

Reporting All The Bits

February 2008

What's
Inside

**The top three
deadly sins that
are committed
on the internet.
Turn to Page 3.**

**Did you Know?
Some interesting
bits on Valentines.
Story on Page 2**



**Special Offer
On Page 4**

Looking for Love in all the wrong places!

In 2006 a report was released on Internet usage within 400 US government and public sector organizations. The numbers are reviewed and compared every three years. In the survey they found a 16 percent increase in cases of staff accessing pornography or other inappropriate material. This now accounts for almost half (47 percent) of all incidents of computer misuses and fraud in the workplace.



Thompson, who specializes in the area of sexual health, expressed concern for what the live action and more explicit material will do for boys' expectations.

Add that to the results of an earlier survey that found that one in five (20%) men have admitted to viewing pornography at work and that 13% of women have also admitted to viewing pornography at work. Those are the ones that admit to it!

On February 22, 2007 University of Alberta researcher Sonja Thompson released the summary of her survey results. More than one third of 13 year old Alberta boys view Internet porn "too many times to count". Nor were those encounters accidental pop-ups on the way to do their homework or converse with their friends on facebook. Three quarters of the boys and almost half of the girls in her survey said they deliberately logged

on to sexually explicit material.

The issue for kids and porn is there is a whole sub culture out there as well most kids are more computer and technology savvy than their parents. If parents even think of putting in a basic porn blocker at home most kids can figure a way to get around it.

There is the same abuse, but a different issue, at the school or workplace. At work the expectation is that we are employed to provide services on our employers' behalf. Few of us are employed to do personal banking, shopping or view pornography during business hours. There is a pure economic cost of our time. Secondly there is correlation to the amount of gratuitous web surfing we do and the amount of trash we attract on our PCs. With surfing we collect all sorts of trash—some of it is harmful. Even if there is a firewall and up to date virus software is used our surfing invites in other "undesirable" software.

Continued on Page 2...

Typically this is classed as spyware or malware. It is more difficult to control. If there is no content filter then the spyware will infest your PC. The most noticeable impact is that your PC will run slower.

WHAT CAN WE DO?

The first thing we can do is to face up to the fact that potentially unacceptable surfing could occur at your work, school or home. At work or school you would set an "Acceptable Usage Policy" that spells out what is acceptable usage of technology in your environment and potentially the consequences. Personally I am not in favour of a one strike your out policy. There is a lot of garbage out there and it is easy to trip along into the wrong path. Habitual use of the organization's resources for clearly unacceptable uses may have consequences and they should be spelled out in advance.

The second thing we can do is to employ technology to monitor and block potentially unacceptable or hazardous sites. The NetSentron is a firewall with an intelligent content filter as well as traffic and bandwidth monitoring. We can report and block all regular web surfing activity. It has also been configured to report and block on peer to peer programs and chat at the application level. Implementing the NetSentron has reduced the time and cost of technicians from the tedious task of spyware removal so they can be redeployed to more strategic tasks.



Did you know?

- A single perfect red rose framed with baby's breath is named by some florists as a "signature rose," and is the preferred choice for most for giving on Valentine's Day, anniversaries and birthdays.
- The red rose was the favorite flower of Venus, the Roman goddess of love. The color red stands for strong romantic feelings making the red rose the flower of love.
- Every year around 1 billion Valentine Cards are sent across. After Christmas it's a single largest seasonal card-sending occasion.
- Teachers receive the most Valentines Day Cards, followed by children, mothers, wives, and then, sweethearts. Children between ages 6 to 10 exchange more than 650 million Valentine's cards with teachers, classmates, and family members.
- Cupid is a symbol of Valentine's Day. Cupid was associated with Valentine's Day because he was the son of Venus, the Roman god of love and beauty. Cupid often appears on Valentine cards and gift tokens holding a bow and arrows as he is believed to use magical arrows to arouse feelings of love.
- Verona, the Italian city where Shakespeare's play lovers Romeo and Juliet lived, receives about 1,000 letters every year sent to Juliet on Valentine's Day.
- In the Middle Ages young men and women drew the names from a bowl to see who would be their Valentine. They would wear this name pinned on their sleeves for one week. This was done so that it becomes easy for other people to know your true feelings. This was known as "to wear your heart on your sleeve".
- On February 14th wooden love spoons were carved and given as gifts on Valentine's Day in Wales. Hearts, keys and keyholes were favorite Valentine decorations on the wooden spoons. This Valentine decoration meant, "You unlock my heart!"
- The most beautiful and incredible gift of love is the monument Taj Mahal in India. Built by Mughal Emperor Shahjahan as a memorial to his wife it stands as the emblem of the eternal love story. Work on the Taj Mahal began in 1634 and continued for almost 22 years and required the labor of 20,000 workers from all over India and Central Asia.
- In America, the pilgrims used to send confections, such as sugar wafers, marzipan, sweetmeats and sugar plums, to their affianced. Lot of value was placed on these gifts because they included what was then a rare product, sugar. After the late 1800's, beet sugar became widely used and more available, and sweet gifts continued to be cherished and enjoyed.
- Amongst the earliest Valentine's Day gifts were candies.

Three of the Deadly Internet “sins”

1. No Virus Protection

Most people know that they should have an anti virus program. An anti virus program can be running at the “gate” or on the computer. Most viruses come as an attachment in email. The advantage of having an anti virus program “At the gate” is that the mail never gets to your desktop. What is meant by “at the gate” is the anti virus program runs on an email server or internet gateway (firewall) server and screens the email and quarantines the email before it ever has a chance to get to your desktop. Having anti virus “at the gate” is good; however, it is inadequate. It can be like the Maginot Line. All of the defenses were lined up against a particular ground attack and the German’s just went around the line. In the same way viruses can be spread via a diskette, CD-rom, or another computer on the network. So an anti virus program should be running on your PC and every other computer on the network.

An anti virus program is only as good the company behind it. It is pointless to have an anti virus program if the pattern files are not kept up to date. The anti virus program will not prevent the damage done from a brand new virus, but it will detect, notify and quarantine any known virus. The catalogue of known viruses is kept in the “pattern files” that are built for each anti virus program. If the company is not up to date on the latest viruses or if your computer does not get the latest pattern files it is about as effective as having no anti virus protection at all.

The cost of not having virus program can be steep. One person became our client when her program detected a virus and she needed to get her accounting done. Once the virus had been removed, the technician updated her anti-virus program only to find six more viruses. Four hours later and late into the night, the computer had finally been re-built, programs reloaded and files restored.

2. No Appropriate Firewall

A firewall can either be a device or software that puts a barrier between you and the network. In our case the network is the internet however, a firewall can also be used internally to stop other people in the office from “hacking” into your computer. The first “sin” is not to have a firewall at all. If you are on a high-speed internet connection you have a permanent connection to the internet and a door way to the internet. A firewall is one way to close and lock the doors allowing only the traffic that you want to come in or go out of the gate to internet.

Rather than using a router or other network devices, those on dial-up may choose to use a basic firewall software package. The longer you are on the internet the greater the chance you will be found! Once you are found without a firewall it would take little time or effort to compromise your system or other systems through your PC.

An example of a compromise would be a salesman gaining access to the corporate network in the hotel room at night using a VPN (Virtual Private Network). The VPN is secure; however, the salesman has neglected to run a firewall. While the salesperson is busy keying in orders and checking the status of his accounts his PC has been detected on the internet. The PC is of very little interest; however, the fact that the PC is currently attached to the corporate network is of interest to the hacker. The hacker now has access to the corporate crown jewels. In ten minutes the network has been mapped and a copy of the customer file has been transferred to the hacker’s PC. All of this occurred without the knowledge of the salesperson. All he noticed was that the system was slow at times.

Continued on the back page ...



#404-17768 65A Avenue,
Surrey, BC,
Canada, V3S 5N4
www.kdi.ca

Phone: 604-574-7225
Fax: 604-574-7256

Managing all the Bits

Services We Offer:

- General Network Repair and Troubleshooting
- Network Design & Implementation
- Disaster Recovery
- Virus Protection & Removal
- Network Security
- E-mail & Internet Solutions
- Wireless Networking
- Spam Filtering
- Storage Solutions
- Web Design/Hosting
- IBM iSeries Software Development/Management

3. Unnecessary Services Are Turned on or Not Blocked

Blocking or turning off unnecessary services, is not just an issue for the internet, it is also an issue for your PC on any network. An example of this sin is having turned on the share on the hard drive of your PC. This gives anyone on the network the ability to read or even write to your hard drive. If you want to share files with your colleagues at work perhaps a shared drive mapped to the server with all of the other relevant documents can be stored there. If you intend on sharing your drive then when you do shut down your PC your colleagues will get disconnected. It would be better to put these items on the company server.

The security issue of leaving FTP or shared drives on is best illustrated when you are on a cable internet connection. Perform a Network Neighborhood and then you can see who else is connected in an insecure manner to the cable service.

For corporate networks, ensure that only the services you want made available to the internet are turned on. While your server can host web pages don't turn on the HTTP server unless you intend to host web pages and want to deal with the security patches and monitoring that is required to run the services securely on your server. This applies for all other services available on your network.

To learn more about the "Deadly Sins" feel free to contact KDI.

Call During February and March for a FREE Network Security Audit!

At no cost or obligation, we will come on site and install a NetSentron demo server to expose lurking problems caused by inappropriate employee usage of the Internet and e-mail, spam, or inadequate virus protection.

Within one week, we will pinpoint where your vulnerabilities are and show you what you can do to protect your company. We will also be able to detect how much time your employees are spending on non-business related web activities, and how it is affecting your bottom line profitability. To do this type of audit yourself would cost over \$4,000 in hardware and software.

By letting us perform the audit for free, you get a risk free way of assessing your current situation to determine whether or not you even have a problem, and whether or not you need to take further action.

Request Your Free Network Security Audit by calling: 604-574-7225

