BIZCOMMUNITY

10 tips for keeping your data safe in the cloud

By Steven Cohen

30 Mar 2015

If you choose a credible cloud software provider, it will host your accounting or payroll applications and data in a secure data centre underpinned by world-class technology. This will free you from doing backups, buying and installing new versions of the software, and fencing your data behind high security software.

Yet that doesn't mean you can neglect information security in your business. You'll still be using your own devices to access the cloud, so there are some security vulnerabilities you need to take care of on your side. Here are a few ways to protect your business from data security threats.

1. Choose the right provider

Buy cloud services only from reputable software vendors and Internet service providers. These companies will have put a range of processes and policies in place to secure their infrastructure and your data from information security risks. For example, our online solution, Sage One Accounting and Sage One Payroll, is hosted with Internet Solutions, who run one of the country's most secure data centres.

That means our clients can rest assured that their data will be secure, backed-up, and accessible - safe from hackers, weather disasters, theft, Eskom and all the other challenges you need to manage if you run the software on your own computers.

2. Educate your end-users

Educate your end-users about the basics of information security - for example, make sure they know why they need to choose strong passwords and that they're alert to the dangers of phishing emails designed to persuade them to give their log-in details to people with criminal intentions.

3. Install antimalware software

You should install antivirus and antimalware software on your laptops and desktop computers, and then keep it up to date with the latest definitions. This will help to protect you from malicious software programs such as Trojans and keyloggers. Such software can be used to steal information such as your log-ins for online banking or cloud applications.

4. Enforce strong passwords

Cloud services can usually be accessed through any device connected to the public network. You will authenticate yourself to the service with a username and password. Protect yourself by choosing a strong password that is difficult to guess, but easy for you to remember. It is just as important to change your password periodically. You must also take care not to let your password fall into the wrong hands.

5. Get serious about mobile security

It's great that you can access your accounting software or payroll through your smartphone or tablet, but there's also a risk attached to this. If you save your passwords on the device, anyone who steals your device or finds it if you lose it will be able to access your information.

Thus, be sure to lock your device behind a PIN code or password when not in use. Also, most mobile devices today allow you to track their location or remotely wipe data. It's a good idea to enable this functionality just in case the device goes missing.

6. Keep software up to date with security patches

When it comes to desktops and notebooks, be sure to keep your operating systems and browsers up to date with the latest security patches. These close off known vulnerabilities in the software, making your computer more secure.

7. Apply two-step verification

Where your cloud provider allows it, enable two-factor authentication. For example, you could set your account up to ask for a code sent to you by SMS when you log in or use a fingerprint in addition to a password. Thus, even if someone steals or guesses your password, they won't be able to access your sensitive data.

8. Be careful about where you log into cloud services

If you sometimes log into your cloud applications using public, borrowed or shared computers, make sure that you opt to not save your password and ensure you log out of your account after you are done. Also, if you're working with particularly sensitive data, be aware that public wireless networks are usually not secure.

9. Keep your passwords secret

Look after your passwords. Don't keep them in an easily accessible file on your computer or scribble them on sticky notes that you paste on your screen where everyone can see them.

10. Check the security certificate

Get in the habit of checking that any cloud sites you use have a security certificate in place. The certificate should be valid for the vendor providing the cloud service, should not be expired, and must be issued by a reputable certificate company.

ABOUT STEVEN COHEN

Steven Cohen is the MD of Sage One AAMEA (Africa, Australia, Middle East and Asia)
- Maximising business mobility in the economic downturn - 30 Jun 2016
- Cloud is the next big leap in the evolution of accounting software - 10 Jul 2015
- 10 tips for keeping your data safe in the cloud - 30 Mar 2015
- How the cloud helps SMEs tidy up the IT mess - 28 Oct 2014

View my profile and articles...