Forced upon Us

Departing somewhat from the main topic of this article, we should be aware that no matter how good and moral we are, and how responsibly we use the internet, and how much we trust ourselves, there is another danger inherent in browsing the web: inappropriate content that is *foisted upon us*.

For the most part, pop-ups aren't a problem anymore; most browsers automatically block them. But there are countless websites with important content that are ruined by immodest advertisements. Not only that, but an innocent entry into a search engine can yield undreamed-of results. Some links are deceptive. Image searches for mundane words can return unsuitable results.

Facebook is cited in one out of every five divorces in the United States, according to the Loyola University Health System. (One out of three in the UK, according to a Divorce-Online survey.)

This entire effect is exacerbated when it comes to children using the internet. Children can be exposed to the worst sights and influences purely by accident. They don't even know how to distinguish the warning signs of a bad link. And what they see can have very damaging effects on their undeveloped psyches.[23]

[23] For specifics, see http://tinyurl.com/bqaeeon

Internet users by country

A 2007 study by the University of New Hampshire found that 28% of children aged 10–17 had been inadvertently exposed to inappropriate content that they did not seek out.[24] A different study gives a figure of 70%![25] These exposures occurred through websites (misleading links, misspelling web addresses, etc.), chat with friends, file-sharing programs, and online games.

Illusion of Knowledge

One of the pitfalls of internet use is the generally low quality of huge amounts of information available there. The intrepid Googler is often hard-pressed to distinguish between reliable and unreliable sources in his research, and many are simply too lazy to verify the truth. What this leads to is the ability for a person to feel well informed on a topic while really being completely misled.

Nowhere is this more perfectly demonstrated than by everyone's favorite Source of All Information About Anything That Ever Existed: Wikipedia.

Wikipedia lures us with its professional-looking design and its 3.95 million articles (in English alone!), many of them exceedingly long, on any topic imaginable. Here you can get a quick introduction and overview to almost any topic you want, or find out biographical information about almost any person who is even moderately well known. It's an increasingly popular destination on the web: the English site had 6.75 billion views in March of 2012 (that's almost one for every person on the planet, over the course of just one month).[26]

This is boosted immensely by search engine references. For example, over half of the 1,000 most popular Google searches will yield a Wikipedia entry as one of the first few results. "Wikipedia is one of the most powerful sites on the web in terms of shaping public perception. Because Google favors it so heavily, the entries on Wikipedia have become supremely important and relevant."[27]

At least Wikipedia is fairly straightforward about the nature of the project: its English language main page states right at the top, "Welcome to Wikipedia, the free encyclopedia that anyone can edit."

In its essence, what this actually means is that anyone – anyone – can add any content they wish to this "encyclopedia." Pause for a brief moment to let the implications of this sink in. The people making entries and edits need claim no credentials, no expertise or special knowledge. On Wikipedia, the information entered by a

[24] http://www.foxnews.com/story/0,2933,250247,00.html (42% exposed x 66% unintentional = 28% of total)

[25] http://www.internetsafety101.org/Pornographystatistics.htm#_ftnref

[26] http://stats.wikimedia.org/EN/SummaryEN.htm

[27] Catone, J. "Just How Powerful Is Wikipedia?" http://www.sitepoint.com/just-how-powerful-is-wikipedia/. 4 Sep. 2008.

Statistics on Internet Dangers

- 47% percent of families said addiction to inappropriate websites is a problem in their home (Focus on the Family Poll, October 1, 2003).
- 86% of men are likely to click on inappropriate Internet sites if no one else will know about it (Journal of the American Psychological Association).
- 9 out of 10 children between the ages of 8 and 16 have viewed inappropriate stuff on the Internet, in most cases unintentionally (London School of Economics January).
- "Never before in the history of telecommunications media in the United States has so much indecent (and obscene) material been so easily accessible by so many minors in so many American homes with so few restrictions."—U.S. Department of Justice, Post Hearing Memorandum of Points and Authorities, at I, ACLU v. Reno, 929 F. Supp. 824.
- 38% of Facebook users in the last year were under the age of 13. (Consumer Reports, June 2011)
- 51% of parents either do not have or do not know if they have software on their computer to monitor their teenagers' online navigation and interactions. (National Center for Missing & Exploited Children and Cox Communications Parental Internet Monitoring Survey, May 23, 2005)
- A new website is launched every 2 seconds (covenanteyes.com).
- In 56% of divorce cases today, a major contributing factor is one spouse's inappropriate use of the Internet (covenanteyes.com).
- The past 10 years has seen a 162% increase in the amount of time that youth spend online (covenanteyes.com).
- Americans spend over 20 hours a week surfing the internet (covenanteyes.com).

high-schooler can seem as accurate and look as clean and professional as that of the most renowned professor. Someone looking for a quick fact he needs for his next business presentation or educational lecture could copy information posted on Wikipedia by a 12-year-old, unsuspectingly present it as fact, and be exposed to ridicule by experts who know better. Of course, it would be his own fault – but Wikipedia actually seems to try its best to convince us that it's a good source of information.

(Fortunately for the author of this article, and his readers, he consulted real sources for the facts!)

The intrepid Googler is often hard-pressed to distinguish between reliable and unreliable sources in his research, and many are simply too lazy to verify the truth. What this leads to is the ability for a person to feel well informed on a topic while really being completely misled.

Wikipedia enthusiasts claim that cases of "vandalism" and lies posted on the website will be quickly rooted out by the thousands of editors and millions of visitors the site receives constantly. But what about the case of John Seigenthaler, Sr., former editor of *The Tennessean* newspaper, who in 2005 discovered a false Wikipedia entry on himself that said he had been implicated in the assassination of John F. Kennedy? The lie had already been on the site for several months.[28]

There is much more to say about the Wikipedia phenomenon, but the constantly unfolding saga of Wikipedia is but one chapter in the debate on the reliability of online information.

The internet may greatly facilitate real learning and research, but it doesn't provide a shortcut to substitute for the process of learning in-depth. Additionally, it lacks the controls that are in place in many published works. Let the "information consumer" beware.

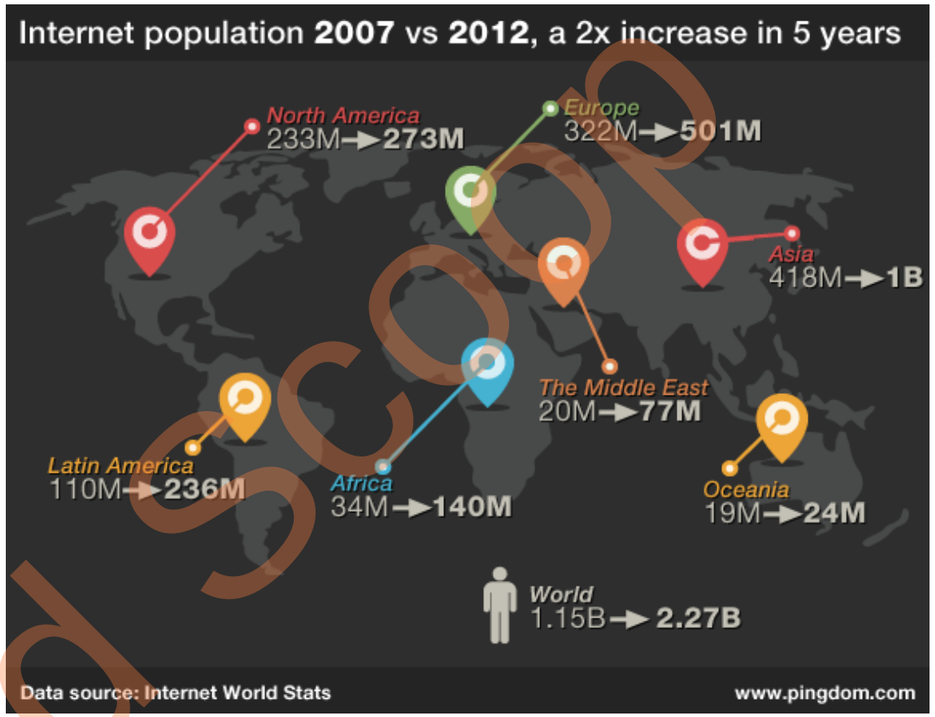
Addiction

Internet addiction has been a hotly debated topic for years. Whether it's called "problematic computer use" by those who doubt its status as a true addiction, or a full-fledged "Internet Addiction Disorder," this problem has become very prominent.

An article published in *The New York Times* in 2005 describes the addiction:

[S]pecialists estimate that 6 percent to 10 percent of the approximately 189 million Internet users in this country have a dependency that can be as destructive as alcoholism and drug addiction, and they are rushing to treat it. (...)

Skeptics argue that even obsessive Internet use does not exact the same toll on health or family life as conventionally recognized addictions. But, mental health professionals who support the diagnosis of Internet addiction say, a majority of obsessive users are online to further addictions to gambling or [immodest activities] or have become much more dependent on those vices because of their prevalence on the Internet.



Internet users doubled in only five years

But other users have a broader dependency and spend hours online each day, surfing the Web, trading stocks, instant messaging or blogging, and a fast-rising number are becoming addicted to Internet video games.[29]

The "most wired" country in the world, South Korea, is also the home of the most people affected with this problem. According to the "Big Think" website:

Fact: over half the world's population lives in cities. Fact: all developed cities like New York, Tokyo, Singapore and London, are in a race to become 'wired'. Fact: the most wired city in the world is Seoul, Korea with 97% broadband penetration. Ergo if we want to imagine life in a digital city, we should look for inspiration and lessons to Seoul. In fact, journalists, researchers and public officials have done exactly that. What they've discovered is a country which is one of the top investors in technology in the world, but whose population has become infested with 'internet addiction'. Does this mean our children and even us adults are vul-

[28] Seelye, K. "Snared in the Web of a Wikipedia Liar." *New York Times*. 4 Dec. 2005. Web.

[29] Kershaw, S. "Hooked on the Web: Help Is on the Way." *New York Times*. 1 Dec. 2005.

nerable to such a predicament over the next twenty years?[30]

Various factors have been blamed for this phenomenon, including the fact that culturally Koreans are driven to work very long hours for six days a week, leading to a high stress level and a need to find an "escape" in online games. There are also internet cafes on every corner and connection speeds are faster there than anywhere in the world, making everything so much more accessible. Still, the article goes on to warn that this is the reality all developed nations may be grappling with in 20 years from now.

"Instead of looking at Korea as the ultimate fate we will face as digital nations, we should think strategically to avoid falling into the same traps," the authors recommend.

The Far East is way ahead of the United States in coming to grips with this problem, even considering that the prevalence of Internet addiction is much higher there. Still, in America some symptoms of this growing problem are beginning to manifest themselves:

> *For $14,500—WiFi not included—an addict can spend 45 Internet-abstinent days at the Heavensfield Retreat Center [run by the reStart Internet Addiction Recovery Program] and, hopefully, emerge into the real world free of an obsession with Facebook, online gambling or even text messaging. (...)*
>
> *Meanwhile, in China, 400 private rehabilitation clinics and camps tend to some of the estimated 10 million teenage Web addicts, according to CNN. That's about 10 percent of the country's 100 million Internet users.*
>
> *"Both China and South Korea have designated Internet addiction as their number one public health danger," notes reStart in a statement. "The United States, by contrast, has been slower to recognize and respond to the problem but now is beginning to take some active steps. This program is part of that process."*[31]

Internet addiction can literally ruin people's lives. It can seriously harm or ruin a marriage. It can cause people to neglect serious responsibilities, lose their jobs and their homes. It has physically detrimental effects.

"[W]hen Internet use becomes excessive, it can—like other impulse disorders—be distressing and disabling," says psychiatrist Nathan Shapira, MD, Ph.D.[32] "Loved ones are always the first to identify this problem—those glued to the screen rarely recognize it in themselves," Shapira told WebMD.com. "Interpersonal relationships are the first to suffer."

The internet, as an engaging, interactive, and often fun medium, lends itself to addiction. As responsible, religious Jews, we must strive to find a balance, using the internet as a tool and not letting it c'v take over our lives. ■

The author of this article advises that anyone who wishes to follow up on the sources cited below should do so with a default browser setting of "Display no images" and only turn them on when necessary.

[30] Khanna, P. and A. "Korea's Internet Addiction: Fate of the World?" Big Think. 6 July 2010. http://bigthink.com/hybrid-reality/koreas-internet-addiction-fate-of-the-world

[31] Peeples, L. "Breaking free from the Web: New rehab caters to Internet addicts." *Scientific American*. 21 Aug 2009. http://www.scientificamerican.com/blog/post.cfm?id=breaking-free-from-the-web-new-reha-2009-08-21

[32] Davis, J. L. "Internet Addiction: Ruining Lives?" WebMD.com Health News. 7 Aug. 2003. http://www.webmd.com/baby/news/20030807/internet-addiction-ruining-lives

Re-Solutions

We've learned all about the terrible problems associated with the internet. We've all undertaken only to use only it if we must, and then only with the proper filters.

Ok, so what do we do now?

The answer is that there is a wide assortment of filtering products available to you today. It is important to be well informed of the options so you can choose the filtering solution that is most suitable for you. A wrong solution is as good as no solution.

The following information is provided by Technology Awareness Group (TAG).

Baruch Hashem, we have reached this point. אילו קרבנו לפני הר סיני ולא נתן לנו את התורה דיינו – Just gathering together with tens of thousands of concerned Jews to make the commitment and proclaim "נעשה ונשמע – We will act!" is the most empowering step in our newly launched War on Technology. We are prepared to implement the safeguards necessary to maintain the purity of our minds.

Now the question is, "What must we do to protect ourselves?"

If you are thinking to yourself, "Put a filter on the computer," you are only partially correct. There are a number of products and services, each with their own set of benefits and problems. No single solution is perfect. In fact, the wrong solution may be no better than none at all.

Let's begin with a general overview of the pros and cons of the various approaches to filtering the internet:

1. Using a kosher internet provider does protect your computer from accessing unfiltered internet through a cable or DSL, but if your computer is outfitted with a wireless adapter, it does nothing to protect you from your neighbor's unlocked, unfiltered Wi-Fi. This is a growing problem, as more and more wireless "hot spots" are being set up, such as at public libraries, internet cafes and elsewhere.

2. Installing a filtering software program on your computer may protect that computer entirely, but it will not protect another computer or device you use to access the same internet connection.

3. Some businesses use a router filter that acts as a physical barrier between the internet connection and the workers' computers. This has the drawback that in theory a worker could bypass the router filter and connect his computer directly to the internet. (We will offer solutions to this problem below.)

There are two general approaches to filtering: whitelisting and blacklisting. Whitelisting blocks all sites other than those specific ones needed by that individual for his work. This makes it extremely unlikely for a slip-up to occur. Blacklisting, on the other hand, seeks to block only those sites that are known to the filter to be problematic. Local filtering software offers a weaker level of protection, since it can be circumvented, especially by those who are computer savvy. In any case, no filter can be considered 100% foolproof.

In the case of blacklisting filters, it must be understood that the filter is no more than a program that attempts to identify problematic sites and then block them. It is only as good as the programmer who designed it. Different filters rely on different algorithms to decide which sites to block, and no system is perfect.

Some filters block the URLs to websites which are considered problematic. They are programmed with a list of which websites to block. The obvious flaw in this system is that it offers no protection against brand new websites that have not yet been brought to the filter's attention. It is impossible for the filter provider to remain fully up-to-date with all of the new websites that are constantly being set up.

A more sophisticated type of system is called dynamic filtering. Under this system each website is first examined by the filter when the user tries to access it. If the filter detects "unkosher" material, it will block that page from opening. Some of the filters do a better job than others.

Even the best of filters are—in most cases—not produced by Orthodox Jews. As a result, not everything that the filters allow through is necessarily in keeping with what we should be seeing. For example, even if a site may not contain any filth, it may carry material from Christian missionaries. Photos may be permitted even though they would not pass our standards of decency. As has been made abundantly clear, avoiding even partially indecent images is not לפנים משורת הדין – beyond the letter of the law. It is required by basic Torah law.

Even with a filters that does supposedly block 100% of the problems, the following issues may still exist:

1. Most software filters allow the user himself to control the filter under his own username and password. In that case, the computer is technically protected, but the user is not. He may deactivate the filter in a moment of weakness. It is critical that a trusted third party should set up the filter with a password unknown to the user.

2. If the filter does not block an image search and the user can look for pictures, the computer cannot be considered protected. Not only can the user utilize an image search to view inappropriate pictures, he can also use the pictures to reach linked, unsuitable sites that the filter may miss.

3. Even if the filter does a flawless job of blocking problematic websites, the user can still insert an inappropriate CD or DVD, or even a USB device with non-kosher content.

It would seem that the best solution to these problems would be to install one of the several monitoring programs that are available. These programs track all internet activity and send a periodic report to an outsider who is appointed to oversee that computer. The knowledge that an outsider will check the log can be a powerful deterrent from accessing filthy sites.

BUT—even a monitoring service has its drawbacks:

1. If the monitor is a close friend, he may not be a sufficient deterrent to prevent the user from visiting inappropriate sites. Even worse, the innocent monitor may now have in his hands a list of non-kosher websites.

2. Monitoring programs can miss some websites. If the user has access to the report, he can discover which sites are immune to the monitoring and then visit them with impunity.

3. It is advisable that the program be able to monitor non-internet activities taking place on the computer. This is important because the computer can be used to view unsuitable videos or games.

4. Monitoring software should only be considered effective when used together with a filter. This is because the monitor only prevents intentional accessing of improper websites but does not block inadvertent exposure to indecent material. Especially in the case of children, one wrong glance can affect the child for life.

In light of this, we must point out a widespread misconception in the Orthodox community... an unfortunate number of people continue to walk around with full internet access in their pockets. These people remain as unprotected as they were before

In short, the solution to the internet problem is far from simple. For each situation there is a

different solution, and for some there is no easy solution at all. In such a case the potential user must reassess whether it is worth the risk to use that particular device.

We must emphasize that all the talk about the importance of filters in recent years should not be understood to imply that a filter is an ideal solution. Any technician can tell you that this is not the case. Filters are no more than a backup solution. To properly protect a computer requires far more than just a filter. In this article we hope to educate the public about the different options that are available to make our computers as safe as we can.

*

If we are able to implement a standard of universal filtering of all computers in our community, we will have won a tremendous victory in our battle with the internet. Unfortunately, we will still not even have begun to solve the problem in its entirety. This is because the internet problem is no longer computer-based.

The times when you needed a computer to access the internet are long behind us. It is becoming easier each day to log on with smaller and smaller devices. In light of this, we must point out a widespread misconception in the Orthodox community: thousands have heeded the advice of our *rabbonim* and protected their computers from the internet. At the same time, though, an unfortunate number continue to walk around with full internet access in their pockets. These people remain as unprotected as they were before.

Many people today have tablets which may facilitate internet access even more than smartphones, and perhaps even the traditional computer. Until recently MP3 players were treated as harmless devices that could only be used to play back recorded music or speeches. (Some have pointed out that because they require computer access to load them, in many cases MP3 players became the villains that introduced innocent youths to computers.) Today, many come with internet access, as well as screens which can be used to watch videos.

It is shocking to discover how many in our community remain uninformed about how dangerous these items truly are. If they are not aware of the problems, they will not employ the available safeguards to protect themselves. The *rabbonim* have ruled that no one should own a smartphone, tablet or any similar device that offers internet access unless safeguards are implemented to prevent their misuse.

Following is an overview of the variety of computers and other devices that offer internet access and the appropriate steps to be taken for each category.

Computers, Laptops, Netbooks

Desktop Computers

For years the desktop computer was the most basic method for accessing the internet. This device, composed of a hard drive, monitor (screen), keyboard and mouse is clumsy to move around. Even recent models which are far lighter and smaller than their predecessors are inconvenient to move.

Recommendations

- Desktop computers should be kept in the most public location available. The more open the area is and the more people that can view the computer, the safer it is.
- These computers should be stored in a way in which they are not accessible to children (e.g. a locked cabinet).

Pros

- Because it is inconvenient to move around, a desktop computer is unlikely to be removed even temporarily by a child.
- At this point in time, the typical desktop does not come with a Wi-Fi option. That means that unless the computer is hooked up to an internet line there is no need to worry about it being misused. **Important Note**: Some newer models do have a built-in wireless connection. Aditionally, small USB wireless adapters are very inexpensive and can be covertly plugged in to the computer at any time.

Cons

- Even if the desktop has no internet connection, or it has internet with a proper filter, there is still the potential of it being used to view unsuitable materials on the CD or DVD player. You may need to ask your supplier to sell you a computer that does not include a DVD drive, or you can have the media codec removed to prevent the computer from being used for videos.

Laptop (Notebook) Computers

The laptop came out not long after the PC came into common use, but its popularity exploded in the last 10–15 years when the price dropped. The laptop is intended to provide the same options as a desktop computer, albeit with less power, in a compact and therefore more transportable form. Laptops are particularly popular for those who need to save space or to carry their work with them wherever they go.

Recommendations

- Laptops should be stored under lock and key when not in use so that children or other unauthorized persons cannot access them.

Cons

- Aside from the fact that almost all laptops come with a built-in DVD player, they also usually have a built-in wireless adapter. That means that even if the internet connection in your home or office is filtered, the computer can still access the internet through an unfiltered wireless connection, particularly when travelling.

Netbooks

Netbooks first appeared in 2008 and they became an instant success due to their much smaller size and price compared to laptops. Netbooks are intended as a lighter and cheaper alternative for those who can afford less computing power than the laptop or find the laptop either too bulky or too expensive.

Pros

- Netbooks are so small that they do not contain DVD drives. **Important Note**: Netbooks can still be used to view videos or movies through an external apparatus plugged into its USB port.

Cons

- Because they are small and lightweight, Netbooks easily lend themselves to being "borrowed" and misused by children or others without the owner's knowledge. It is extremely important that they be locked safely away when not in use.

Kosher Internet Providers

J-net

J-net is the only Jewish company to offer a blacklist filter, meaning that you can access anything on the internet except for those sites that are deemed inappropriate and blocked. J-net also offers whitelist filters that block all access except to those specific websites that are needed by the user. The internet can also be blocked entirely, leaving e-mail access only.

Pros

- The filter is produced by Jews in accordance with Jewish values.
- J-net's filter can detect unsuitable material even when it is written in Hebrew.
- The internet is filtered before it enters your home or office, meaning that every computer or device using that connection is protected.
- J-net uses real time filtering to filter websites in 4 milliseconds as you open them.
- J-net is one of the only companies to offer the option of blocking any exposed skin or entire images that are deemed inappropriate.

Cons

- The internet is slightly slower than without the filter.
- Requires a monthly subscription.
- A wireless connection to a different provider will allow you to access the internet without filtering.

Possible Solutions

It is advisable to disable the Wi-Fi option on your computer. Ask your supplier or call TAG and ask how this can be done. If for some reason you need to maintain your wireless option, such as to access the internet while on a business trip, make sure to install a separate software filter on your computer.

Kosher Internet Providers

YeshivaNet

YeshivaNet offers whitelisting to block out all internet except the specific sites you need. YeshivaNet also offers an e-mail only option.

Pros

- YeshivaNet is extremely careful about which sites it permits. There is no way to open a site that is not on your whitelist.
- Access is filtered outside your home or office, protecting all computers and devices that share that internet connection.

Cons

- The internet is slightly slower than without the filter.
- Requires a monthly subscription.
- A wireless connection to a different provider will allow you to access the internet without filtering.

Possible Solutions

It is advisable to disable the Wi-Fi option on your computer. Ask your supplier or call TAG and ask how this can be done. If for some reason you need to maintain your wireless option, such as to access the internet while on a business trip, make sure to install a separate software filter on your computer.

Software

K9

K9 is a free filter that is produced by a respected company, Blue Coat, which is a leading provider of Web security solutions. The filter does a reasonably good job at filtering out most inappropriate websites, especially when it is set to a higher security level.

Pros

- The filter is free and can be installed on as many computers as you like.
- The software is installed on your computer, eliminating the possibility of bypassing the filter through a wireless connection.
- Can be programmed to allow internet access only at set times of day.
- Also blocks virus-infected and malicious websites.

Cons

- K9's greatest drawback is that it is designed to protect children, not adults. The computer's owner enters the password and can therefore uninstall the filter at any time.

Possible Solutions

- Have the password entered by an outsider who is not a close friend and will not share it with you. For more details, call TAG.
- A popular method to protect the computer is for two or more people to each know part of the password. That way no single person can disable the filter. This method is *not* recommended.
- Because it is produced by a company whose views differ from ours, K9 permits material that is inappropriate for our adults as well as children.
- Although the filter has a good success rate at blocking unsuitable websites even in foreign languages, it is not guaranteed. On occasion, sites that should not be viewed are permitted.

Software

KosherNet

KosherNet provides software that can be downloaded directly to your computer for a relatively low price.

Pros

- Because the filter is installed in your computer, the computer is protected against any internet connection, including wireless.
- The filter is produced by Jews in accordance with accepted Jewish values.
- The password is kept by the company so it cannot be disabled by any user.
- KosherNet provides separate user accounts when more than one person uses the computer, allowing each user to choose the filtering level appropriate for him or her. A user that needs only e-mail service can block the internet entirely.

Cons

- The filter protects only that particular computer and not other computers or devices that may share the same internet connection.
- The filter employs lists of improper websites and various keywords. There is a chance that an inappropriate site may slip through the filter.

FilterNet

FilterNet is another company that provides filter software that is downloaded directly to your computer.

Pros

- Because the filter is installed on your computer, the computer is protected against any internet connection, including wireless.
- The filter is produced by Jews in accordance with accepted Jewish values.
- The password is kept by the company so it cannot be disabled by any user.
- FilterNet provides separate user accounts when more than one person uses the computer, allowing each user to choose the filtering level appropriate for him or her. A user that needs only e-mail service can block the internet entirely.

Cons

- The filter protects only that particular computer and not other computers or devices that may share the same internet connection.
- The filter employs lists of improper websites and various keywords. There is a chance that an inappropriate site may slip through the filter.
- Requires a monthly subscription.

Router-based Software

VocaTech

VocaTech, under Orthodox ownership, provides high-quality PBX, VoIP, filtering and other services for businesses. Since their filter is router-based there is no software to download and it is very hard to circumvent even for a professional.

Pros

- The filter was created by Orthodox Jews in accordance with Jewish values.
- Professional team researches and updates VocaTech's blacklist daily.
- Ability to whitelist as many as hundreds of thousands of websites.
- VocaTech gets an alert if the administrator unplugs the router.
- VocaTech claims its router actually speeds up the client's web-services.

Cons

- Laptop computers are not protected when outside of the office.
- Requires purchase of router and a monthly subscription.

SonicWall

SonicWall offers a line of router filters for both small and large businesses, allowing the business to control the content of the internet that its workers can access.

Pros

- Provides filtering for any computer or device relying on that router.
- Allows different settings for each computer so access can be customized for each individual worker.
- If a worker accesses a site that is not permitted or commits any other forbidden computer activity, the administrator is immediately notified through an e-mail message.

Cons

- Despite SonicWall's good performance rate with its whitelist, its blacklist filter should be considered below par.
- It doesn't apply real time filtering.
- The administrator has the password and can use it to permit unsuitable material to his/her own or others' computers.
- SonicWall will not block outside wireless connections.

Router-based Software

OpenDNS

OpenDNS is a free (for personal use) DNS service that also offers free filtering. When installed in one computer it blocks inappropriate sites and content in all computers and devices that are relying on the same router.

Pros

- Provides filtering for any computer or device relying on that router.
- Protects computers from malware and spyware.
- Blocks phishing websites from loading on your computer. It uses data from Phishtank, a community site that is also used by Yahoo! Mail to determine if some particular website is part of any online phishing scam.

Cons

- The one who installs it knows the password.
- Does not block outside wireless connection.
- If a domain cannot be found or a webpage is blocked, the service redirects users to a search page with search results and advertising unless the user has paid for an upgraded service.

iBoss

iBoss provides router filters for homes, businesses and schools that both filter content and offer time limits.

Pros

- Provides filtering for any computer or device relying on that router.
- Allows different settings for each computer and even different users on the same computer.
- Can be set to send an e-mail or text message in case someone unplugs the router filter. (This does not protect the individual who receives the message from unplugging the filter himself. Solution: Have the message sent to an outsider who does not have access to the router.)

Cons

- The one who installs the router knows the password.
- Does not block outside wireless connections.

Router-based Software

Livigent

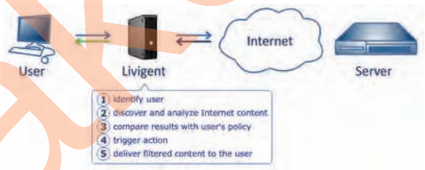
Livigent is designed specifically for businesses. The company uses updated technology to block websites that may slip past other filters. J-net recently partnered with Livigent to sell its products to Orthodox Jewish business owners and homeowners who wish to use a mainstream internet provider and still benefit from a strong filter.

Pros

- Aside from blocking bad websites, the filter uses cutting-edge technology to analyze the text content and images of each and every website, allowing it to block sites that have not been blacklisted by other filters.
- Understands 12 different languages, guaranteeing that indecent material will be blocked in foreign languages as well.
- Permits blocking bare skin or entire images deemed inappropriate.
- Password is kept by the company, preventing individuals from bypassing the filter.
- Optional software installed on computers can block the internet if the Livigent device is unplugged.

Cons

- Does not block outside wireless connections.



Monitoring Software

Monitoring software employs an entirely different approach to the above solutions, in that it does not provide filtering. Instead it provides a deterrent to viewing inappropriate material by sharing a log of sites visited with a designated outsider.

Important Note: Even a computer that benefits from a strong filter must have monitoring software as a backup, since even the best filters will occasionally allow certain unsuitable sites to be accessed. Monitoring compensates for the shortcomings inherent in the filtering systems. At the same time, monitoring without a filter is insufficient for a number of reasons, the primary one being that it does not prevent an unsuitable site from being opened inadvertently.

WebChaver/Covenant Eyes

WebChaver and Covenant Eyes are very highly regarded monitoring software programs that log each site visited by the computer on which it is installed and send a monthly report to a responsible outsider appointed as that computer's monitor.

Pros

- Generally do well at noticing sites that filters may overlook.

Cons

- If the monthly report contains improper sites, it can lead to complications, such as compromising the monitoring individual.

Possible Solution

Choose a responsible, upstanding monitor who is sufficiently removed from the computer's owner and users to present a serious deterrent.

Like filters, monitoring programs only report on internet activity and not the programs, games and videos which may have been used on the computer.

Monitoring Software

eBlaster

This monitoring service tracks other computer activities in addition to internet use, but is also more complicated.

Pros

- In addition to monitoring online searches and websites, it tracks which programs were used, records chat conversations and e-mails as well as every keystroke.
- Separately tracks each user, including exactly when and how long they were on the computer.

Cons

- Reports are complex and difficult for non-experts to follow.
- Does not report on the types of videos viewed on the computer.

PC Black Box

PC Black Box takes screenshots of all activities performed on the computer and sends it to a pre-arranged e-mail address.

Pros

- Saves the standard keys pressed, programs used, websites visited and takes screenshots at selected intervals.

Tablets

(iPads, Androids, etc.)

These devices were specifically designed to provide constant mobile access to the internet, any time and any place. Their extreme portability combined with the increasing prevalence of Wi-Fi present a serious challenge—far worse than the desktop computer. Because of their small size, the deterrent factor of being seen by others while browsing the web is virtually eliminated.

Because they are so new, there are far fewer established solutions for filtering these devices. Purchasers of these devices are urged to proceed with extreme caution. Beware of the fact that there are currently no satisfactory solutions available. The following represents the best recommendations based on what we know at this point in time.

iPad

K9 provides a filtered browser for iPads that can be downloaded for free. The filter blocks unwanted websites, but our technicians have found that on the iPad it can be bypassed. In addition, the iPad can be reset, returning it to its pre-filter state.

Solutions

Until a better filtering option becomes available, be forewarned that the iPad is completely unsuitable for children. Download an apps lock and place a lock on all apps that can be used to browse the internet, excluding the K9 browser and whatever apps are critical for you. It is advisable that the user not have the password to the apps lock.

A monitoring app can be downloaded to monitor all activities on the iPad and send an e-mail report to a selected address. The monitoring app must be locked so it cannot be deactivated.

Android

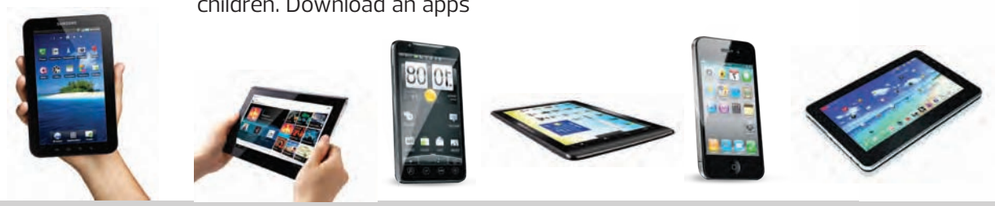
K9 has just released a filter for the Android. Our initial tests indicate that this is a strong filter for blocking unsuitable websites. However, it suffers the same issue as all other K9 filters: namely, that the administrator has the password and can bypass the filter. This problem can be solved with one of the solutions we mentioned above in the K9 section for computers. An additional problem is that the Android can be reset, returning it to its pre-filter state.

Another option is the McAfee app which can be used for filtering and monitoring, but from what we have heard thus far, it is not too difficult to bypass.

Solutions

No filter is ideal, so be certain that in addition to K9 you download locks and apply them to all apps that involve internet usage. It is advisable that the password be known only to someone other than the Android's user.

You can also download a monitoring app to monitor all activities on the Android and send an e-mail to a selected address. The



monitoring app should be locked to prevent it from being deactivated.

Blackberry Playbook, Windows Tablet

At this point in time there is no filter available for Blackberry Playbook or Windows Tablet. We strongly discourage the purchase or use of these devices.

Cell Phones

Virtually all cell phones today offer internet access, but the greatest danger lies in smart phones, such as the Blackberry, iPhone and Android since they function as pocket-sized computers with full internet capabilities.

Blackberry

The only company that provides a filter for Blackberries is J-net. This filter costs just a few dollars per month, but to use it you have to add a service called Enterprise to your plan. Enterprise is offered by Verizon and Sprint for approximately $20 per month. The J-net filter for the Blackberry performs well and cannot be bypassed. At the client's request, J-net can also block internet entirely and provide e-mail-only service.

A much cheaper solution is to use the everylock app to shut off the browser completely. Again, though, the bearer of the password has the power to unlock the browser.

iPhone

K9 offers a free filtered browser for the iPhone. Or, for $4.99 you can download Mobicip, which does a very good job of providing filtered internet service. The browser relies on Mobicip's servers to filter unwanted URLs and search results.

The problem with both of these filters is that they are designed to protect children, not adults. As such, whoever downloads the browser also knows the password and can bypass the filters. In addition, these filters are not foolproof. In short, at this point in time there is no satisfactory filtering solution to protect iPhones from accessing unsuitable websites.

To further protect your iPhone, you should download an app lock and lock the app store, Safari browser and YouTube to guarantee that unsuitable content will not be accessible.

There is one additional solution for the iPhone: mymobilewatchdog.com provides a good monitoring service, but this service has issues and may be difficult to use.

Important Note

The internet is evolving faster than anyone can imagine. There are many more devices than just computers that can access the internet, including but not limited to MP3s, iPods and gaming devices for kids. Most of them are extremely difficult to monitor and filter. People should be extra cautious about those devices and children should not be allowed to have access to any device that has internet capabilities.

In the coming years as the internet becomes much more sophisticated and internet access will become standard on many more electronic devices, the struggle against the negative influence of the internet will become ever tougher. We have to be on constant alert in the fight against this terrible enemy and to ensure the spiritual and physical safety of our kids. ■

וכתוב בספר וחתום וכו' למען יעמדו ימים רבים

(ירמיה לב)

באותיות של זהב ייחקק כאן, כי זכיתי לקחת חבל במעמד הנדיר והנפלא **"כינוס כלל ישראל"**, כינוס אשר כמוהו לא נהייתה, בהקבץ חמש רבבות יראים ושלמים מאחינו בני ישראל בגולת אמעריקע, בראשות גדולי ומאורי חכמי האומה שליט"א, ביום המיוחס ערב ראש חודש סיון, שנת תשע"ב לפ"ק, בשטח האדיר "סיטי-פיעלד".

זכיתי לקחת חלק, ולקבל על עצמי _____

זכיתי לשמוע את דרשת _____

זכיתי לקבל עול מלכות שמים ביחד עם המון רבבות אחינו בני ישראל!

הערות ורשימות

_____ חתימה

Souvenir of Attendance

וכתוב בספר וחתום וכו' למען יעמדו ימים רבים (ירמי' ל"ב)
And record it in writing and seal it...
that it may last for many days. (Yirmiyahu 32)

Let it be recorded for posterity that I _____ עמו"ש heeded the call of the Gedolim and participated in person at the historic Asifa at which Klal Yisrael, with the Gedolim of America at the helm, gathered together at Citi Field on Erev Rosh Chodesh Sivan 5772, May 20, 2012, to unite in committing ourselves to facing the challenges of modern technology.

In the course of the evening I listened to and was inspired by addresses by:

_____

_____

The following points in particular made an impression on me:

_____

_____

_____

I was deeply moved by the following aspects of the program:

_____

_____

As a result of this event I have taken upon myself the following resolution/s:

_____

_____

Impressions/Notes: _____

_____

_____

_____

_____

Signed: _____

Back Page

ad for TAG