

## Internet Explorer 8 Makes Security Strides

Dawn Gordon, Senior Network Analyst

Are you using the latest web browser? Many studies have shown that most internet users are not using the latest browser version or even bothered installing the latest patches for their browser of choice. This leaves most users vulnerable to exploitation of their web browsers and the security protections it can provide. Internet Explorer (IE) 8 is designed with the web developer in mind and Microsoft has brought to the forefront better support of Web Standards (W3C). In this article, I'm focusing on the latest security improvements of IE 8 and how it will hopefully keep you safely browsing the web.

IE 8 focuses its security improvements on three key exploits:

- Social engineering exploits
- Browser-based exploits
- Web server exploits

### ***Social engineering exploits***

Building upon the Phishing filter introduced in IE 7, Microsoft has integrated a SmartScreen® Filter for launch with IE 8. This filter is similar to the add-ons of other web browsers. SmartScreen Filter helps protect against a broad range of threats including rogue sites distributing malicious software designed to steal personal information (credit card numbers, usernames, passwords etc.). Malicious sites are identified by making use of phishing lists (sites reported to Microsoft) and prevent or block known sites from downloading malware. A red SmartScreen blocking page will pop-up warning you of the potential exploit and assists in navigating you safely away from the site. As with previous IE versions Microsoft verifies all reported sites before adding it to the phishing list.

The SmartScreen Filter also utilizes certain heuristics and telemetry to help protect against websites that have not yet been reported as malicious such as IP-based sites asking for personal account information. A different blocking page alerts you of the potential threat, but again will assist in navigating you safely away from the site.

Additionally, Microsoft's new Domain Highlighting will supplement the SmartScreen Filter to protect against deceptive URL's. The idea behind this improvement is to highlight the top level URL in bold black font while leaving the remainder of the URL grayed out. This eliminates any doubt as to which website you are visiting.

### ***Browser-based exploits***

IE 8 continues to protect against browser-based exploits with enhanced ActiveX controls. Because blocking ActiveX controls isn't an option, this enhanced design helps reduce the chances of malicious ActiveX controls from exploiting your site.

These enhanced controls provide you with more control in two different methods:

- Per-Site ActiveX
- Per-User ActiveX

Per-Site ActiveX controls, by default are only allowed to run from the point of installation. This enables administrators to manage where the ActiveX controls are allowed to run. In contrast, Per-User ActiveX controls, by default will only be activated for the user that installed it. Administrators can now decide which users will be allowed an ActiveX installation through Group Policy.

Data Execution Prevention or DEP is one of the major security advances now enabled by default in IE 8. DEP helps prevent certain types of viruses and security threats from being written in executable memory space. If a website or ActiveX control triggers a DEP error, the browser tab considered the security threat will close leaving all other browser tabs open. This can be implemented on a tab by tab basis because each browser window is now considered its own process in task manager.

A new security approach deployed in IE 8 Beta 2 is called InPrivate mode. This security approach takes “privacy” browsing to the next level with 3 different methods:

- InPrivate Browsing
- InPrivate Blocking
- InPrivate Subscriptions

InPrivate Browsing allows you to control how your browsing history, cookies, temporary internet files etc. are stored. This browsing feature is turned on in a window by window basis. All tabs opened up during this session are protected. Some data is stored during the session to allow the pages to work correctly, but are discarded as soon as the browser window is closed. This feature would work well in a Kiosk environment or where multiple users share the same PC.

InPrivate Blocking allows you to control what information is shared with the websites you visit. If your information is being shared across multiple websites you can decide to allow or block the content automatically or manually.

InPrivate Subscriptions builds upon the InPrivate Blocking mode and allows you to subscribe to a published list of websites that will allow or block the content for you. As with most IE features administrators can control these features using Group Policy.

## ***Web server exploits***

As of late, one of the more prevalent web exploits that can potentially affect all of us is Cross-Site Scripting (XSS). In a nutshell, XSS is a reflection attack, where a user receives a URL with an embedded script either from e-mail or a malicious website. When a user clicks on the URL it takes them a trusted site where the malicious script is reflected and executes. When the script runs it can provide a variety of tasks including downloading malicious code, stealing cookies, user credentials etc. IE 8 will introduce the Cross-Site Scripting Filter to help mitigate the threat of XSS attacks by dynamically detecting and blocking the attack, but still allowing the website to remain up and running as normal.

## ***Conclusion***

As web exploits such as URL phishing attacks continue to grow exponentially, Microsoft is attempting to take necessary security measures to address the concerns of internet users. The latest security improvements of IE 8 will help put you back in control of your data. Even though IE 8 has been out a short time I've seen significant security improvement over previous versions of Internet Explorer. As long as the security features are “enabled”, as with most security features, I believe IE 8 will help you browse the web safely.

#

#

#

Dawn Gordon, Senior System Analyst  
(937) 384-0444 ext 2171  
Email:dawn.gordon@digitalcontrols.com

Dawn Gordon has been a member of Digital Controls service team for 4 years. As a Senior Systems Analyst, Dawn is responsible for diverse security and networking disciplines including Microsoft Enterprise Server deployments and design and installation of network infrastructures across a variety of business sectors.

Digital Controls is a local IT services and software company. Digital Controls Technology Services Group provides services to IT in the key areas of security, data storage management, networking, Microsoft infrastructure, and product sourcing. These services are delivered through consulting, professional services, on-site and remote managed services.