page - Windows Internet Explorer

https://www.fiddler2.com/test/securepageinsecureimage.htm

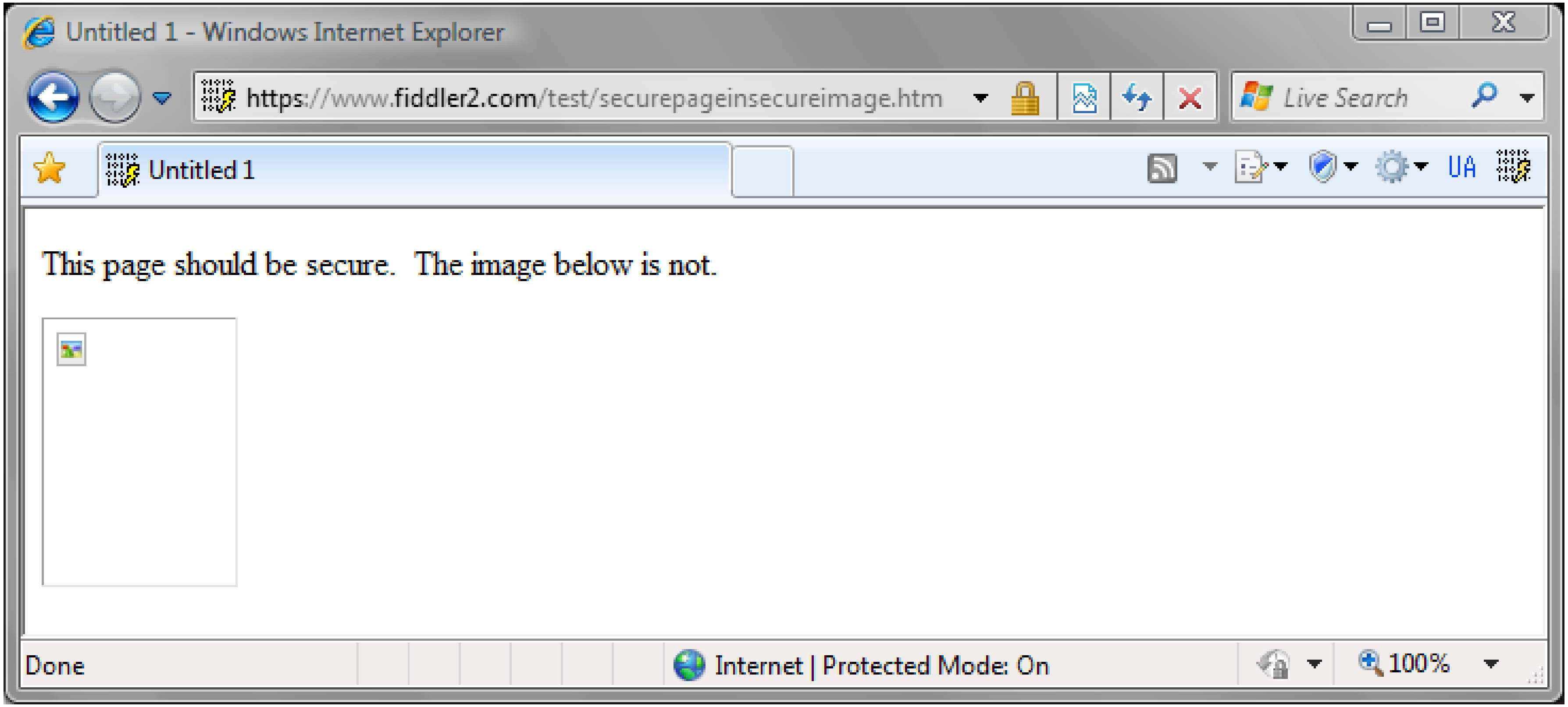
Connecting...

Security Warning

Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

Mixed Content Blocked

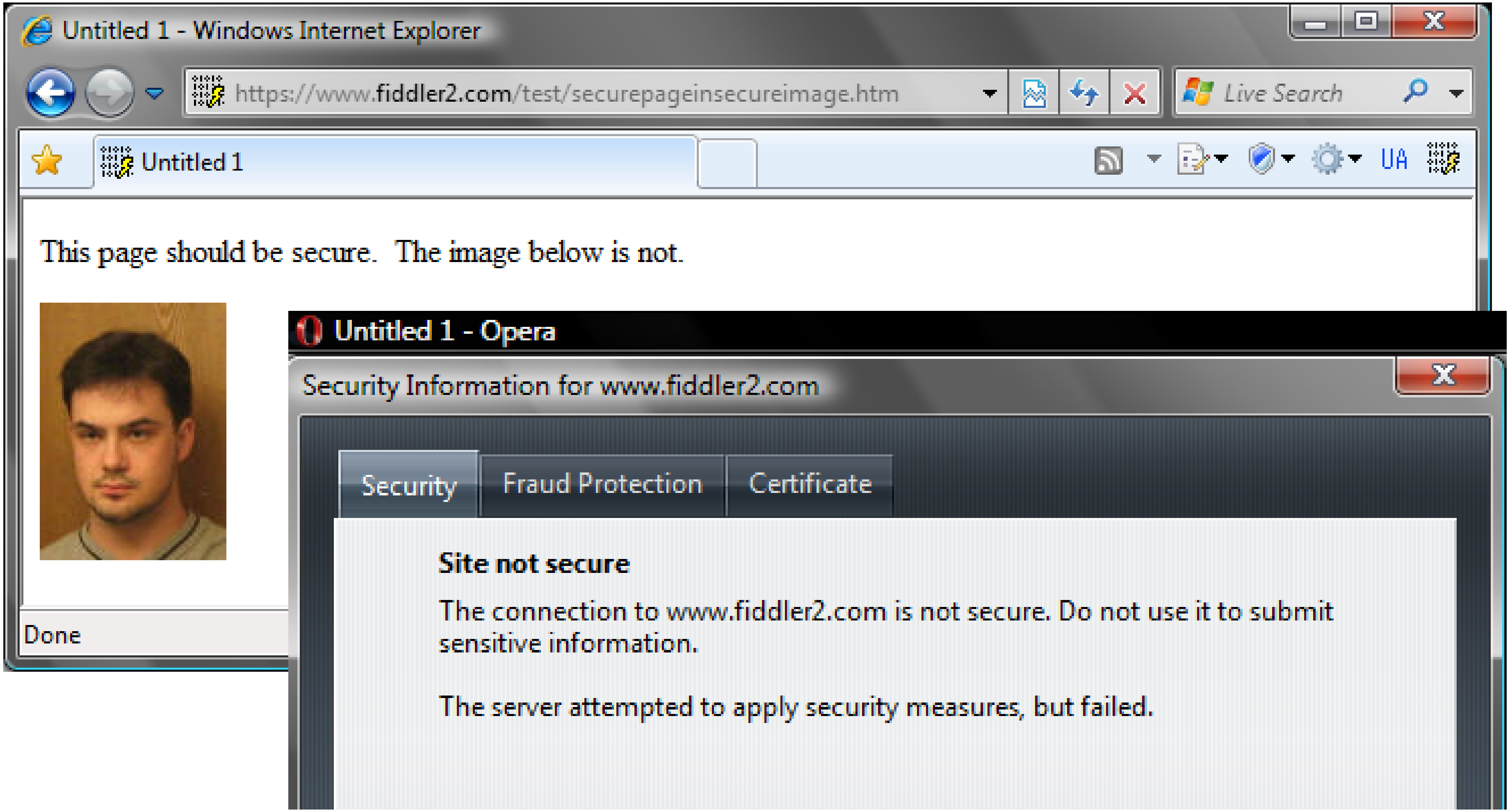


Untitled 1 - Windows Internet Explorer
https://www.fiddler2.com/test/securepageinsecureimage.htm
Live Search
Untitled 1
UA

This page should be secure. The image below is not.

Done
Internet | Protected Mode: On
100%

Mixed Content shown – No lock



Untitled 1 - Windows Internet Explorer
https://www.fiddler2.com/test/securepageinsecureimage.htm
Live Search
Untitled 1
UA
Done
Untitled 1 - Opera
Security Information for www.fiddler2.com
Security
Fraud Protection
Certificate

This page should be secure. The image below is not.

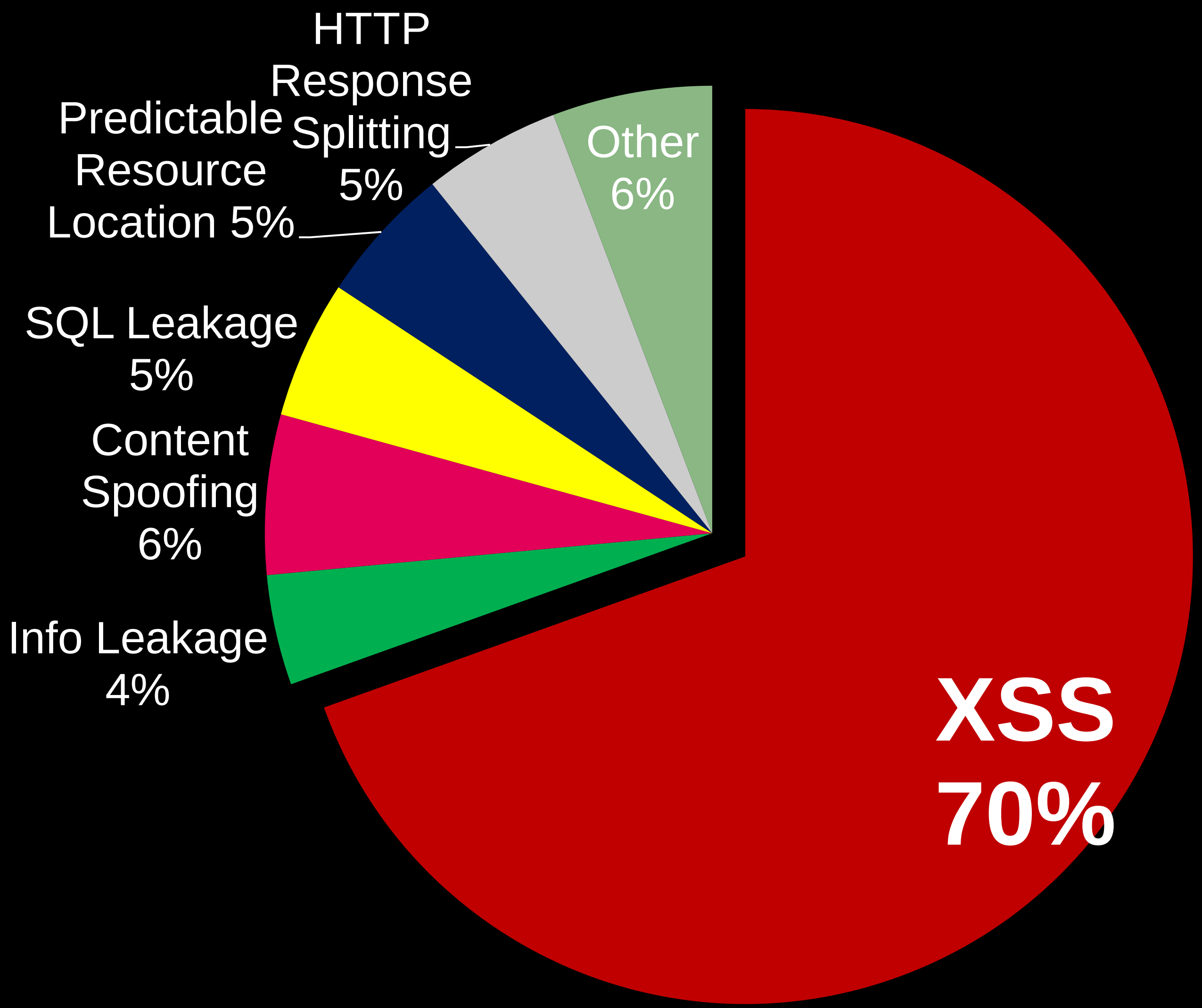
Site not secure

The connection to www.fiddler2.com is not secure. Do not use it to submit sensitive information.

The server attempted to apply security measures, but failed.

Mitigating XSS

XSS Statistics



Source: WhiteHat Security, August 2008

XSS Threats

Researcher Bryan Sullivan: “XSS is the new buffer overflow.”

- Steal cookies
- Log keystrokes
- Deface sites
- Misuse credentials
- Port-scan the Intranet
- Launch CSRF
- Steal browser history
- Abuse browser/AX vulnerabilities
- Evade phishing filters
- Circumvent HTTPS
- etc…

Demo

IE8 XSS Filter

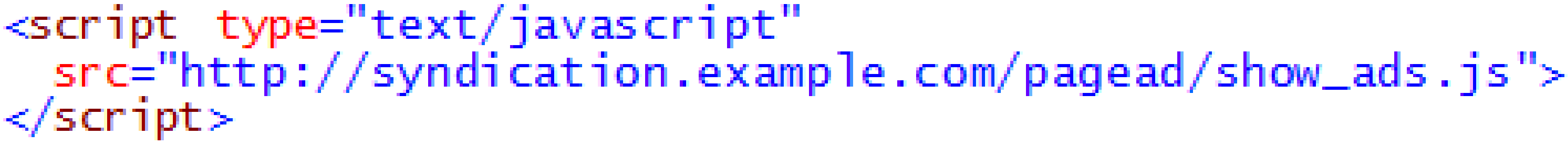
Comprehensive XSS Protection

- Disable US-ASCII codepage
- Disable sniffing of UTF-7 codepage
- Fix other codepage-related bugs
- Disable CSS expression() in IE8 Standards mode
- Offer script-sanitization functions for sites building mashups

Securing Mashups

How are mashups built today?

- Cross-domain script inclusion
- IFRAMEs



```
<script type="text/javascript"
  src="http://syndication.example.com/pagead/show_ads.js">
</script>
```

XDomainRequest

- Enables web developers to more securely communicate between domains
- Provides a mechanism to establish trust between domains through an explicit acknowledgement of cross domain access
- Access-Control-Allow-Origin syntax standardized

HTML5 postMessage()

- Enables two domains to establish a trust relationship to exchange object messages
- Provides a web developer a more secure mechanism to build cross-domain communication
- Part of the HTML5 specification; supported by all latest-version browsers.

postMessage – Sending

```
// Find target frame
var oFrame =
document.getElementsByTagName('iframe')[0];

// postMessage will only deliver the 'Hello’
// message if the frame is currently
// at the expected target site
oFrame.contentWindow.postMessage('Hello',
    'http://recipient.example.com');
```

postMessage – Listening

```
// Listen for the event.  For non-IE, use
// addEventListener instead.
document.attachEvent('onmessage',
function(e){
  if (e.domain == 'expected.com') {
      // e.data contains the string
      // We can use it here.  But how?
  }
});
```

JavaScript Object Notation

```
{"Weather":
{
  "City": "Seattle",
  "Zip": 98052,
  "Forecast": {
    "Today": "Sunny",
    "Tonight": "Dark",
    "Tomorrow": "Sunny"
  }
}}
```

Native JSON Support

- JSON.stringify()
- JSON.parse()

Based on ECMAScript 3.1; natively supported by modern browsers.

window.toStaticHTML()

Client-side string sanitization, based on the Microsoft Anti-XSS Library.

```
window.toStaticHTML(
"This is some <b>HTML</b> with embedded
script following... <script>
alert('bang!'); </script>!“
);
```

returns:

```
This is some <b>HTML</b> with embedded
script following... !
```

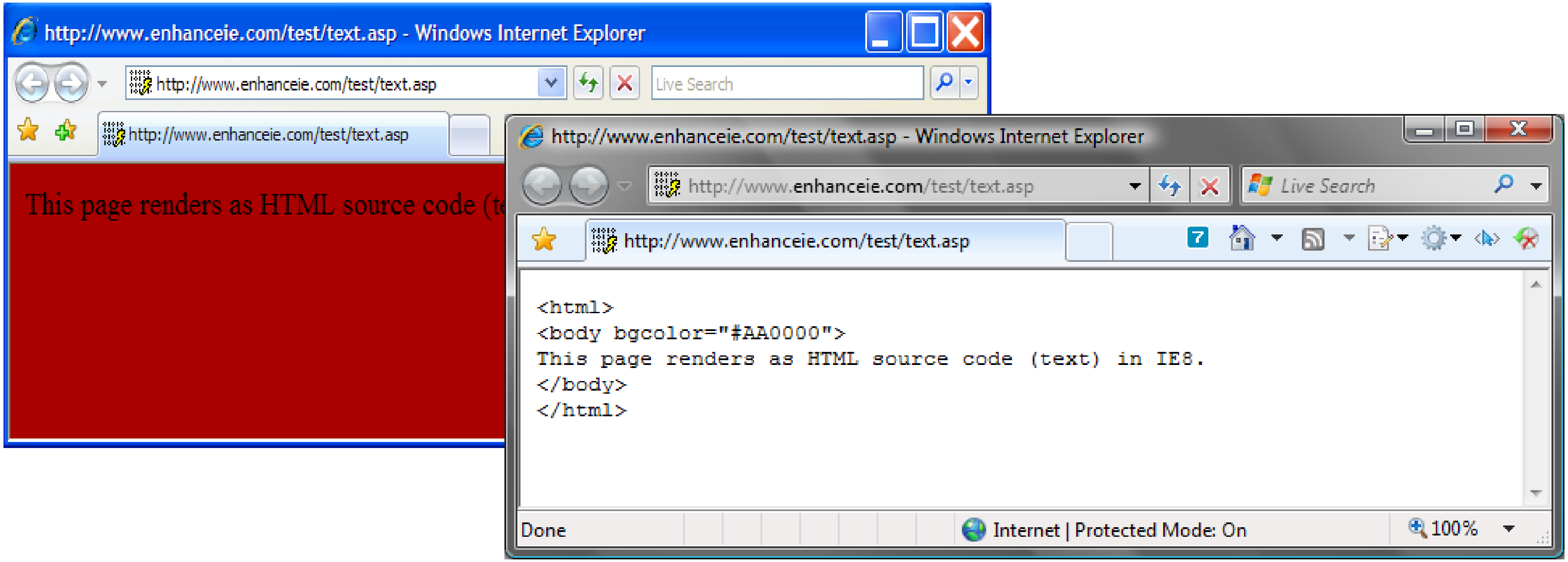
Putting it all together…

```
if (window.XDomainRequest){
  var xdr = new XDomainRequest();

  xdr.onload = function(){
    var objWeather = JSON.parse(xdr.responseText);

    var oSpan = window.document.getElementById("spnWeather");
    oSpan.innerHTML = window.toStaticHTML(
"Tonight it will be <b>" +
objWeather.Weather.Forecast.Tonight +
"</b> in <u>" + objWeather.Weather.City + "</u>."
);
    };

  xdr.open("POST", "http://evil.example.com/getweather.aspx");
  xdr.send("98052");
}
```

MIME-Sniffing

- No upsniff from image/*
- X-Content-Type-Options: nosniff
- Option to force file save:

```
Content-Disposition: attachment;filename="file.htm";
X-Download-Options: NoOpen
```


http://www.enhanceie.com/test/text.asp - Windows Internet Explorer
http://www.enhanceie.com/test/text.asp
Live Search
http://www.enhanceie.com/test/text.asp
http://www.enhanceie.com/test/text.asp - Windows Internet Explorer
http://www.enhanceie.com/test/text.asp
Live Search
http://www.enhanceie.com/test/text.asp
Done
Internet | Protected Mode: On
100%

This page renders as HTML source code (te

```
<html>
<body bgcolor="#AA0000">
This page renders as HTML source code (text) in IE8.
</body>
</html>
```

Best Practices

- Filter content using the Microsoft Anti-Cross Site Scripting Library.
- Use JSON, toStaticHTML for local content sanitization
- Specify encoding using in the Content-Type header:

  ```
  Content-Type: text/html; charset=UTF-8
  ```
- Use XDomainRequest and postMessage() rather than using <SCRIPT SRC=>
- Use HTTPOnly cookies

  ```
  Set-Cookie: secret=value; httponly
  ```

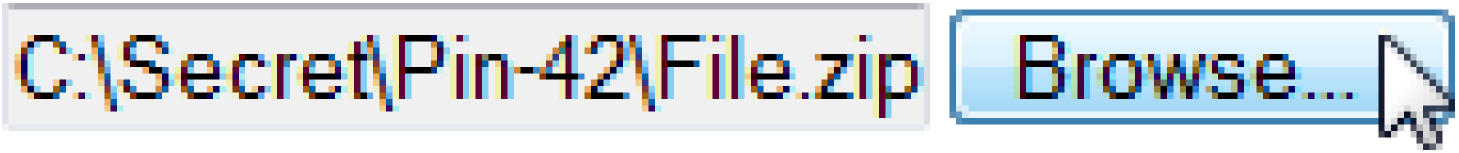
Demo

Design Flaws in the Web Platform

Privacy

File Upload Control

- Text input control now read-only



C:\Secret\Pin-42\File.zip

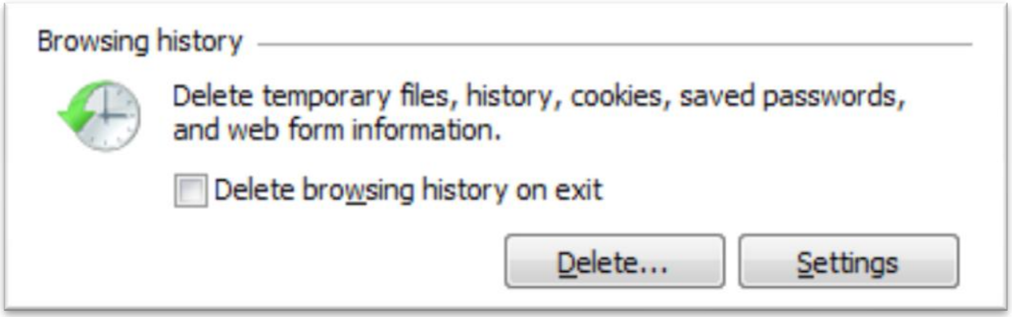
Server no longer gets full filename:

```
Content-Disposition: form-data;
name="file1"; filename="File.zip“
```

Local JavaScript sees a fixed path for compatibility:

```
file1.value == “C:\fakepath\File.zip”
```

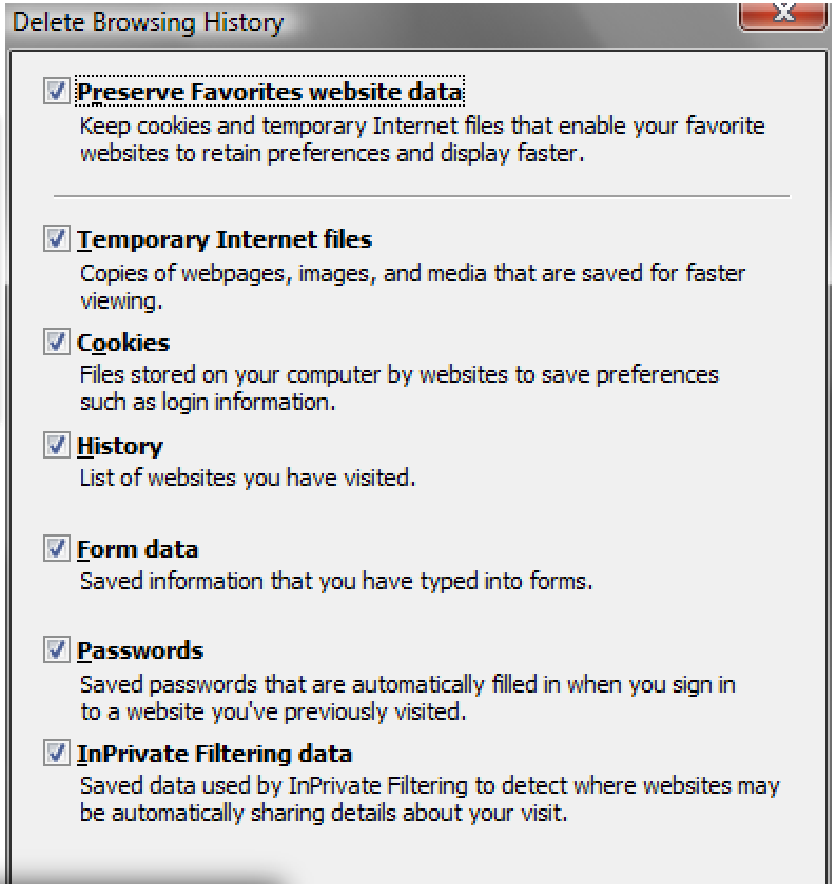
Enhanced Cleanup



Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit



Delete Browsing History

☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

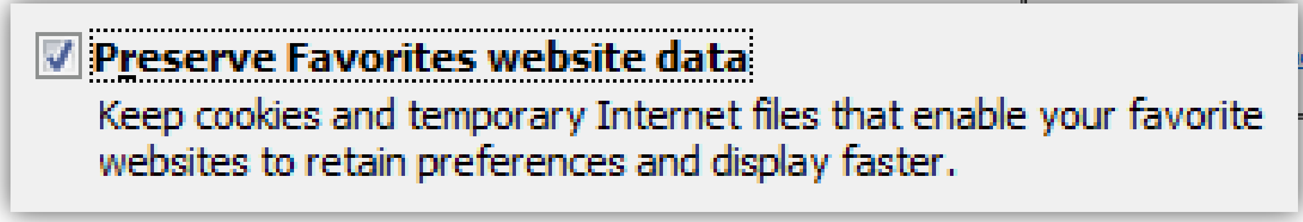
☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

☑ **History**
List of websites you have visited.

☑ **Form data**
Saved information that you have typed into forms.

☑ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

☑ **InPrivate Filtering data**
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.



☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

InPrivate™

InPrivate™ Browsing

Shared PC privacy

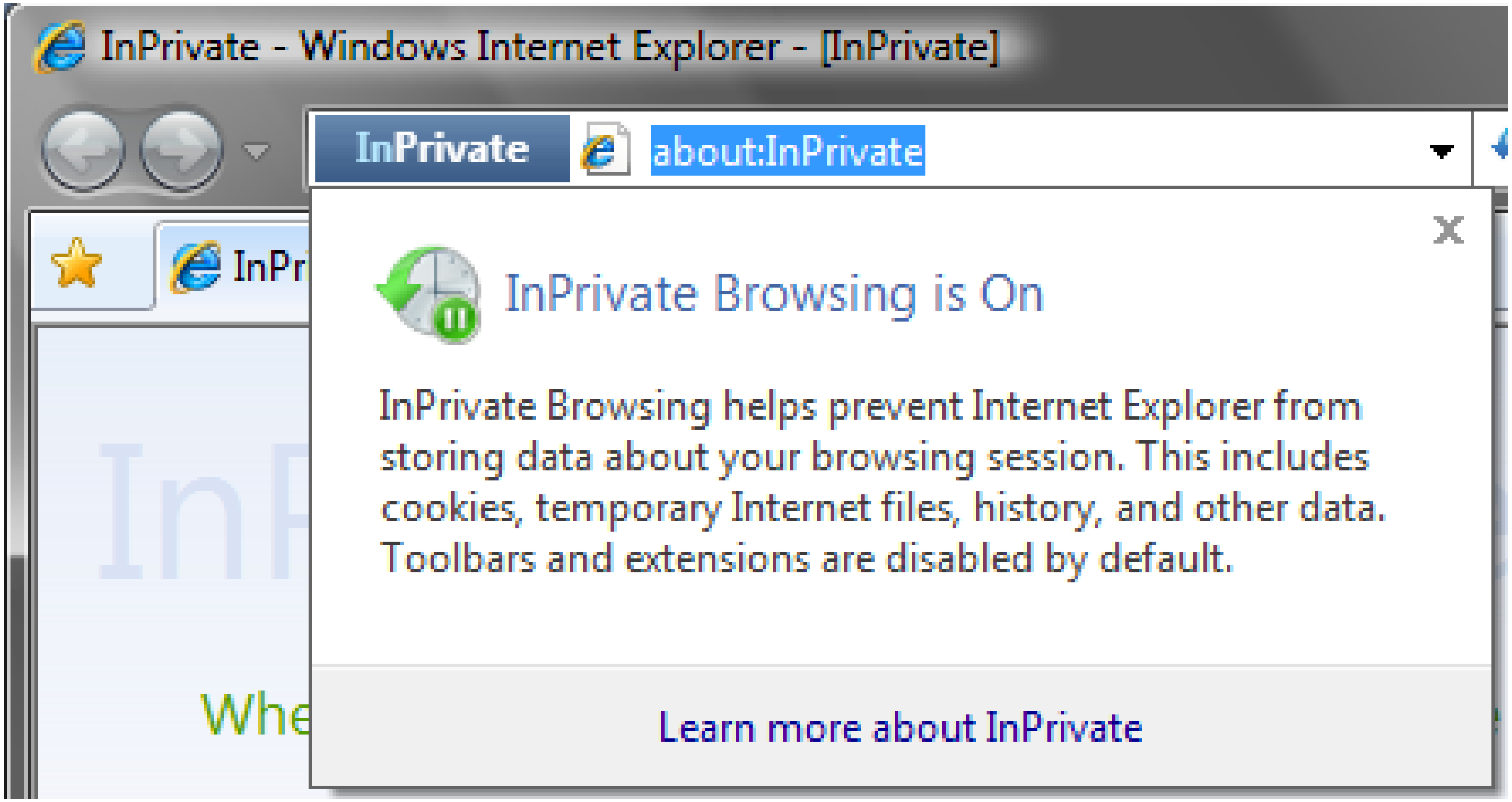
- Browsing leaves no tracks locally (cookies, DOMStorage, cache, history, etc)

InPrivate™ Filtering

Awareness and control of web profile aggregation

- Assess, on an ongoing basis, user exposure to third-party content.
- Helps to prevent information disclosure by automatically blocking high-frequency third-party content from sites users visit.

InPrivate™ Browsing



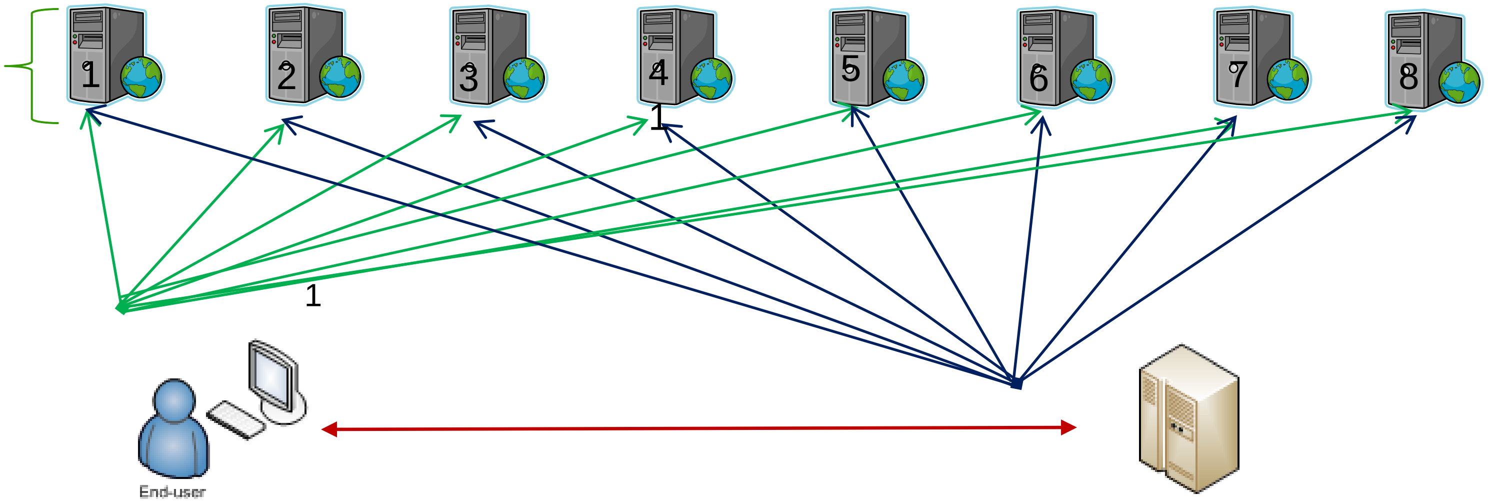
InPrivate Browsing is On

InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default.

Learn more about InPrivate

Background on 3rd Party Aggregation

- Over time, users' history and profiles can be surreptitiously aggregated
  - *Any* third-party content can be used like a tracking cookie
    - There is little end-user notification or control today
    - Syndicated photos, weather, stocks, news articles; local analytics, etc.…
  - Unclear accountability with third party security & privacy policies



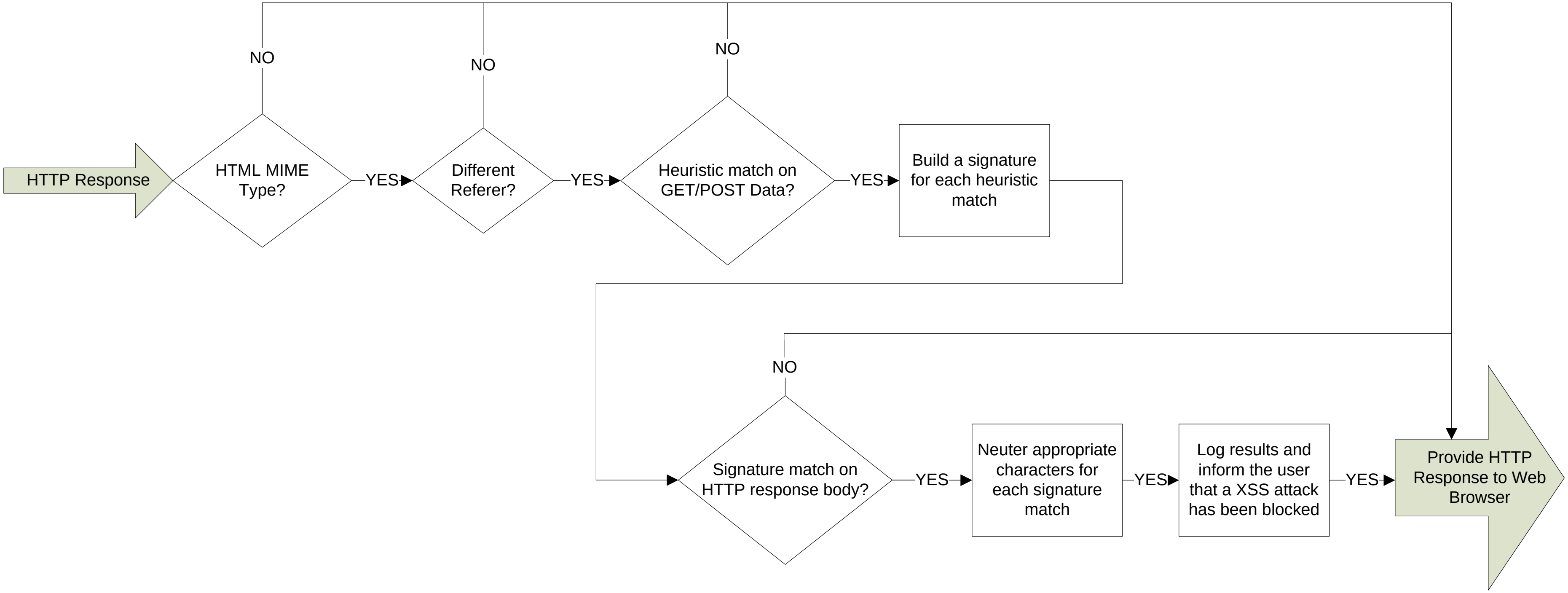
Are we finished yet?

Questions?

ericlaw@microsoft.com

http://**blogs.msdn.com**/ie/archive/tags/Security/default.aspx

XSS Filter


HTTP Response
HTML MIME Type?
NO
YES
Different Referer?
NO
YES
Heuristic match on GET/POST Data?
NO
YES
Build a signature for each heuristic match
NO
Signature match on HTTP response body?
YES
Neuter appropriate characters for each signature match
YES
Log results and inform the user that a XSS attack has been blocked
YES
Provide HTTP Response to Web Browser