

Microsoft SmartScreen is a phishing and malware filter implemented in several Microsoft products, including Internet Explorer 8 and up, Hotmail, and the Windows 8 operating system. The system is designed to help protect users against attacks that utilize social engineering and drive-by downloads to infect a system by scanning URLs accessed by a user against a blacklist of websites containing known threats.

SmartScreen in Internet Explorer

SmartScreen was first introduced in Internet Explorer 8. When enabled, the system checks web pages against a whitelist of sites known not to be potential security risks. If SmartScreen does not encounter a match, it automatically displays a warning message before allowing access to sites that have been identified in that way to be potential security threats; such as those that could infect the system with malware or be a phishing scam. In July 2010, Microsoft claimed that SmartScreen on Internet Explorer had ample of sites from April 2011 containing malware, Internet Explorer 8 and SmartScreen had an average block rate of 90%, as opposed to the 13% achieved by Firefox, Chrome, and Safari; which all use a malware filter provided by Google. Internet Explorer 9 achieved an average block rate of 100% on the same test.^[1] The SmartScreen filter was also noted for quickly adding legitimate sites to its blocklists almost instantaneously, as opposed to the several hours it took for blocklists to be updated on other browsers.

In July 2010, Microsoft claimed that SmartScreen on Internet Explorer had blocked over a billion attempts to access sites containing security risks.^[2]

Criticism

Users cannot report phishing URLs via an online form. Rather, users must click the suspicious URL and visit the website using Internet Explorer's "report this website" feature.^[3] This exposes the user to drive by downloads or other malicious content in order to report the phishing website. Users cannot use Google's Chrome, Mozilla's Firefox, Apple's Safari, Opera or other web browsers to report phishing URLs to Microsoft.

SmartScreen filters can be bypassed. Some phishing attacks use a front-end URL that is published in the phishing email sent to users. Once clicked, the front-end URL redirects the user to a second site.^[4] The "report this website" option in Internet Explorer only reports the currently viewed page. The front-end URL in the phishing attack cannot be reported to Microsoft and the phisher can continue to redirect to other URLs

SmartScreen in Windows 8

Windows 8 introduced SmartScreen filtering at the desktop level, performing reputation checks by default on any file or application downloaded from the Internet. Microsoft faced concerns surrounding the privacy, legality and effectiveness of the new system; suggesting that the automatic analysis of files (which involves sending a cryptographic hash of the file and the user's IP address to a server) could be used to build a database of users' downloads online, and that the use of the outdated SSL 2.0 protocol for communication could allow an attacker to eavesdrop on the data. In response, Microsoft later issued a statement noting that IP addresses were only being collected as part of the normal operation of the service and would be periodically deleted, that SmartScreen on Windows 8 would only use SSL 3.0 for security reasons, and that information gathered via SmartScreen would not be used for advertising purposes or sold to third parties.

Disabling SmartScreen in Windows 8.1?

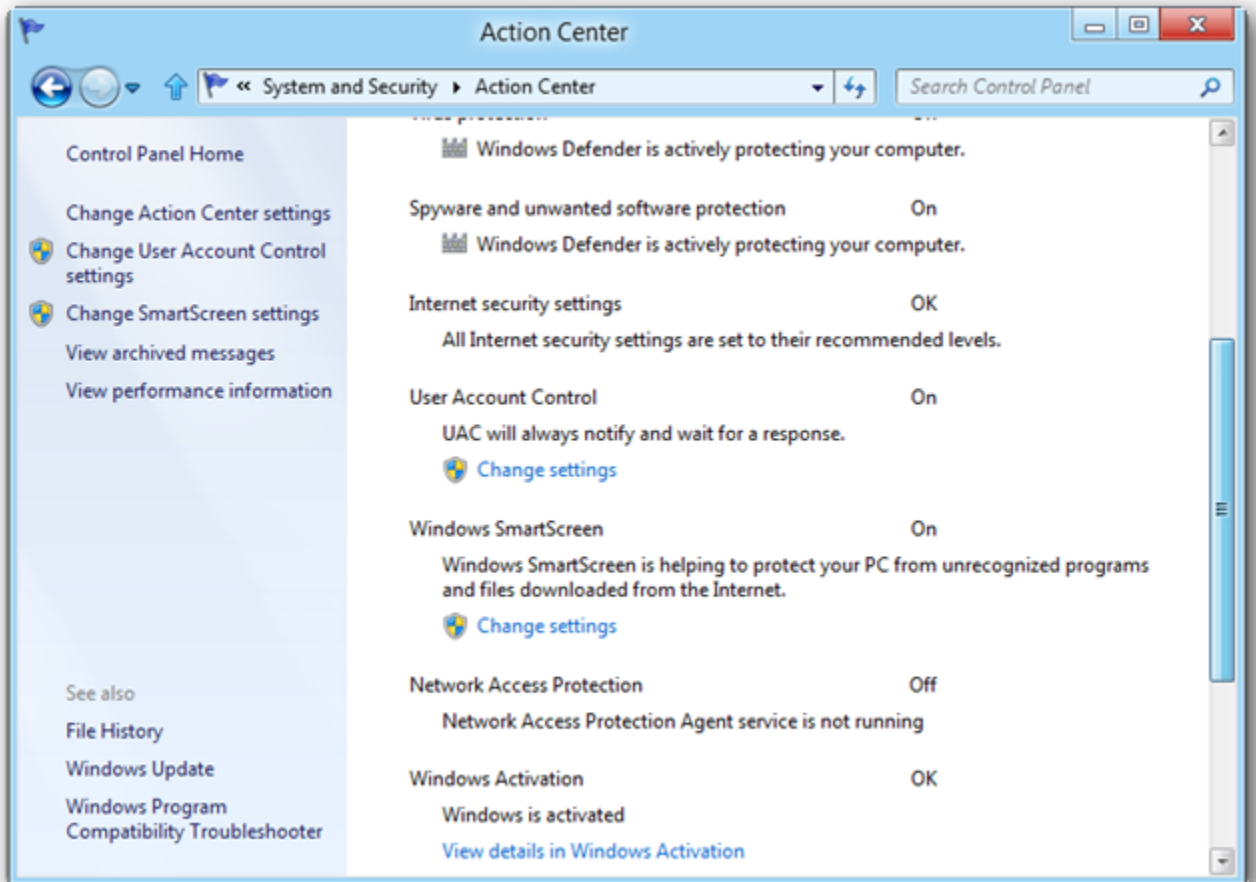
1. Open up the classic control panel, and select the System and Security link



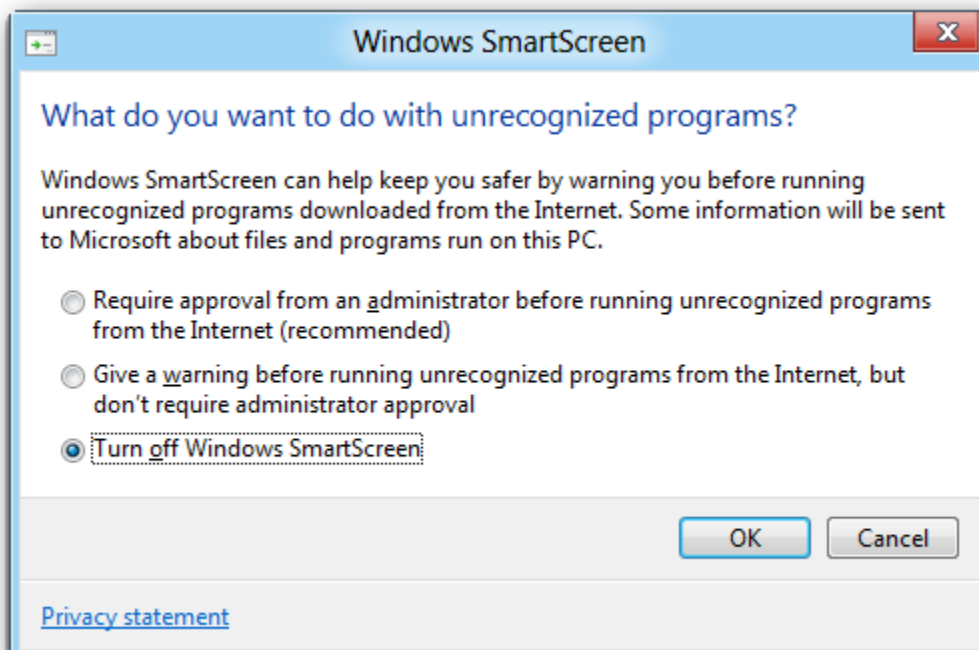
2. Now select the Action Center option.



- Once you are in the Action Center expand the security list, and scroll down looking for the Windows SmartScreen option. Once you have found it click the change settings link.



- You will most likely be prompted by UAC to enter your password, now you can totally turn off the SmartScreen Filter. Change the radio button from the default to the bottom option.



مایکروسافت اخیراً یک فیلتر SmartScreen برای نرم افزارهای ویندوز ۸ معرفی کرده است. این فیلتر مشابه فیلتر Internet Explorer SmartScreen عمل می کند و کاربران را از عوامل مخربی که در سراسر اینترنت از طریق هشدارهای وب سایت های فیشینگ پخش شده است محافظت می کند. متأسفانه این فیلتر جدید SmartScreen کمی هم آزاردهنده است زیرا اغلب حتی در مقابل برنامه های کاربردی امن نیز باعث ایجاد امنیت های ناخواسته می گردد. بیشترین مسائل قابل توجه در خصوص نرم افزارهای دسته بندی نشده ای است که اغلب به اجرا نیاز دارند. آزدگی عمدتاً از نمایش متوالی فیلتر SmartScreen هنگام اجرای این برنامه ها ناشی می شود.