

Bloxx Anonymous Proxy Security Survey - 2009

The Results

Analysis of Survey Results

INTRODUCTION

This is the second year Bloxx has run its Anonymous Proxy Survey, an assessment of the impact of anonymous proxies on over 200 organisations in the education and private sectors.

Anonymous proxies are the most popular and easiest way for users to bypass Internet filtering. Once connected to an anonymous proxy, users can view any site even if the web filter should have blocked it. Proxy sites have proliferated in the past few years due to availability of open source tools, which allow a proxy site to be created quickly and easily.

Many hundreds of anonymous proxy sites are created each week and blocking them using traditional web filters, which rely on anonymous proxy URL lists, is no longer efficient or effective. Consequently, the responsibility often lies with IT managers to identify and block these sites, which allows users to surf freely until the site is blocked.

ANALYSIS

In general, the results of the Bloxx survey seem to determine that IT teams in the education sector are more aware of the issue of anonymous proxies and their use than in the private sector. Students tend to be more tech-savvy and have traditionally been more adept at finding ways round filters than users in other types of organisation, who are more constrained by company policies, time, and so on.

Are you concerned that Anonymous Proxies may pose a security threat to your network?

The majority of respondents from both sectors agree that anonymizers pose a security threat to their organisation and network but it seems the issue is more prevalent in education: 64% agreed that they posed a security threat. IT teams in the private sector are aware that they could cause trouble - 46% said they may pose a security threat but many don't see them as much of a problem yet as they don't think that many employees are aware of them. However, 12% of private sector respondents were unsure if they posed a threat indicating that there may be a lack of knowledge within some parts of this sector of the use of proxies for filter avoidance.

What impact are Anonymous Proxies having in your establishment?

Further evidence for this point is indicated by the data on the impact anonymizers are having on the organisation. Again, they are much more of an issue in education than the private sector; 49% in the private sector said that, at the moment, they weren't a problem, whereas in education 90% of users agree that they are a problem to some degree. Education IT Teams agreed that 33% thought it was a serious problem, spending a fair bit of time keeping it under control and 3% claimed it's a major problem; they spend excessive amounts of time keeping it under control, compared to 4% and 1% respectively in the private sector.

What types of issues are anonymous proxies causing in your establishment?

Anonymizers cause a variety of issues for organisations, but the focus in each sector seems to be different. The private sector are more concerned about Acceptable Use Policy violation, threats to network security (e.g. viruses and phishing) and information loss. Loss of employee productivity is a huge issue for the private sector who don't want to pay employees to surf non-work related sites instead of doing their job.

In education it's a different set of issues: child protection and bullying prevention are currently big issues where the use of anonymous proxies could potentially lead to increased risk of these activities going undetected. Unfiltered access to social networking sites is an issue for both sectors as well as the serious impact that sites accessed via anonymous proxies have on network bandwidth usage.

How does the problem of Anonymous Proxies compare to 12 months ago?

Worryingly, it looks like the proxy problem hasn't improved for IT Teams; 65% in the private sector and 47% in education claim they're still spending the same amount of time dealing with them as they did last year with 15% (private) and 20% (education) saying the problem is slightly worse and 2% (private) and 9% (education) revealing the problem has got significantly worse and they're spending much more time dealing with them.

In a typical week, how much time would you say you spend dealing with Anonymous Proxies?

Education IT Teams seem to spend more time dealing with anonymous proxies each week than their private sector counterparts with 41% indicating they spend between one and four hours a week doing this and 3% spending more than four hours a week whereas only 16% in the private sector say they spend over one hour dedicated to the problem. This again indicates the higher prevalence of their use within education as well as highlighting the awareness of education IT Managers of the importance of blocking their use from students, who could be exposed to any type of material through their use.

Typically, how long does it take to find out about a new Anonymous Proxy site and get it blocked?

A problem with many web filters on the market is that because of the high turnover of proxies, they simply don't have the proxy URL in their database so students can access it and consequently bypass the web filter. When a new proxy is discovered by IT, usually through web access reports, the URL is often given to the filtering company to add to their database. 44% of respondents in education and 24% in the private sector claim it takes between a day and a week or more to get a proxy site blocked – which is a huge amount of time, and the implications of this for education users is worrying.

CONCLUSION

The issue of anonymous proxies will not go away and continue to be a 'cat and mouse' game between users discovering new anonymous proxy sites and IT detecting and blocking access to them. The education sector is traditionally one step ahead of other types of organisation in finding new ways to bypass filters; however, the private sector can't afford to keep its eye off the ball. They are aware of the huge potential security threat they pose to their network and organisation if users deploy them so they must ensure they have correct measures in place to deal with the threat when it arises.

To ensure protection of networks and users, organisations must adopt a strategy against anonymous proxies which should include a third-generation filtering technology that combines the best in traditional approaches with more sophisticated, point-of-request page analysis that spots anonymous proxies in real time; clear and well publicized AUPs that not only forbid access to anonymous proxies but emphasize the organization's ability to detect them; and an organizational willingness to consistently enforce AUPs.

The latter two points are managerial issues but the former requires a technology that most filters do not have. Bloxx Tru-View Technology conducts live contextual analyses to rapidly classify web traffic in real time to provide zero-day protection. With respect to anonymous proxies, the technology not only looks for common words and phrases, but for code structures characteristic of such sites, and analyzes the relationships between these elements to build levels of classification confidence. If the level rises above a specified threshold, Tru-View Technology will block the web page, even if no one in the organization had previously visited it. The technology also examines all layers of a site to find hidden proxy functionality, and it is extremely accurate. It will not, for example, mistake a Wikipedia page about anonymous proxies for an anonymous proxy itself. Yet if the Wikipedia page were to link to a real anonymous proxy, Tru-View Technology would block that site as soon as a user tries to visit. Moreover, the extensive reporting capabilities allow IT to identify users who try to access anonymous proxies. ■

To find out more about Bloxx web filtering call us on +44 (0)1506 426 976, email info@bloxx.com or visit www.bloxx.com/demo to book an online demonstration.

Education Sector - Example Comments

WHAT TYPES OF ISSUES ARE ANONYMOUS PROXIES CAUSING IN YOUR ESTABLISHMENT?

“Web surfing outside of prescribed safe limits, lesson disruption.”

“Uncontrolled access to the internet.”

“Kids trying to access blocked social networking sites.”

“Primarily the children use them for live chat, but there are a few little darlings that try accessing them for Hacking purposes.”

“Accessing unsavoury or unproductive content, bypassing email system (we block all the web email systems we can).”

“Allowing pupils to access banned sites such as games or inappropriate materials.”

“Access to porn from within school.”

“Excessive game playing, pornography on occasion, but in particular, compromised sites that downloads viruses to the workstation.”

“Loss of bandwidth.”

“Child protection.”

“Disruption to lessons and small incidents of bullying.”

“Illicit music and video access/download.”

GENERAL COMMENTS

“They are a pain.”

“We find students using proxies built into USB keys, or placed in social networking sites they use.”

“Can become a very serious problem, especially in schools.”

“Waste time for kids and threat to kids.”

“There are that many being created day after day, it is a case of doing a weekly check. We can't afford to do a daily check because of the time constraints.”

“Close them all down.”

“Is this a personal freedom issue?”

“Is blocking internet any use when our students go home and use unfiltered, unmonitored access? We take an approach that education on internet safety is more important than trying to prevent all access in school, although we still filter students!”

“The number of anon Proxies seems to be enormous and ever increasing, especially as students can easily access updated lists at home.”

“Almost impossible to keep up with new ones appearing.”

“Should be made illegal.”

Private Sector - Example Comments

WHAT TYPES OF ISSUES ARE ANONYMOUS PROXIES CAUSING IN YOUR ESTABLISHMENT?

- “Violation of internal Information Assurance policies”
- “Loss of productive hours through accessing sites like Facebook.”
- “Loss of productivity, potential bypassing of network security, breaching of IT policies.”
- “Allowing staff to bypass web filtering in order to access restricted or potentially unsuitable for work materials”
- “None at all; we’re a small company who are able to trust our staff.”
- “In truth, we do nothing about anon proxies at all. We have no idea if they are being used or if they pose a problem.”
- “HTTPS proxies are the biggest problem due to the encryption. The other major problem is the ability to code an anonymiser easily and host on any 3rd party platform.”
- “None - Security policies very tight. ie no access to uncategorised sites.”
- “Bypass potential security measures.”
- “Various nefarious internet based activity, tracing the source of any sustained scanning/enumeration activity would be difficult.”
- “Time - employess getting paid to surf.”
- “Bypassing existing filtering rules, allowing staff access to restricted or anonymised resources that put the company at legal risk.”
- “Not something we are concerned about.”
- “Allowing unmonitored web access to websites.”
- “We host our own websites so bandwidth is at a premium; hence the importance of being able to block access to these proxies.”
- “Access to blocked sites and getting virus into the newtwork.”
- “Viewing x rated sites.”

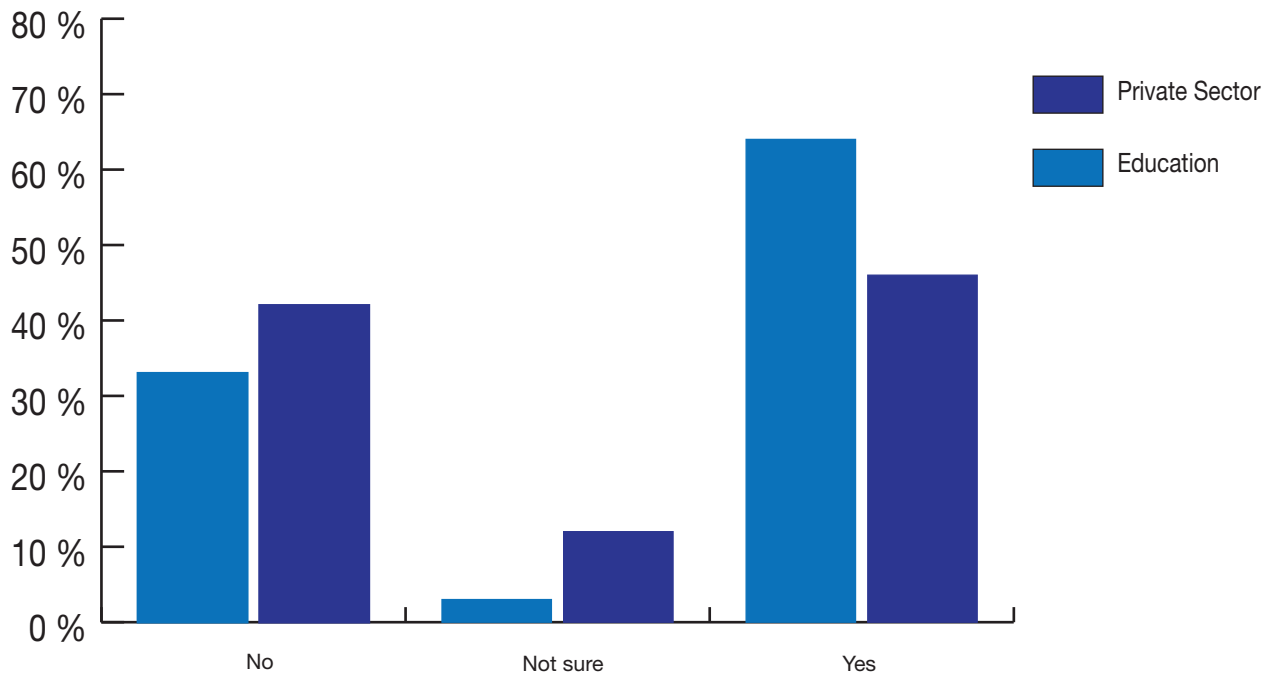
GENERAL COMMENTS

- “They are a pain.”
- “I don’t see them as much of a problem.”
- “The anonymisers are a serious problem.”
- “Need to be careful with these.”
- “No need for staff to use them because they can access the entire internet - nb work related!”
- “They are a bit in the geek field at present so aren’t of much threat now.”
- “Could cause disaster!”
- “If you attempt to control users. they will find a way around it. education is better than “old fashioned” company ideals.”
- “Should be banned.”

Q1.

ARE YOU CONCERNED THAT ANONYMOUS PROXIES MAY POSE A SECURITY THREAT TO YOUR NETWORK?

ANSWER OPTIONS	RESULT EDUCATION	RESULT PRIVATE SECTOR
No	33%	42%
Not sure	3%	12%
Yes	64%	46%



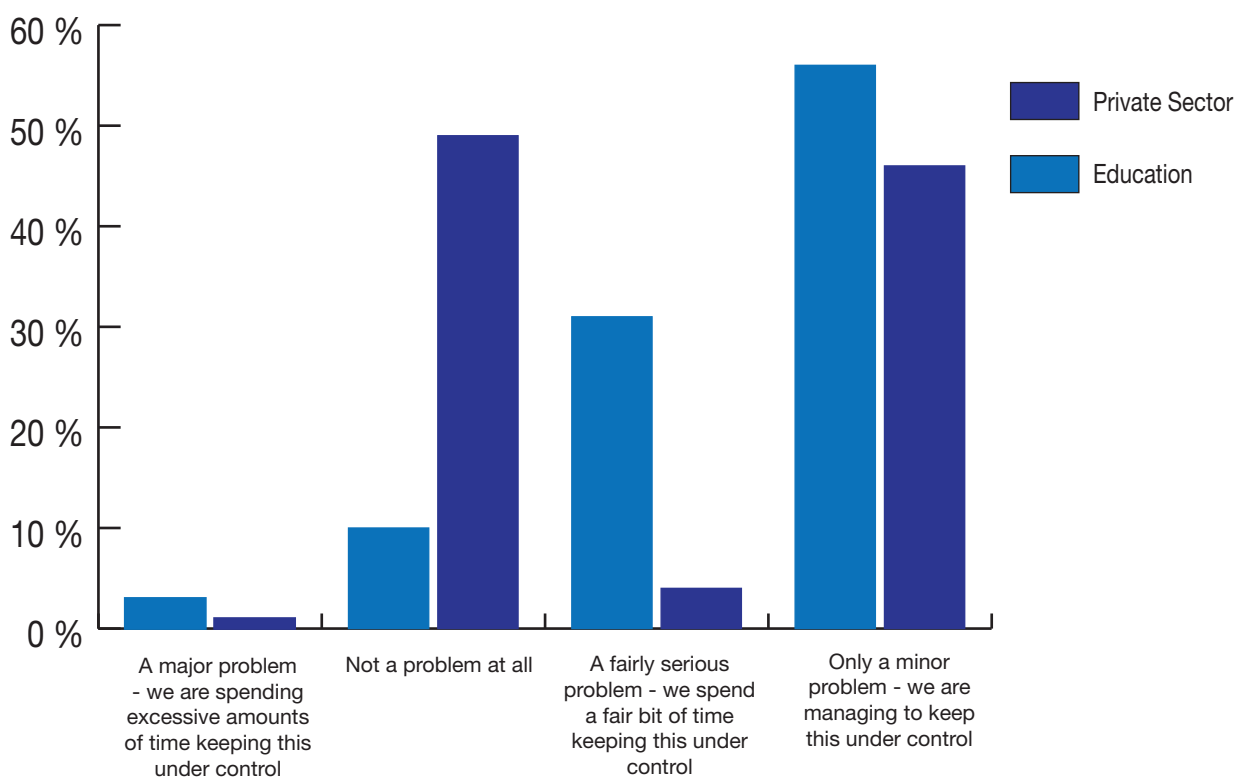
“ They can become a very serious problem, especially in schools. ”

Education user

Q2.

WHAT IMPACT ARE ANONYMOUS PROXIES HAVING IN YOUR ESTABLISHMENT?

ANSWER OPTIONS	RESULT EDUCATION	RESULT PRIVATE SECTOR
A major problem - we are spending excessive amounts of time keeping this under control	3%	1%
Not a problem at all	10%	49%
A fairly serious problem - we spend a fair bit of time keeping this under control	31%	4%
Only a minor problem - we are managing to keep this under control	56%	46%



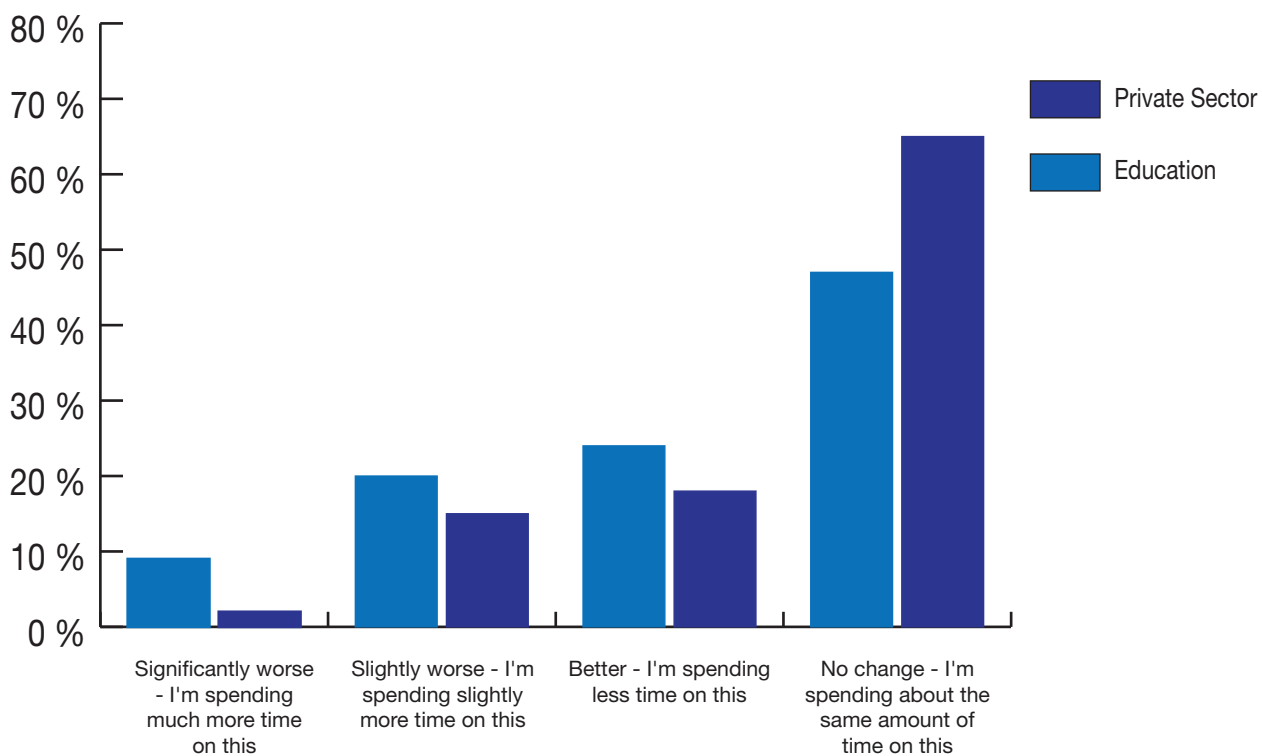
“ There are that many being created day after day, it is a case of doing a weekly check. We can't afford to do a daily check because of the time constraints. ”

Education user

Q3.

HOW DOES THE PROBLEM OF ANONYMOUS PROXIES COMPARE TO 12 MONTHS AGO?

ANSWER OPTIONS	RESULT EDUCATION	RESULT PRIVATE SECTOR
Significantly worse - I'm spending much more time on this	9%	2%
Slightly worse - I'm spending slightly more time on this	20%	15%
Better - I'm spending less time on this	24%	18%
No change - I'm spending about the same amount of time on this	47%	65%



“ They are a pain! ”

Education user

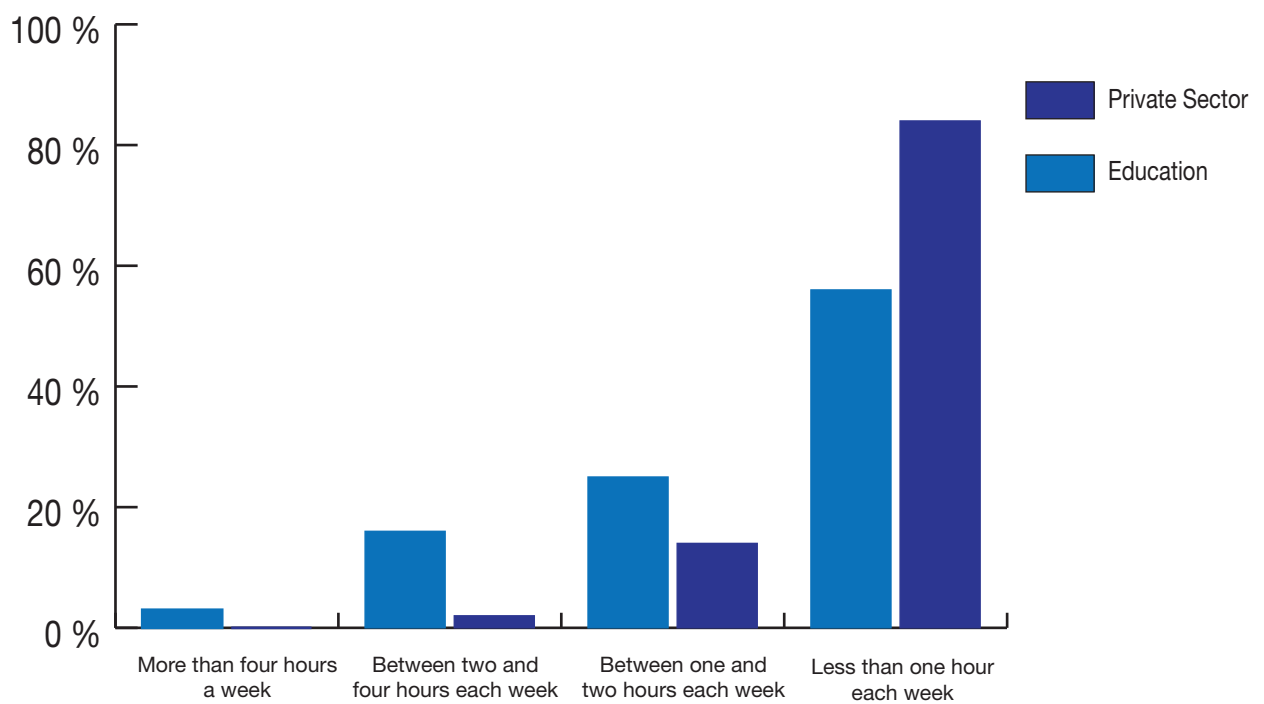
“ No need for staff to use them because they can access the entire internet - nb work related! ”

Private sector user

Q4.

IN A TYPICAL WEEK, HOW MUCH TIME WOULD YOU SAY YOU SPEND DEALING WITH ANONYMOUS PROXIES?

ANSWER OPTIONS	RESULT EDUCATION	RESULT PRIVATE SECTOR
More than four hours a week	3%	0%
Between two and four hours each week	16%	2%
Between one and two hours each week	25%	14%
Less than one hour each week	56%	84%



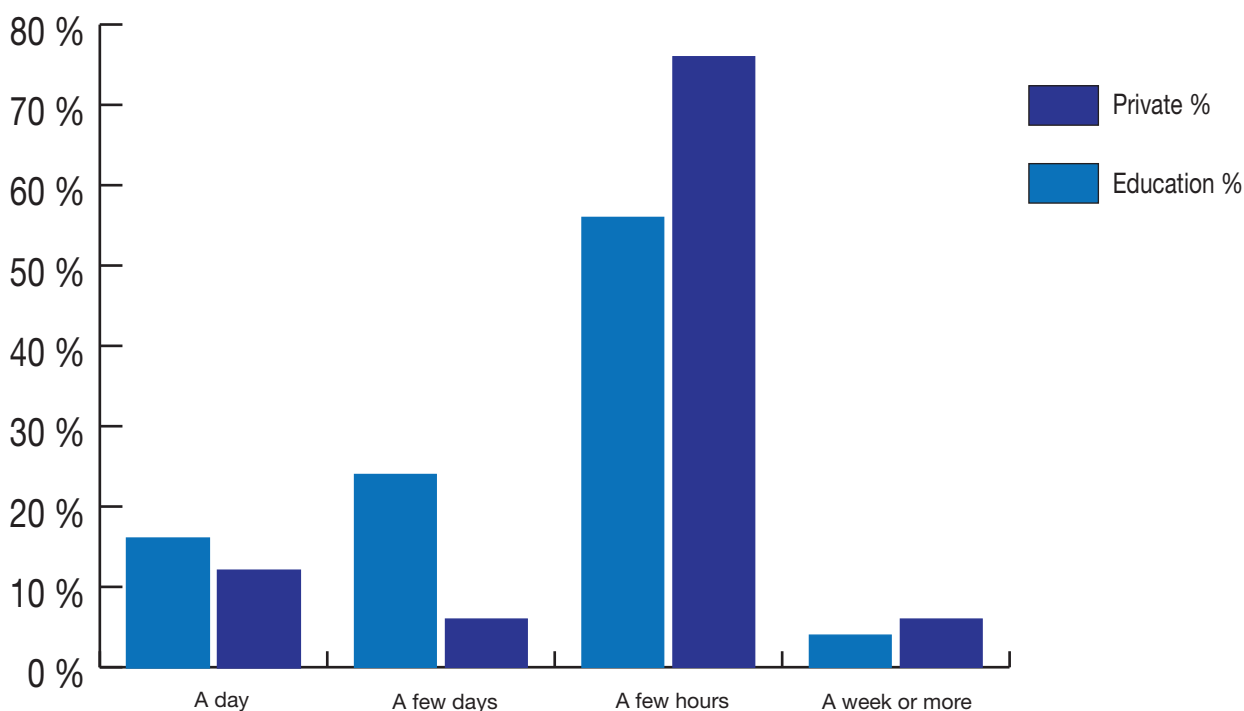
“ *Almost impossible to keep up with new ones appearing.* ”
Private sector user

“ *So far we rely on our “snouts” to keep us informed!* ”
Education user

Q5.

TYPICALLY, HOW LONG DOES IT TAKE TO FIND OUT ABOUT A NEW ANONYMOUS PROXY SITE AND GET IT BLOCKED?

ANSWER OPTIONS	RESULT EDUCATION	RESULT PRIVATE SECTOR
A day	16%	12%
A few days	24%	6%
A few hours	56%	76%
A week or more	4%	6%



“ They allow staff to bypass web filtering in order to access restricted or potentially unsuitable for work material. ”

Private sector user



ABOUT BLOXX TRU-VIEW TECHNOLOGY

Bloxx Tru-View Technology uses internationally patent pending technology to analyse and block web sites quicker and more accurately than other web filters, which use manual classification and keyword scoring. Tru-View Technology uses intelligent identification and analysis providing instant classification of web content as soon as it is accessed even if the content has not been seen by anyone before.

Bloxx Tru-View Technology helps organisations proactively manage users' access to web content which might lower productivity, expose the organisation to risk and liability or pose a network security threat.

An estimated 1 million + users already benefit from enhanced security and performance with low administration and no cost per user charges. Additional protection is provided via anti-virus, anti-spyware and anti-phishing functionality, alongside onboard cache.

ABOUT BLOXX

Headquartered in the UK with sales offices in Australia, Netherlands and the USA, Bloxx offers web filtering appliance-based solutions for medium and large organisations in both the business and public sectors. Leading UK investment groups such as Braveheart Investment Group Plc and Archangel Investments Ltd. have invested in Bloxx.

FOR FURTHER INFORMATION

For more information, please visit www.bloxx.com, call +(44)1506 426 976 or email info@bloxx.com.



Deloitte.
Technology Fast50
EMEA 2008

Deloitte.
Technology Fast50