Google™ Apps for Business

5 myths about security in the cloud

Four million businesses are already using Google Apps for Business. It's helping them be more productive, improve teamwork and reduce costs. But some business owners still have concerns about security. And we understand. When it's your business on the line, you don't want to take any chances.

There are a lot of myths about security in the cloud. Here are a few worth busting:

Myth: Google will sell my information.

Fact: On Google Apps, your data will always belong to you[1].
Unless you use your services to do so, we do not share your data with other people (barring the very special cases covered in our privacy policy). In fact, we don't sell, trade or rent any personally identifiable user information[2] at all. Your information is your information - and that's the way it will stay.

Myth: If it's on the internet, it's more vulnerable to hackers.

Fact: Your data is safer in the cloud than it is in your office.
We protect your data in transit over the internet with SSL encryption. Our large information security team constantly monitors our global network of data centers to keep your data safe when it is in our care. Our admin and security controls passed a ISAE 3402 Type II audit and we are the first Cloud based messaging and collaboration suite to achieve US FISMA (Federal Information Security Management Act) certification. You can also choose two-step authentication in addition to a password to make unauthorised access much harder.

Myth: I'll never be able to get my data back if I change my mind.

Fact: You can export your data wherever and whenever you want it.
We'll keep your data for as long as you have an account with us - but if you do want it back, we have tools to help you export your emails, diaries, contacts, documents and sites. You can, for example, export your documents to various Microsoft-compatible formats. Find out more at Google's Data Liberation Front.

Myth: Google can read my email and documents.

Fact: Google cannot read your email and documents.
Google employees may not access the data in your account outside of extremely special circumstances for which we will still require your permission (See our privacy policy for details)[3].

Myth: Most businesses' existing systems are secure enough.

Fact: Not so much.
Our research has shown that most owners and managers of small businesses dangerously overestimate their current level of security. They don't have recent back-ups and don't secure them off-site (with Google Apps, data is automatically backed up in our global data centres, protecting it from accidental damage, loss, theft and fire). They don't have a disaster recovery plan for when things go wrong (we guarantee 99.9% uptime[4] and offer robust, built-in disaster recovery - better than most in-house hardware and software). And they don't encrypt their valuable data (with Google Apps, all data is encrypted in transit and access is further secured by two-step authentication, meaning data is far more secure in our cloud than it would be stored locally on a laptop).

[1]http://www.google.com/enterprise/apps/business/benefits.html?section=security#security

[2]http://googlepublicpolicy.blogspot.co.uk/2012/02/busting-myths-about-our-approach-to.html

[3]http://support.google.com/a/bin/answer.py?hl=en&answer=60762

[4]SLA Guarantee 99.9% availability with zero scheduled down-time

© 2012 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc.
All other company and product names may be trademarks of the respective companies with which they are associated.