Is the cloud safe for consumers?

Written by Dan Conlon, Engineering Director, Trend Micro

It is almost impossible in today's world to turn on a computing device without using a cloud-based service, from Google Docs to World of Warcraft, and Facebook to Yahoo Mail, they are now so much a part of our everyday lives. However, while they offer lower prices, a massively improved user experience and in some cases entirely new and innovative services, there are risks involved.

Users under attack

The risk of your data being stolen by criminals is real and present. According to the Internet Crime Complaint Center (www.ic3.gov), the dollar loss from all cases of crime referred to law enforcement totalled $559.7 million in 2009, up from $264.6 million in 2008.

In data published by the EU statistics office, around three percent of internet users across the 27 EU states lost money due to phishing attacks or fraudulent payments. In fact, according to TrendLabs' own data, of computers scanned by HouseCall, one infected machine reports on average 6 viruses.

Cyber crime these days is big business. The days of the teenage amateurs launching viruses from their bedrooms for kicks are long gone. In their place are highly organized, well resourced and determined criminal gangs motivated by one thing alone: money.

The main way they'll try to make money out of you is by infecting your machine and quietly stealing your personal banking and other information using malware such as the infamous ZeuS Trojan. This information will then be bought and sold on underground internet forums. It's stealthy, it's dangerous and thanks to the ready availability of malware toolkits online, it's incredibly widespread.

There are many ways the criminals will try and trick you into downloading this stuff. Sometimes it is by persuading you to open a malicious attachment or click on a malicious link in an email which often looks like it has been sent by someone you know. Sometimes it is by spreading the same links via social networking sites. And sometimes it is by infecting legitimate websites and waiting for a visit from a user who has failed to keep their PC up-to-date with the latest security patches.

Aside from malware, there are also phishing sites which the criminals have constructed to look like real log-in pages from legitimate sites. They'll try and direct you to these sites with the intention of stealing your data. The challenge for users is that, with the exception of FAKEAV, such attacks are invisible.

Is the cloud safe?

It's important to remember that cloud computing is not as insecure as many people make out, and not necessarily less secure than your PC. The knee-jerk reaction is to want control over your own data and not have it stored away in some data center on the other side of the world. But the truth is that most reputable providers are accredited and audited to a high standard, spending millions on their IT and security systems to ensure your data is secure.

In many ways using the cloud is like riding a bicycle. Yes, there are potential dangers involved in taking your bike out on the streets, but if you wear the right protective clothing and headgear and are aware of the dangers around you, it should be no more dangerous than walking down the street. Similarly the cloud is no more dangerous than your regular PC environment as long as you take the right precautionary measures and act sensibly.

Below we have outlined some of the key dangers to watch out for and then some of the steps you can take to ensure you reap the many benefits of the cloud without exposing yourself to unnecessary risk.

However, there are still concerns over availability which plague some firms. Hotmail users have been struck more often than most. At the end of 2010, for example, over 17,000 email accounts lost all of their data. It took Microsoft three days to restore the data and there are still some complaining of missing emails. Then there are more extreme examples, such as T-Mobile which faced a consumer backlash in 2009 after it was revealed an internal employee had been selling on customer data.

There are also security concerns on the public-facing side of the cloud. Social networks and other sites are constantly being infiltrated by hackers keen to exploit the greater sense of trust people have on these sites in order to get you to click on to a malicious link or download a dodgy app which could end up stealing your information. Mobile app stores also contain risky software and jail-broken phones represent a particularly high risk

Risks of the cloud

- There is always the risk of outage, depending on the strength of the provider's back-end systems and your internet connection.
- Many people feel it is too difficult to completely erase their profile for sites such as Facebook once they leave.
- Users can sometimes leave their data exposed to all because they can't get to grips with the complicated privacy features on some sites.
- Increasingly, malicious mobile apps are being uploaded onto app stores.
- There is a slight risk of a cloud provider itself being hacked or suffering some kind of internal fraud.
- Users should be cautious when clicking on malicious links/downloading malicious apps on social networking sites.
- Criminals sometimes use brute force hacking of accounts, where automated password guessing software enables hackers to break in to accounts protected by weaker passwords.

Things to do

- Always check the terms and conditions on sites for how easy it is to leave an online service and have your data wiped from their systems, and familiarize yourself with privacy policies thoroughly.
- Don’t jail-break your smartphone because it could expose you to non-vetted applications.
- Be careful clicking on links, even if they appear to be from a friend. Be especially wary of shortened URLs.
- Check your accounts frequently, maintain strong passwords – such as those which use a combination of upper and lower case letters and numbers, and have different passwords for different sites.
- Perhaps most importantly, keep OS and browsers up to date with latest version as it’ll be the most secure. Keep them patched.
- Use a security provider who leverages a cloud-based security service as they can prevent you from following malicious links in social networking sites and emails, or visiting malicious web pages.

As we have seen, cloud computing has changed the way we live our lives for the better. It provides us with fast, efficient, easy and cheap access to emails, blogs, online gaming, social networks, all the latest mobile apps and much, much more. It helps us to safely back up our data and access it securely from any device. It allows us to manage, record and share our lives in new and exciting ways. Yes, there are risks involved, but if we take the right precautions then everyone should be able to benefit from this revolutionary technology.