

# Computer Security and Web Filtering

For Small and Medium Sized Businesses and Organizations



Michael J Sancin  
Web Marketing Manager  
CyberPatrol  
July 2010

---

## Table of Contents

### Contents

<b>Introduction</b> .....	<b>3</b>
<b>Emerging Web Based Threats Facing Small Businesses and Organizations</b> .....	<b>4</b>
Malware.....	4
Legal Liability .....	5
Productivity .....	6
<b>Implementing Web Filtering Effectively</b> .....	<b>7</b>
CyberPatrol, Designed for Small to Medium Businesses and Organizations.....	7
CyberPatrol Online Protection PRO .....	7
CyberPatrol SiteSURV Web Filtering.....	7
<b>Conclusion</b> .....	<b>8</b>

## **Introduction**

The Internet has much to offer small businesses. Quick and easy access to information and contacts have made doing business easier than ever. Unfortunately, it has also unleashed a new set of issues to confront; loss of productivity, downloading illegal content, exposure to pornographic material, and new kinds of malware and viruses.

These problems leave companies vulnerable to loss of profits, legal liability, and devastating malware attacks. Managing these threats can seem overwhelming. More and more computers are being infected by bad or harmful web sites. Productivity issues and accessing inappropriate or illegal content at work can lead to a Human Resources nightmare. Employees working remotely with company laptops are exposed through insecure wi-fi networks. And because they are remote, it is difficult to monitor behavior and control online activity. All this exposes your business or organization to problems that didn't exist just a few years ago.

Dealing with these issues can cost money and take up valuable time. Many of the products available on the market today were designed for enterprise accounts and can be expensive and complex to use. Basic web filtering offers an easy and affordable solution that allows businesses to proactively address these issues. Not only does it help keep employees on task and eliminate the temptation of random surfing, most importantly it provides a proactive security solution.

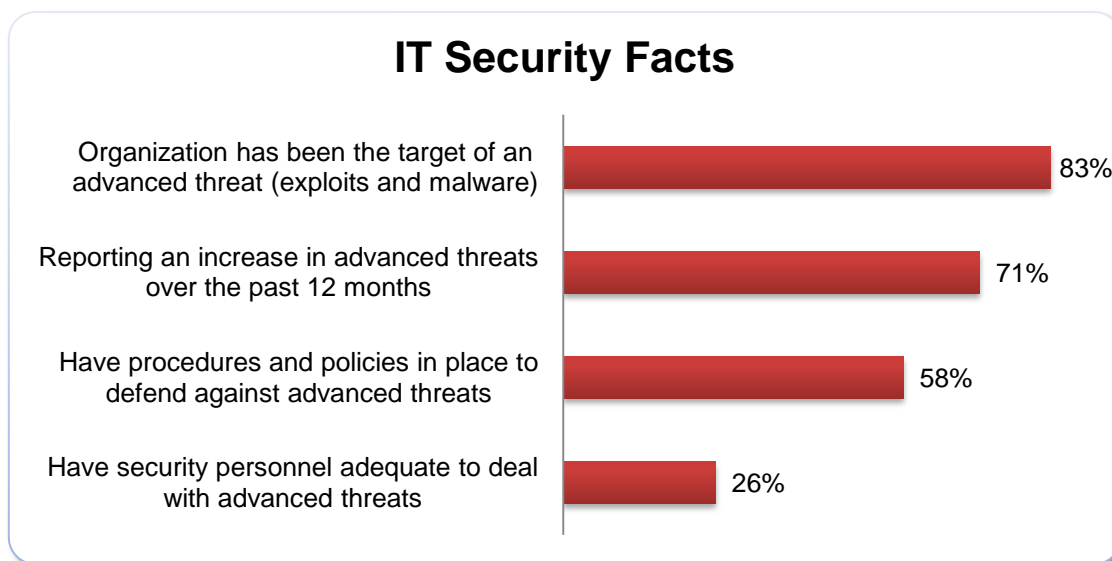
## Emerging Web Based Threats Facing Small Businesses and Organizations

Today's online business environment presents companies with three primary web based threats; data corruption and loss from malware, legal liabilities, and a decrease in productivity. What makes these threats particularly significant is that they can have a major impact on the success of a business and they are all a byproduct of the simple act of browsing the web.

### Malware

Malware, spyware, and computer viruses are some of the most challenging concerns of businesses and organizations. Malware in particular is on the rise and can put companies at serious risk. It can happen through innocent browsing. The simple act of clicking on a link can load up a computer with devastating malicious code.

Most companies have anti-virus software installed to help catch or contain most of these threats after they have already been launched. But in a recent study released by Ponemon Institute, IT professionals stated that *"advanced exploits and malware have successfully evaded their anti-virus (AV) and intrusion detection system technologies."* On top of that, 46 percent of the respondents reported that it can take over a month to even detect the threat<sup>1</sup>. If these threats are not stopped or fixed with protection software, dealing with attacks can put a significant strain on a company's resources. Many small businesses don't have an IT professional on staff or under contract and when systems go down, they have to call "the guy". Unfortunately when these types of attacks occur, calling someone in to troubleshoot the problem can take hours or even days.



Source: PC World

Taking a proactive approach and stopping attacks before they happen is increasingly becoming a requirement in a company's security strategy. By implementing web filtering, many of these attacks are stopped before they ever happen. By blocking the most notorious offenders of malware, porn, hacking sites etc., an effective web filtering solution reduces the amount of attacks on your network and your individual computers. That's particularly important when employees are on the road with laptops and more vulnerable to threats.

Some sites, like porn sites, are notorious for delivering malicious code. However, not just 'bad' web sites are infected. One of the most popular and frequently visited sites, Facebook, is increasingly the target and delivery method for Malware. In one event, clicking on a link leads the user to a picture of actress Jessica Alba containing a clickjacking link.<sup>2</sup> One of the more serious attacks that averted many Facebook users was the "Koobface" virus. Users got

<sup>1</sup> PC World June 30, 2010

[http://www.pcworld.com/businesscenter/article/200224/study\\_advanced\\_threats\\_a\\_growing\\_problem\\_for\\_security.html](http://www.pcworld.com/businesscenter/article/200224/study_advanced_threats_a_growing_problem_for_security.html)

<sup>2</sup> Facebook Hit With Clickjacking Attack, by Mathew J. Schwartz, InformationWeek June 15, 2010

messages from their friends inviting them to view videos, but were prompted to update their flash player first. Clicking “update” installed malicious executable code that turned their machines into zombies and it’s a pain to undo the damage.

Using effective web filtering software, IT professionals can manage and maintain the kinds of sites employees can access when using business computers. More important, using software, like CyberPatrol Online Protection, gives that same capability to business owners and managers. Because it’s easy to use and manage, you can select the level of protection for each employee without dealing with the complexity that is typical of expensive large enterprise solutions.

Blocking access to certain sites not only helps the random innocent click to the “wrong” site but can also lock down the repeat offenders. Some employees seem to get attacked more than others and may be a little looser with their personal restraint.

### Legal Liability

There are certain places on the web that no employee has any business going to for any reason. Adult and Illegal download sites are two perfect examples. Not only are these sites inappropriate for the work environment, they also present companies and organizations with potential legal issues.

Pornography in the workplace is an uncomfortable topic for most businesses. Company policies may already be in place to let employees know that this type of behavior is not tolerated. Unfortunately the internet is full of adult sites and inevitably many employees will access porn on company time—either on purpose or by mistake. Adult content is not always the intended result of a clicked link or Google search. It can pop up during even a seemingly simple search. Search engines like Google have a safe search feature that when turned on blocks most pornographic images. When turned off, results can be quite graphic.

Try it for yourself. Go to Google and turn safe search off. Then type the word “girls” and click on “images”. See what you get. If you are offended by pornographic images, don’t do this test. If this happens during a meeting or presentation it can be both offensive and embarrassing and possibly lead to complaints of sexual harassment.

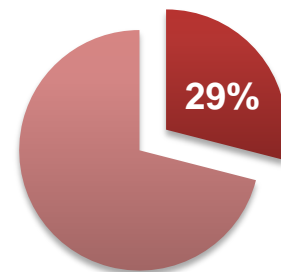
While most employers would like to believe that no one would deliberately access adult content during company time, some statistics show that it is far too common. In April of 2010, it was reported that SEC staffers watched porn as the economy crashed.<sup>3</sup>

In March 2010, the Nielson Company reports that more than 21 million Americans accessed adult websites on work computers. That’s 29% of working adults.<sup>4</sup> Viewing and sharing of this type of material puts companies in a difficult situation. This type of simple exposure to porn is subject to sexual harassment laws. The United States Court of Appeals upheld the right of an employee to sue stating “the mere presence of pornography in a workplace can alter the 'status' of women therein”.<sup>5</sup>

Not only is any porn in the workplace an HR nightmare but resulting law suits can be disastrous. Yet viewing online porn is easily prevented with web filtering software.

It’s not just adult content that causes problems. Content that is downloaded illegally, such as music and movies, leaves a company or organization open to prosecution. This is not a

**Accessing adult sites on work computers**



Source: CBS News

<sup>3</sup> CBS News, WASHINGTON, April 23, 2010, SEC Staffers Watched Porn as Economy Crashed, <http://www.cbsnews.com/stories/2010/04/22/business/main6423548.shtml?tag=contentMain;contentBody>

<sup>4</sup> CBS News, April 23, 2010 4:29 PM, 29% Accessed Porn on Work Computers Last Month [http://www.cbsnews.com/8301-503544\\_162-20003319-503544.html](http://www.cbsnews.com/8301-503544_162-20003319-503544.html)

<sup>5</sup> Ice Miller LLP, US Court of Appeals ruling. <http://www.icemiller.com/enewsletter/InformedEmployerBriefing/PornSexualDiscriminationinWorkPlace.htm>

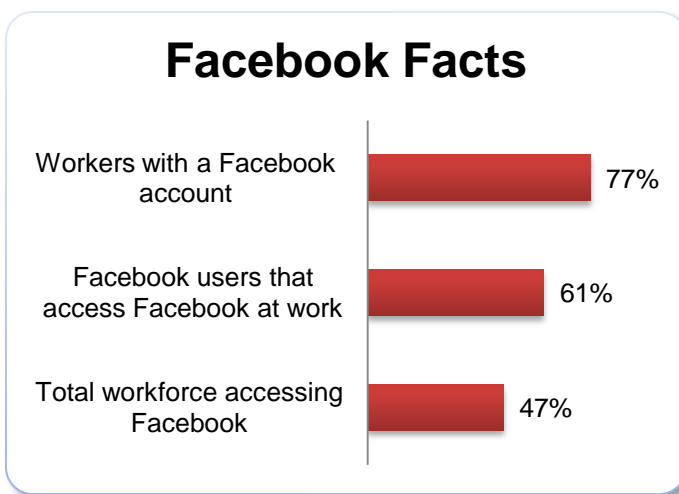
matter of improper discretion, it is breaking the law. And if it is done on an organization's PC's, they can be held liable. Not only does this activity expose business to legal action it also increases bandwidth usage and associated cost.

*"Piracy is theft. Clean and simple. It's smash and grab. It ain't no different than smashing a window at Tiffany's."*

*--Joe Biden, U.S. vice president*

## Productivity

When it comes to productivity and the Internet there is a lot of conflicting data. Just how big is the problem? While there is some evidence showing that productivity is unaffected or increased with access to Facebook and other social networking sites, most reports show that productivity is in fact hampered.



Source: Nucleus Research

In a July 2009 study, Nucleus Research, an IT research company, found that nearly half of office employees access Facebook during work. The study found that employees effectively lose an average of 1.5 percent of total office productivity when employees can access Facebook during the work day.<sup>6</sup>

The survey of 237 employees also showed that 77% of workers who have a Facebook account use it during work hours.

Social networking sites blur the lines between personal and professional use. Odds are someone in the company will need access to Facebook for legitimate business use but that does not mean everyone needs to be updating their status throughout the day. Access to Facebook can and should be limited to those who use it as a business tool.

As mentioned earlier not only can access to Facebook, MySpace and other social networking sites reduce employee focus and productivity, it can also deliver malicious code.

<sup>6</sup> Nucleus Research Report, Facebook: measuring the Cost to Business of Social Networking, July 2009.  
[http://nucleusresearch.com/index.php?option=com\\_remository&Itemid=65&func=download&id=928&chk=e535d9090525de0fa8f7dd627dd7bb14&no\\_html=1](http://nucleusresearch.com/index.php?option=com_remository&Itemid=65&func=download&id=928&chk=e535d9090525de0fa8f7dd627dd7bb14&no_html=1)

## Implementing Web Filtering Effectively

An effective web filtering solution for small businesses contains a few simple ingredients; low cost, easy implementation and management and customizable controls. With this in mind, an organization should look for a simpler web filtering solution than those used by larger enterprise. One designed specifically for SMBs that cost hundreds rather than thousands of dollars yet still does an effective job of blocking and monitoring web activity.

### CyberPatrol, Designed for Small to Medium Businesses and Organizations

CyberPatrol offers two types of filtering products to meet these needs, CyberPatrol Online Protection Pro and CyberPatrol SiteSURV. CyberPatrol Online Protection Pro is a web based solution that monitors & filters each PC individually and is managed through one online interface. CyberPatrol SiteSURV filters at the Internet access point with virtually no software to install on users PC's and works with both PC and MAC platforms.

No matter which solution works best in your environment both of these products were designed for ease of use, little maintenance and to be very cost effective. Both products provide the same robust filtering capabilities.

### CyberPatrol Online Protection PRO

CyberPatrol Online Protection Pro offers small to medium sized businesses all the control they need in a solution that is easy and flexible and at an affordable cost. CyberPatrol Online Protection Pro was built to help small businesses get a handle on web based threats and take back control over how their resources are used. The last thing a business owner needs is another job or task to manage. That's why CyberPatrol Online Protection Pro is designed to be straight forward and as easy to implement as possible.

This software is designed for businesses that require a web filtering product to manage individual PC's and implement different user rights. Since CyberPatrol Online Protection Pro is an online service, its web based interface makes it easy to manage multiple PC's from a single location. Custom filtering profiles can be created for various groups of employees such as managers, executives, etc., or a specific single user could have custom settings applied. Many of the features, such as safe search, are as simple to deploy as turning the feature off or on.

#### CyberPatrol Online Protection PRO has several key features:

- **Web Filtering** - 44 website categories plus custom white and blacklist
- **Custom Profiles** - select default profiles or create custom profiles based on individual needs
- **Safe Search** - enforce safe search on popular search engines
- **Time Management** - easily select time limits by users
- **Instant Alerts** - monitor for sexually explicit or violent conversations and receive instant email alerts
- **Reports** - reports provide a snapshot of online activity

### CyberPatrol SiteSURV Web Filtering

CyberPatrol SiteSURV offers businesses a broad comprehensive approach that filters at the internet access point. It is a managed service that requires virtually no software to be installed on individual PCs and quickly enhances security, reduces risk and helps organizations manage online activity.

This solution works best for companies that have a mix of operating systems (PC and MAC), and/or want the fastest implementation. Since this solution blocks at the access point, all users are given the same amount of access including outside laptops accessing the companies Wi-Fi.

#### SiteSURV features include the following:

- **Control Panel** - manage from any PC with Internet access
- **Easy to implement** - no user application software or hardware required
- **Multiple Profiles** - can change to different profiles at any time
- **Create your own block or allow list** - easily upload your custom lists
- **Monitor and Graph** - number of sites accessed and blocked
- **Reports** - graph 30 days of activity easily saved in CSV format

## **Conclusion**

As web based threats continue to present new and increased problems for small businesses, it's easy to feel helpless. Too often companies think that they can only react to these issues as they happen. Web filtering offers a proactive solution that can help to mitigate these problems and prevent costly and embarrassing catastrophes. By monitoring and controlling what is accessed online, companies can better control cost and keep distractions to a minimum. Being proactive when it comes to security can save time and money, allowing business owners to focus on growing a successful organization.

With CyberPatrol, implementing effective web filtering doesn't have to be complicated or costly. Whether the concern is malware, employees accessing inappropriate content or just spending too much company time surfing the web, CyberPatrol has the solution.