

## **TopSec Technology - Secure Internet Service**

### **Enhance productivity with Secure Internet Services**

Secure Internet enables organisations to improve employee productivity by managing Web site access considered to be non-business related and especially time-consuming.

The policies and categories available for Secure Internet, as attached, provide enhanced internet filtering and a higher level of protection from Web-based threats. This allows you to set and enforce policies with respect to emerging threats, such as bandwidth-intensive streaming media, malicious mobile code (MMC), Phishing sites, and Spyware, that pose productivity, resource, and security risks to your organisation.

### **Secure Internet Services help manage employee access to the following categories:**

- **Advertisements** - Sites that provide advertising graphics or other advert content files.
- **Message boards & clubs** - Sites for online personal and business clubs, discussion groups, message boards, and list servers; includes 'blogs' and 'mail magazines.'
- **Freeware / software downloads** - Sites whose primary function is to provide freeware and software downloads.
- **Online brokerage & trading** - Sites that support active trading of securities and management of investments
- **Instant messaging** - Sites that enable instant messaging.
- **Pay-to-surf** - Sites that pay users to view web sites, advertisements, or email.
- **Streaming media** - Sites that primarily provide streaming media content, such as movie trailers.
- **Internet radio & TV** - Sites whose primary purpose is to provide radio or TV programming on the Internet.
- **Personal network storage** - Sites that store personal files on internet servers for backup or exchange.
- **Internet telephony** - Sites that enable users to make telephone calls via the internet or to obtain information or software for that purpose.
- **Peer-to-peer file sharing** - Sites that provide client software to enable peer-to-peer file sharing and transfer.

### **Manage network bandwidth with Top Sec Secure Internet Service**

Bandwidth is a limited resource in any network. Such internet activities as accessing streaming media sites, loading personal files or photos to internet storage sites, or downloading copyrighted music and video consume bandwidth needed for business-critical applications and potentially pose legal liability and confidentiality issues as well.

Our Secure Internet Service is a powerful bandwidth management tool.

**Malicious mobile code** is software designed to move from computer to computer and network to network and intentionally cause harm or modify computer systems. MMC may reside on seemingly innocent sites that employees visit to shop or plan travel, and its presence is often undetected. MMC can be delivered via Web borne viruses, Trojan horses, worms, script attacks, and rogue internet code, such as the Nimda worm.



Using proprietary Web site mining techniques, Secure Internet scans its URL database of millions of sites for malicious code, including ActiveX controls, Visual Basic script, JavaScript, and Java Applets. Then, using sophisticated algorithms, Secure Internet categorizes those sites infected with MMC and blocks employee access to them.

## **Block access to Spyware, Phishing sites and MMC with a Secure Internet Service**

Add an additional layer of security to your network by preventing employees from unknowingly accessing Phishing sites, sites that are infected with MMC, and sites that distribute Spyware. Should Spyware already reside on your corporate desktops, Secure Internet stops the transmission of sensitive information to host Spyware servers.

**Spyware** is software installed on a computer, without the user's knowledge, that gathers information and relays it to advertisers or other interested parties. Spyware can collect and transmit information such as keystrokes, Web surfing habits, passwords, email addresses, and more. Spyware wastes system resources and bandwidth as it tracks and transmits information. More seriously, Spyware can also pose grave security, confidentiality, and compliance risks.

Secure Internet stops Spyware first by blocking access to sites that distribute Spyware, then by preventing the transmission of employee and network information to host sites. Through proprietary processes and the WebCatcher™ feature – by which uncategorised web sites from customers are sent back to Secure Internet for review—Secure Internet is able to identify Spyware servers and block backchannel communications via port 80 connections.

**Phishing** and other fraud sites counterfeit legitimate business sites for the purpose of eliciting financial or other private information from users. Secure Internet helps address Phishing by identifying URLs and blocking employee access to those sites.

### **Secure Internet help manage employee access to the following categories:**

- **Spyware** - Sites or pages that download software that, without the user's knowledge, generates http traffic (other than simple user identification and validation).
- **Malicious Web sites** - Sites that contain code that may intentionally modify end-user systems without their consent and cause harm.
- **Phishing and other frauds** - Sites that counterfeit legitimate business sites for the purpose of eliciting financial or other private information from users.

### **Set Up**

Like our Blockmail service, Secure Internet runs over broadband with minor changes on your web browser.

Topsec Technology Ltd.  
Unit 1, Block C,  
The Exchange,  
Calmount Park,  
Ballymount, Dublin 12

T: 01 466 0686

E: nmackey@topsectechnology.com