

Entensys Corporations Usage of Internet at Work 2009 - Q2

Statistical Analysis:
Categories of Websites Visited by Employees at Work

Introduction

The study presented below was completed in April-June, 2009. The results are based on the analysis of websites visited by 41,200 employees in 1,600 enterprises.

BrightCloud Inc. provided the URL categorization source utilized in this study via the hosted BrightCloud Service.

Methodology



In the end of 2008, Entensys released a new version of UserGate Proxy & Firewall that included a content filtering tool. This feature enables the administrator to allow or deny users access to certain categories of websites.

The filtering tool's work is based on the following principle. When a user is trying to connect to a website from a corporate LAN, anonymous data containing website address and classification request (this request is later used to allow or deny access depending on the policy of the company that uses UserGate Proxy & Firewall) is sent to the content filtering server where it is stored and becomes available for further assessment.

We have analyzed information collected over the course of three months. The normal divergence was found to be within the range of 0.1% to 1.5%, depending on the category. Thus, taking into account the specifics of data samples, the results can be considered reliable.

The study was devoted solely to the usage of Internet at work. The reliability of the data samples is confirmed by the fact we analyzed information provided by enterprises from different industry sectors (see the chart below).

Respondents

The subject of analysis was represented by 41,200 employees of enterprises from different industry sectors and with different sizes of staff.

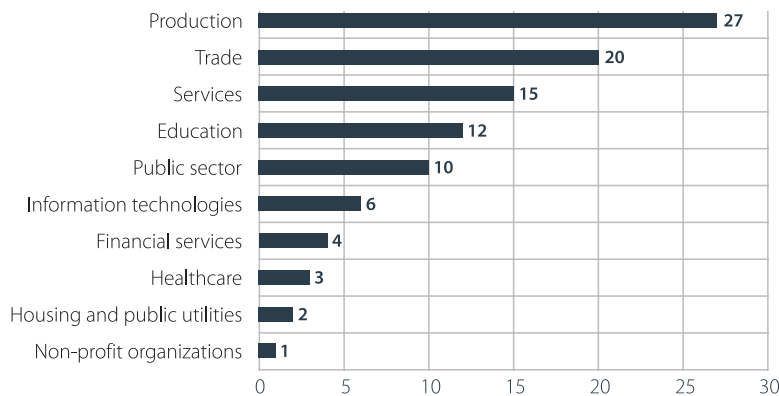


Chart 1: Enterprises by industry sectors, %

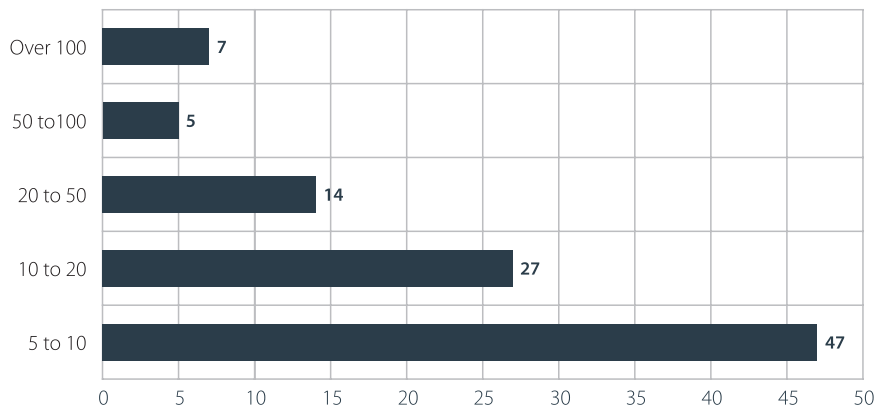


Chart 2: Number of computers in the companies under study, %

Internet Abuse



The content of websites visited by employees at work has been one of the employers' concerns ever since the Internet became a globally- used working tool. The uncontrolled usage of web resources is a problem for businesses that have to deal with the unexpected extra traffic costs and face the threat of malicious software infiltrating their local area networks and potentially causing loss or misappropriation of corporate information.

Moreover, the Internet offers a wide range of entertainment opportunities. Therefore, apart from evident potential threats associated with the Internet, businesses face the problem of Internet abuse during business hours, which is inevitable among employees suffering from low motivation. Quite obviously, this problem also causes businesses significant costs.

Until recently, businesses had only two ways of defending themselves against these risks – either through administrative action, or by monitoring and controlling the corporate resources. Now, new software solutions appear on the market that offers businesses additional opportunities to withstand Internet threats.

Statistics of Website Categories

Analysis of research conducted in the 2nd Quarter of 2009 resulted in the following rating chart of website categories popular among employees:

01.	Social networks, personal sites and blogs	20.40%
02.	Sites devoted to computers and Internet	14.10%
03.	Different categories of sites not related to work	8.70%
04.	Economics and business	7.60%
05.	Search engines	7.30%
06.	News and media	6.70%
07.	Online mail services	4.80%
08.	Parked domains and 'dead sites'	3.80%
09.	Entertainment and games	3.60%
10.	Sites containing malicious software	3.30%
11.	Advertisement sites	3.10%
12.	Data portals	3.10%
13.	Video hosting sites	3.00%
14.	Pornographic and adult sites	2.90%
15.	Personal online file storage services	2.80%
16.	Education and research	2.40%
17.	Online messengers, instant messengers	1.40%
18.	Online music stores	0.60%
19.	Government agencies	0.30%
20.	Peer-to-peer and torrent networks	0.10%

Note: The item "Different categories of sites not related to work" includes websites featuring such topics as beauty and health, cars, sports, etc.

General Conclusions

The study revealed several categories of facts that might be of some interest to information security officers, network administrators, managers and business owners.

The first category includes facts associated with Internet abuse at work.

- Over 20% of employees visit social network sites, blogs and personal sites daily¹. Thus, one of five employees spends a portion of time paid for by their employer socializing on the Web. Due to certain characteristics of such resources, these chats take considerably more time than chats over instant messengers (IMs) and, in the majority of cases, are not related to work.
- A more discrete assessment of the rating chart shows that if we put together category items 03, 07, 09, 13, 14 and 15, we get another 26% of employees who visit non-work related sites at work, in addition to those who visit social networks.
- In addition, 3.6% of employees² visit online gaming resources on a regular basis. While the percentage of such employees is rather small, the magnitude of total business time spent on gaming may be quite considerable.

1 Item 1, Personal sites and blogs.

2 Item 9, Entertainment and games.

The second category deals with the costs of Internet traffic.

- A relatively small number of employees (3%)³ who visit video hosting sites may, as a matter of fact, cost their employers a lot in terms of traffic expenses, channel bandwidth and general network performance. The same effects are caused by the employees who use their personal online file storages⁴ and buy and download music files at work⁵.
- The last category of websites on the rating chart, which is used by only 0.1% of employees surfing peer-to-peer networks, is still a vital threat to employers. In peer-to-peer (P2P) networks, data is constantly downloaded and uploaded, and several connections are kept alive at the same time. This is equivalent to several dozen users who download and send large volumes of data at once. Moreover, the use of P2P networks often implies transfer of data protected by copyright and other rights, which may result in lawsuits against the company from whose computer a P2P application was used.

Potential threats to network security constitute the third and the most significant category of facts.

- Line 10 of the rating chart can be discussed as part of a separate large research. It indicates that 3.3% of employees come across websites that contain malicious software. With no virus protection and application filtering, visits to such resources may result in the loss or misappropriation of corporate information, followed by a number of distressing consequences.

Social Networks



The statistical data on the visits of social networks by employees of small and larger businesses (with 5-25 and 100-200 computers, respectively) was the subject of a separate analysis. Referring to the number of computers, however, we do not mean the size of a company; it is the size of an individual office that is implied. A popular website facebook.com was the actual subject of research.

The frequency of visits to websites of this kind will obviously differ for smaller and larger companies. Reasons for this may include different approaches to employee activity control, different levels of information security, absence of elaborate corporate procedures, etc. The analysis focused on defining the relation of the frequency of visits to odnoklassniki.ru against the total number of websites visited by one employee.

The research results manifest a clear dependence of website popularity on the number of computers in a local area network and, consequently, the size of an office. For example, the frequency of visits to odnoklassniki.ru in LANs with 25 to 100 computers is twice higher than in LANs with 100 to 200 computers. At the same time, employees of offices with less than 25 computers in a LAN visited the website four times more often!

The above findings lead to a conclusion that employees of smaller businesses are subject to less strict control, which results in poorer work discipline.

3 Item 13, Video hosting sites.
 4 Item 15, Personal online file storage services.
 5 Item 18, Online music stores.

About UserGate



UserGate is a complex solution for sharing Internet access among local area network users. The software provides opportunities for traffic control, centralized Internet access administration and protection of a local area network from external threats.

Integrated BrightCloud URL filtering tool denies access to unwanted resources, whether individual website addresses or entire categories of web pages. The tool helps reduce the costs of bad traffic, increase employee performance and minimize risks of LAN being infected by malicious software.

UserGate solution provides a full-fledged protection of your local area network with the help of a built-in firewall and two antivirus modules from Kaspersky Lab and Panda Security. Besides, the program helps manage network activity of individual applications installed on client machines by granting or denying them Internet access.

About Entensys



Entensys is information security software vendor and a developer of Internet connection sharing products. The company's solutions are designed for Internet access management, network threat protection and traffic optimization.

For additional information about the company, visit our official website: www.entensys.com.

About BrightCloud



BrightCloud, Inc. provides hosted Internet security services that are available to enterprise customers from BrightCloud's OEM partners. BrightCloud's OEM partners integrate web filtering and as an added security layer to their existing solutions by leveraging the BrightCloud hosted Internet Security Service to maximize productivity and mitigate security threats. The BrightCloud

Internet Security Service leverages the BrightCloud Threat Operations Center, which provides security threat data, as well as the latest in machine learning algorithms and human classification, to build and maintain the largest and most accurate Internet security service available. For more information visit www.brightcloud.com.