Data Security & Integrity

Over 150,000 users have trusted HyperOffice since 1998. The service was founded on the belief that your data should be available to you – and *only you* – anytime, anywhere. Our ongoing investment and commitment to security allows HyperOffice to guarantee the absolute privacy and confidentiality of our customers' files.

This data sheet will answer many questions about how HyperOffice technology and security practices provide far superior data protection than the common practice of storing information on a personal computer or company network. With HyperOffice, your files are always accessible, up to date, secure and private.

Data Security & Integrity Facts

Percentage of Respondent(s)	With **HyperOffice**	Without* **HyperOffice**
Who have lost data due to computer theft in the last 12 months	0%	44.5%
Who risked integrity of their data due to inadequate data encryption and security measures	0%	88%
Who reported downtime and lost productivity due to inadequate computer access	*less than* 0.01%	72.7%
Organizations that do not have established guidelines for protecting proprietary data (for mobile workforces)	0 %	89.6%
** Brigadoon Software 2003 BSI Computer Theft Survey; 676 Respondents, August 2003*		

Is My Data Safe?

When you choose HyperOffice, you are assured that your data is secure regardless of what may happen to your personal computer, or even your company's network. Today, loss, theft, and virus attacks require companies and individuals alike to contemplate their own backup and security procedures. Even in this environment, HyperOffice has maintained 99.9% uptime. Should your personal computer crash, you may still access critical email, files, projects and contact information on any computer with a web browser.

According to Jupiter Research, 142 million consumers, or 65 percent of the online population, will have made a purchase online by 2007. 87% of those purchases are made using a credit card[1]. Large companies and individuals alike are learning that storing private information and using credit cards online is safe, provided they work with trusted products like HyperOffice.

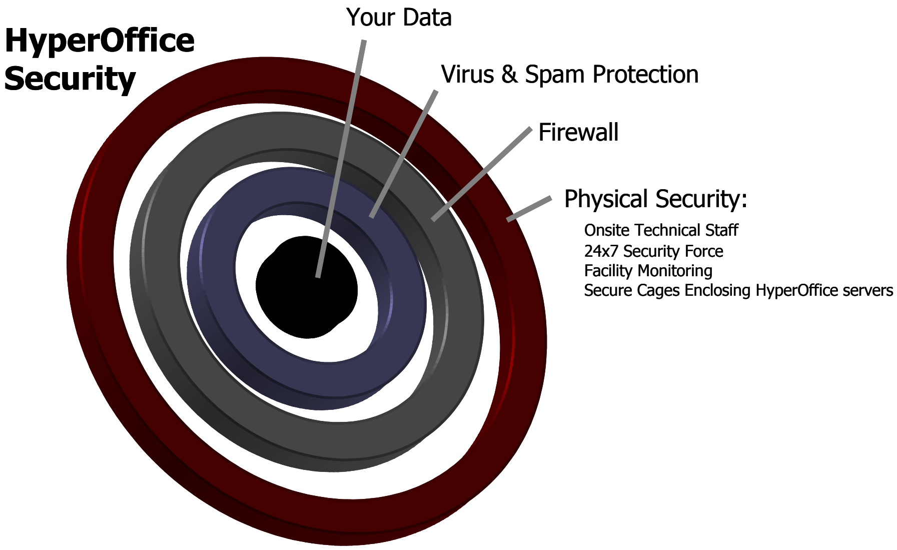
HyperOffice is far safer than storing private information on your own personal or office computer. According to a joint report issued by the Computer Security Institute and the FBI, there were 591,000 laptops stolen in the USA in the year 2001. Physical theft of laptops totals 11.8 billion dollars in the U.S., and according to the 2002 Computer Security Institute / FBI Computer Crime & Security Survey, the average cost of laptop theft to a company is $89,000.

What about Backup?

HyperOffice uses multiple redundant systems to backup your data on a regular basis, guaranteeing that your data and your company's information will be secure and never lost. There is no need for your company to purchase expensive backup hardware or software.

I'm overwhelmed with spam. Can HyperOffice help?

Yes. Today, one of the most common complaints about email is the exploding frequency of unsolicited messages, or "spam." In January of 2004, spam represented 60% of all email sent[2]. Such messages crowd an inbox, slowing worker productivity. In HyperOffice, your inbox is kept clean using industry-leading spam prevention that automatically removes unwanted messages from known "spammers". For added protection, we have also incorporated an intelligent filtering algorithm - *Bayesian filtering*. Users mark unwanted email as "spam" with a single click. Over time, HyperOffice develops a profile unique for each user, learning which messages are important and which are not. Bayesian filtering is the most successful way to *accurately* filter unwanted email, freeing you to spend more time reading and responding to the emails you actually value.



Is HyperOffice safe from Computer Viruses?

Yes. Viruses are small programs that can delete files, crash an operating system, or even use your computer as a tool for sending spam. In January of 2004, the "MyDoom" virus caused over $39 billion in economic damage alone[1]. HyperOffice puts an end to such worry. Our servers are constantly monitored, updated every 24 hours with the latest virus protection software. Thanks to such measures, HyperOffice has never been victim to an Internet virus attack.

Where is my data actually stored?

HyperOffice has partnered with NTT/Verio. With clients in 170 companies, NTT/Verio is one of the world's largest and most secure Tier 1 hosting companies. The NTT/Verio facilities provide the following:

- ✓ Certified Technical Staff Onsite
- ✓ 24x7 Security Force and Facility Monitoring
- ✓ Secure Cages Enclosing HyperOffice servers
- ✓ Fully Redundant Power, Backup Power, and Multiple Generators
- ✓ Early Warning Fire Detection, Gas/Dry Pipe sprinkler system
- ✓ Environmental monitoring system monitors air conditioning and humidity

What technology makes HyperOffice Safe?

We have implemented one of the industry's most rigorous security protocols to protect your data – and our reputation. Our data security strategy is based on three principles:

- ✓ Deployment of multiple levels of data security and backup.
- ✓ Use of the latest security practices and industry-leading security products.
- ✓ Regular reviews, analysis, and updates of HyperOffice policies and security practices to identify potential weaknesses.

HyperOffice has led the industry by implementing multiple levels of security. Your information is protected from other Internet users by way of user authentication, from hackers with industry leading firewall software, and from actual intruders through multiple forms of protection provided by our hosting partner, NTT/Verio, the worldwide leader in hosting and Internet security.

Secure User Authentication When you create a HyperOffice account, directly through HyperOffice or through your private branded company portal, your data is protected by your own unique username and password. Without both, your information is not accessible. Should you forget, misplace, or fear your password may be compromised; only you may change it – by answering a question to which only you know the answer. When this happens, your password is sent to the original email you shared when first setting up your account.

Nothing is more important to our employees than the security of your data. Should you fear your information has been compromised, HyperOffice support staff remains ready to answer any questions and take action.

Browser Security Whenever you close the Internet browser displaying HyperOffice, your data becomes inaccessible unless you re-enter your unique login ID and password. Even If you select a link to HyperOffice from your browser's history file, you must re-enter your ID and password.

Secure Transmission HyperOffice provides 128-bit SSL (secure socket layer) encryption; ensuring data is completely secure between HyperOffice and your computer. This is the same technology used by Banks and Financial institutions for highly sensitive online transactions.

Is my data private, even from HyperOffice employees?

Yes. HyperOffice employees must follow a strict policy on user privacy and security. Some regulations include:

- ✓ All HyperOffice employees must sign a strict non-disclosure agreement concerning user data. Violation of the agreement carries severe legal penalties.
- ✓ Passwords are never provided over the phone.
- ✓ Only select HyperOffice employees with top security access may access the physical servers, which house user data.

Contact Us

If you would like to try HyperOffice or if you would like to learn more about how HyperOffice can help your organization please contact us by email at sales@hyperoffice.com, call us at **1-800-434-5136,** or visit us at www.hyperoffice.com

Should you have any questions related to this white paper or our ongoing commitment to data security and integrity, please contact us by email at support@hyperoffice.com, or call us at **1-800-434-5136** & choose option2.

[1] Home Based Business. http://homebasedbusiness.biz-whiz.com/article333homebasedbusiness.html.
2 Greenspan, Robyn. “The Deadly Duo: Spam and Viruses, January 2004.” InternetNews.com. Feb 4 2004. http://www.internetnews.com/stats/article.php/3308091.