



## Top 10 Ways to Protect Against Web Threats

### 1 Block Access to Malware Servers

When desktop users request HTTP and HTTPS webpages from known malware servers, immediately block the request, saving bandwidth and scanning resources.

### 2 Restrict Mobile Code to Trusted Websites

While mobile code, such as scripts and active code, make the web much more interesting and richer for applications, it brings along with it automated ways for hackers to penetrate desktop computers and launch executable code or applications to execute embedded scripts in files.

### 3 Scan at the Web Gateway

Don't assume all of your desktops have up-to-date, running anti-virus program (AVP), or that visiting computers are well-managed. Easily control all incoming Web (HTTP, HTTPS, and FTP) traffic by centrally scanning for malware as it attempts to enter your network, not when it's already entered the desktop.

### 4 Use a Different Vendor for Desktop and Web Gateway Scanning

Modern attacks are tested against popular AVP's before release. Increase your chances of stopping the threat with diversity in your malware scanning.

### 5 Update Desktop and Server Patches Regularly

Most attacks and threats spread by taking advantage of unpatched applications and systems. Cut your risks by protecting your computers from known vulnerabilities.

### 6 Keep Desktop AVP's Installed and Up-To-Date

Since the days of boot sector viruses, it has been standard procedure to have an AVP running to inspect incoming files, scan memory, and scan existing files. No computer running Windows should be without an up-to-date AVP. If the 'bad' stuff has alluded all other network protections, this is the last defense. Also, great protection for any malware transferred from non-network methods, like CD's or USB flash drives.

### 7 Only Visit HTTPS Websites that Pass all Browser Checks

Most users don't understand the significance of the three SSL browser checks, or fail to understand that they should not visit sites which don't pass all three. The SSL checks are Expired Certificate; Untrusted Issuer; and Hostname Mismatch between the certificate and the requested URL.

### 8 Only Download Executable Programs from Trusted Websites

Social Engineering is alive and well on the Internet! A very effective method to distributing malware is to pair it up with a seemingly useful program. When executed, the malware is free to do as it pleases. This type of attack is also known as a Trojan Horse attack.

### 9 Don't Visit Websites with an IP address as the Server

Recent attacks make more use of compromised home computers with simple web servers installed. Victims are usually directed to the new home computer servers by URL with IP address, not DNS hostname. Legitimate websites will use hostnames in URLs.



### ⓘ Carefully type in website URLs to avoid Fat Fingering

Users never intend to visit a malware site, but it can happen innocently enough. Mis-typing popular websites usually lands users at squatting sites waiting for unsuspecting users. If your browser isn't fully patched, you could easily pick up malware with a drive-by download.

## Secure Web Gateway Requirements Stop Malware

You can thwart many web attacks with protections at the Web Gateway. Make sure your Secure Web Gateway provides the following:

- > URL Filtering to stop malware downloads, phone-home transactions, and fat-fingering
- > Malware Scanning for Virus, Spyware, Malicious Mobile Code (MMC), Unwanted Software, Trojans, Botnet, Worms, etc.
- > Protection for HTTPS web traffic, not just HTTP and FTP
- > Checks the payload for the true file type, instead of trusting the file extension or other file modifications done specifically to elude detection
- > Enforcement of SSL browser checks
- > Block access to URLs with IP addresses instead of hostnames
- > Only allow executable and mobile code from trusted websites
- > Allow selective access to a gray-list of executables by User (such as IT administrators)
- > Regular, multi-day, automatic updates from a respected Anti-Malware provider
- > Scalable scanning optimized for webtraffic, since latency is very noticeable to users
  - Avoids rescanning repeated traffic in between virus updates for cacheable and non-cacheable objects
  - Large web, atypical downloads (> 200kb), don't impair regular web traffic scanning performance
  - Doesn't waste resources maintaining large numbers of active TCP connections (<150 active)
- > Enforces Safe Searching for popular web search engines, to minimize redirection to malicious software servers
- > Offers choice of scanning engines, to better complement your desktop scanning
- > Doesn't trust the IP address supplied by users for webpage requests
- > Can recognize infinite streams, such as Internet radio broadcasts, that never end and hence never be scanned