Windows


# A Safer Online Experience

**White Paper**
**February 2009**

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.



Microsoft, Internet Explorer, the Internet Explorer logo, Smartscreen, Windows and the Windows logo are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Contents



# Introduction

The Internet has enhanced our lives in nearly every way – connecting us to the people and information we care about, keeping us entertained, helping us find the answers we need, and enabling us to be more productive than ever. However, as more of the things we do every day depend on the Internet, online crime has risen in turn.

Cybercriminals are using increasingly sophisticated and deceptive methods, such as:

**Malware**, which is software that a cybercriminal can use to steal your bank account information, track everything you type, send out malicious software or spam, or harm your computer.

**Phishing**, where a cybercriminal pretends to be a legitimate organization, such as your bank, in order to deceive you into giving up personal information such as credit card numbers and account information.

Both of these methods often involve tricking you into clicking on a link or downloading a file that appears legitimate, but is actually harmful. But cybercriminals are also using more elaborate ways to attempt to compromise websites and attack your computer without your knowledge, including "cross-site scripting" and "click-jacking," both of which are becoming increasingly dangerous threats.

Many of these threats can be mitigated simply by keeping the software on your computer up to date – especially your web browser. Older browsers simply aren't equipped to handle today's threats, and even some newer browsers don't provide the level of protection you need.
In this paper, we'll talk about some of the ways Windows® Internet Explorer® 8's new and enhanced security features help keep you safer online, show you some of the tactics

cybercriminals use, and walk you through some examples of the real-world attacks we protect you against.

## How Internet Explorer 8 Helps You Stay Safer Online

Our customers have told us that safety is one of their most significant concerns – that's why we continuously monitor the effectiveness of our safety features and evolve our approach to protection as cybercriminals change their tactics. We take a thorough approach to safety that is grounded in the principle of "defense in depth" – enabling our software and services to be more secure, protecting against current and emerging threats, and helping customers identify and avoid the kinds of tricks that cybercriminals use to harm you. Some of the protection we offer is visible to you – helping you avoid fraudulent content and sites – and some works behind the scenes to protect from attacks on your computer.

As part of this work, we've packed Internet Explorer 8 with more industry-leading features that help keep you safer online.

We're helping to protect you from today's threats, including malware and phishing, as well as emerging threats that can compromise your computer without your knowledge. Other browsers either don't offer you this level of protection or require you to download and configure third-party add-ons to get it, but with Internet Explorer 8 you get it right out of the box, and turned on by default. It's also the only web browser available today that offers free, 24-hour telephone support for viruses and safety issues[1].

For example, we've built upon the phishing protection in Internet Explorer 7 with the SmartScreen® filter, which now adds protection from malware – a threat that is growing significantly faster than phishing. The anti-malware protection works by presenting you with a warning or blocking screen when you visit a malicious site or attempt to download a malicious program.

While we continue to block millions of phishing site views every month, the scale of the malware threat is currently significantly larger than phishing. With Internet Explorer 8, we are blocking 10 times more attempts by cybercriminals to trick users into installing malware as we block attempts to phish users every day. At least one in every 200 downloads is malware that we are protecting users from with the SmartScreen filter in Internet Explorer 8. This protection does not exist for previous versions. In addition, our research has shown that Internet Explorer 8 has better protection from socially engineered malware attacks than other browsers on the market today.

This is why you, your friends, and your family should upgrade to Internet Explorer 8 today – one in 40 of them could be protected from attacks *this week*.

[1] (For phone numbers in your region, please visit www.microsoft.com/protect/support/.)

## How Cybercriminals Operate

So, how are cybercriminals a threat to you?

Today's online threats generally fall into two types: *attacks on you*, and *attacks on your computer*.

*Attacks on you* attempt to trick you into an unsafe activity. They might appear to be something benign or familiar, such as a free game, an email from your bank, or even a security warning. By deceiving you into clicking on a link or entering information on a fraudulent site, cybercriminals can collect your bank account information or logins and passwords for your favorite sites, or install malicious software to steal personal information or send spam. Unfortunately, no matter what operating system or browser you use, this often puts the burden on you to make decisions about whether a particular site, link or download is trustworthy. Our approach to these threats is to make those decisions on your behalf where we can, while giving you the information you need to spot these deceptions and avoid these kinds of attacks.

**What Can You Do To Be Safer?**

The most important thing you can do today is upgrade your browser – download Internet Explorer 8 today at www.microsoft.com/ie8.

You should also keep all the other software on your PC up to date – use Microsoft Update to install all critical and optional updates, and make sure your browser add-ons and other applications are current.

You should also install a current anti-virus product and keep its signatures up to date.

Pay attention to security warnings from your firewall and anti-virus software – but beware of the kinds of fake security warnings described in this paper – and make sure your firewall is on and up to date. And, finally, make sure that your Internet service provider has spam protection, so that less unwanted and fraudulent email reaches your inbox.

For information on how to do all of this, and to learn more about phishing, malware and other threats, visit www.microsoft.com/protect.

*Attacks on your computer* are less prevalent, but just as dangerous. These attacks often deliver malicious programs to your computer, without your consent or awareness. They do this by leveraging vulnerabilities in the websites you visit or the software on your PC to install malicious software or compromise your personal information. A large percentage of these attacks are mitigated just by keeping the software on your PC current, but Internet Explorer 8 also includes some features to prevent or avoid these kinds of attacks.

## Protecting Against Attacks On You

Cybercriminals continue to rely on deceptive social engineering attacks to prey on unsuspecting web users. Whether it's via an email that appears to be from your bank, a search result for popular content such as games and movies, an advertisement or a link in an instant message promising free stuff, or a fake notification from a social networking site, there is virtually no trick they haven't tried. These attacks are intentionally genuine-looking, and rarely does the victim know they're at risk until it's too late. Microsoft developed the SmartScreen filter for Internet Explorer 8 so you can browse with more confidence – knowing you have a greater chance of being protected when you are targeted by one of these attacks.

The SmartScreen filter is a set of technologies designed to help protect users from evolving web and social engineering threats. SmartScreen is "URL reputation-based," which means that it evaluates the web addresses of servers hosting downloads and potential phishing sites to

determine if those sites are known to distribute malicious programs or steal personal information.

SmartScreen leverages advanced intelligence and our community of hundreds of millions of users who report suspicious sites to evaluate millions of web addresses every day to find the most recent and relevant attack sites. You're part of this community, too: if you see a site that looks suspicious or is distributing malicious software, you should report it. Just click on the "Safety" menu, choose "SmartScreen Filter" and click on "Report Unsafe Website…"

The SmartScreen analysis works alongside Microsoft's Malicious Software Removal Tool and Windows Defender, as well as common anti-virus products, in order to provide the most comprehensive protection against malicious software available today.

## Blocking Malicious Websites

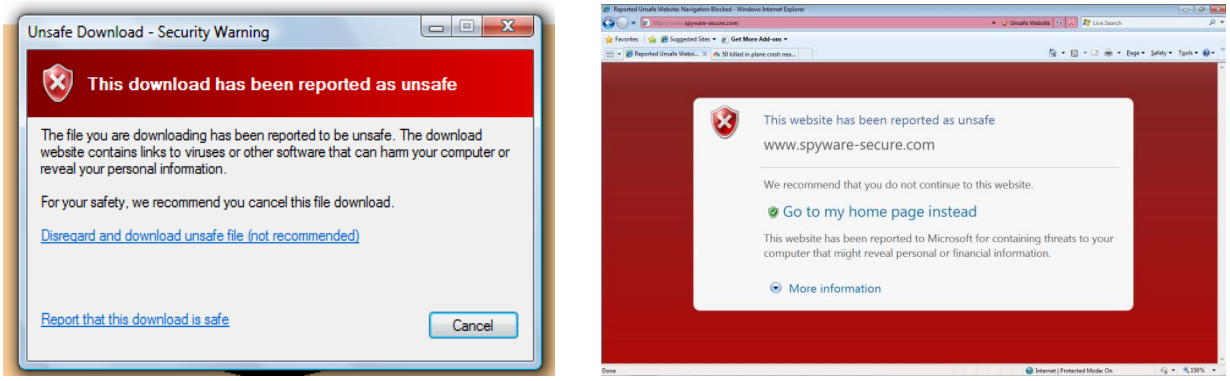


**Figure 1: What you see when SmartScreen blocks sites and downloads that have been reported as unsafe.**

If the SmartScreen filter detects a malicious website, Internet Explorer 8 will block the entire site. It can also provide a "surgical block" of malware or phishing hosted on legitimate websites – blocking just the malicious content without affecting the rest of the site. Here's how it works: if you navigate to a known malware distribution site, Internet Explorer 8 won't show it to you. Instead of an attack site, you see the screen to the right in Figure 1. For Internet Explorer 8, we've redesigned this screen with a bolder look, and included links to information to help educate you about identifying and avoiding these kinds of attacks. Another new feature we have added is protection from malicious downloads – if you attempt a download that has been reported as unsafe, you see the screen to the left.

## Social Engineering Attacks

Cybercriminals have gone to great lengths to disguise their attacks as legitimate websites or security warnings. As these sites are identified and reported, SmartScreen can block them automatically before you fall prey. These sites are being created in high volumes every day, so it's important to know what these attacks look like and how to avoid them. Here are a few examples of how attackers may try to deceive you.

*Fake Anti-Virus Warning*

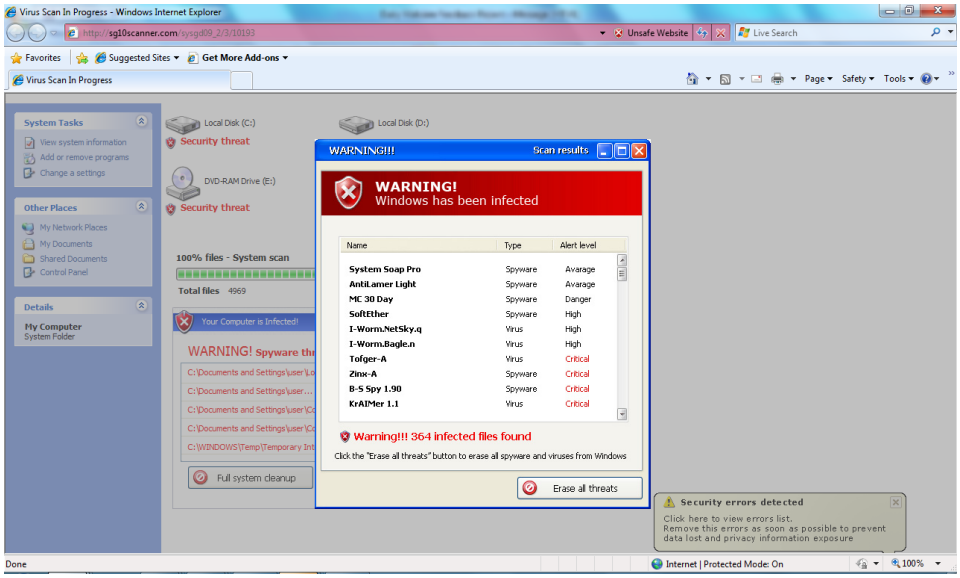


**Figure 2: Fake security warnings could trick you into installing malicious software.**

This common social engineering attack preys on your fear of having a virus installed on your PC, as well as your awareness of anti-virus indicators, like the one pictured above. In this attack, you're prompted with a professional-looking pop-up window from a phony anti-virus software company. It looks like a warning message from Windows. But it's actually a web page designed to look like a warning, and the "remedy" they want you to download can infect your PC with malware. SmartScreen blocks these attacks in large numbers every day, but keep an eye out for any anti-virus warning that looks suspicious. (For example, you should be suspicious if the borders on the pop-up windows look different than other windows on your computer, or if the window consistently pops up after you dismiss it.)

## Websites Offering Free Games, Movies or TV Shows


**Figure 3: Websites that offer free games, movies or TV shows might be a trick to get you to install malicious software.**

Everyone likes games, movies, and TV shows – especially when they're free – and cybercriminals know this. This type of attack is common when you're visiting a "free" website that offers some type of entertainment at no cost. You may have been directed to a site like this after doing a search on "games," or perhaps someone sent you a link to this site. Often, when you click on the free download offer, you're getting more than free content: you're also getting malicious software. SmartScreen blocks these sites when they have been reported to Microsoft, but keep an eye out for offers and sites that look too good to be true – they probably are.

## Phishing Attacks

Phishers masquerade as a legitimate person or business to convince you to give up your banking information and/or username and password. For example, you might receive an email from what looks to be your bank that says they're merging with another financial institution and need to verify your account information. The goal of the phishing email is to trick you into clicking on a link to a fake site where you "verify" your username, password and other personal information – which they can use to access your accounts and personal data. These attacks are increasingly sophisticated – with emails and websites that look exactly like those of the businesses you interact with every day. Internet Explorer 8's SmartScreen filter automatically advises you about known phishing sites, and also includes some tools to help you spot some of the telltale signs of these attacks. Today, Internet Explorer blocks more than one million phishing attempts every week.

The SmartScreen filter in Internet Explorer 8 advises you about known phishing websites to help you more safely browse content on the Internet. The filter analyzes website content for known

phishing techniques, and uses a global network of data sources to assess the trustworthiness of websites.

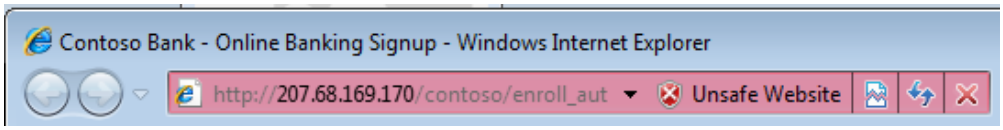


**Figure 4: Internet Explorer 8 warns you about phishing scams. Note that the title bar includes the name of your bank, but the highlighted domain is not the bank's URL.**

In addition to SmartScreen phishing protection, Internet Explorer 8 is the first browser to provide domain highlighting, so you always know which website you're visiting. Domain Highlighting lets you more easily interpret web addresses (URLs) to help you avoid deceptive and phishing sites that attempt to trick you with misleading URLs. It does this by highlighting the domain name in the address bar in black, with the remainder of the URL string in gray, making for easier identification of the site's true identity.
`


**Figure 5: Internet Explorer 8 highlights the domain in links you visit, so you know where you're really going.**

## Protecting Against Attacks On Your Computer

In addition to tricking you into installing malicious software or giving up your personal information, cybercriminals also exploit older software and plugins to conduct "drive-by" attacks using legitimate sites that have been compromised. In addition to blocking known attacks and helping you identify potential threats with the SmartScreen filter, Internet Explorer 8 includes other built-in security features and updates to help fend off drive-by attacks while you're online.

Many of these features operate behind the scenes to keep software components behaving like they should, preventing cybercriminals from accessing your computer's files and settings and keeping them from surreptitiously running their software on your PC. And it's important for you to do your part, too: many of these kinds of attacks exploit older, more vulnerable software, so you should keep all your software up to date with the latest security updates.

### What's a Drive-By Attack?

Some of the attacks Internet Explorer 8's under-the-hood technologies help prevent you from include "cross-site scripting" and "click-jacking." These kinds of attacks are hard to spot and often involve legitimate websites you may visit.

*Cross-site scripting:* Cross-site scripting attacks try to exploit vulnerabilities in the websites you use. In this attack, you might receive an email that contains a tampered website address. Once you click on the link, you are directed to a legitimate website that has been compromised to contain malicious content that can capture keystrokes and record your login and password.

Internet Explorer 8 includes a cross-site scripting filter that can detect these types of attacks and disable the harmful scripts. Unlike other web browsers, Internet Explorer 8 offers this protection right out of the box, and turned on by default.

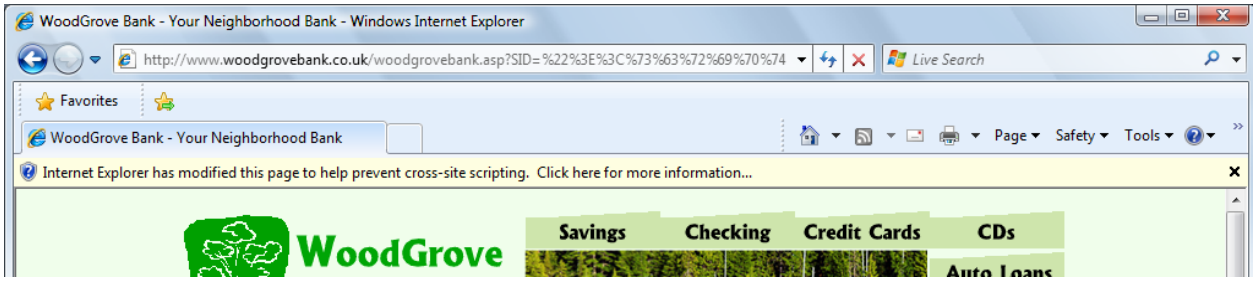


**Figure 6: Internet Explorer 8 detects potential cross-site scripting vulnerabilities and disables harmful scripts.**

*Click-jacking:* Click-jacking is an emerging online threat where an attacker's web page deceives you into clicking on content from another website without you realizing it. For example, it might hide a legitimate webpage as a "frame" inside a malicious page. When you click in the malicious page, you're actually clicking on something else: buying something from the site, changing some settings on your browser or computer, or viewing advertisements that cybercriminals get paid for. It's a complicated attack, but Internet Explorer 8 allows website developers to protect their sites from these kinds of attacks by preventing their legitimate pages from being "framed."

## Conclusion

As more of us depend on the web to learn, work, search, shop and keep in touch, we're becoming even more vulnerable to sophisticated forms of cybercrime. Helping you stay safe online is one of the most important things a web browser can do for you. Internet Explorer 8 is the only browser for Windows-based PCs that delivers a safer online experience right out of the box, dramatically improving the level of protection against current and emerging online threats. By upgrading your browser today, making sure the other software on your PC is up to date, and learning how to identify and avoid common attacks, you can better protect your computer and your personal information.