Top 10 Ways You Can 'Epic Fail' in the Cloud:

What NOT to Do if You Want to Protect Your Data…

***Epic Fail.** [ep· ik feyl] – n. Complete and total failure, when success should have been easy to obtain.*[1]

When it comes to working in the cloud, epic failure is easily preventable, as long as you follow a few simple rules. This guide on what *not* to do is brought to you by a couple of guys who spent the last twenty years helping businesses protect their data by letting the good guys in, and keeping the bad guys out. We've compiled a list of the most common mistakes people make when dealing with online solutions, for a lesson in *what not to do,* so you can prevent data security breaches from happening to you.

1. **Sharing passwords and/or logins.**
   Sharing login credentials means that you never know who did what or when. There is no circumstance where this is acceptable…ever.

2. **Using weak passwords.**
   A weak password makes it easy for others to guess your password and gain access to your confidential data. It also introduces the same issues as sharing passwords or login credentials. Don't use your dog's name as your password if everyone knows your dog's name. And if you are currently using the word 'password' as your password, change it now. Right now. Use the whole keyboard, upper and lower case letters, symbols and numbers.

3. **Accessing cloud services from computers you don't control.**
   Public kiosks such as those found at hotel business centers, airport lounges, and public libraries all fall under machines that you do not control. Downloading, or even accessing, data in your storage cloud can be later recovered or viewed by unknown persons. So next time you are at the Apple store and want to log in and check your bank account balance… don't.

4. **Using weak security questions.**
   Choose your security questions and their answers carefully. With the rise of social media's popularity it is becoming far too easy to find your mother's maiden name and your high school mascot. Choose deeper personal items and be careful about what you share on social networking sites.

5. **Granting too much access.**
   Not everyone in the company gets a key to the front door. Usually this is reserved for managers who open and close the office, not the part time intern or summer helper. If you have an employee who just needs access to some marketing collateral, you

[1] Source: UrbanDictionary.com

wouldn't give her access to filing cabinets where HR documents are stored. The same logic applies to online document access. And remember, just as you collect a person's keys to the office upon termination, you should also ensure that you remove their access to your cloud services provider.

6. **Ignoring routine updates and patches.**
   Just like maintenance you do on your car every 3,000 miles, there is maintenance you should do on your PC to make sure it's well-serviced. Nearly every month a new set of operating system and application patches are released from the vendor community. These should be applied in a timely manner to keep your PC, just like your car, running smoothly and safely.

7. **Being lax with virus/malware protection.**
   An ounce of prevention is worth far more than a pound of cure. Don't be a Typhoid Mary, be sure to get vaccinated. Use malware protection from a reputable vendor, and like your operating system and applications, be sure to keep them regularly updated. Those booster vaccines are around for a reason.

8. **PC sharing.**
   It is highly advisable that you keep work computing and personal computing separated. For example, accessing work files from your cloud storage provider from the same PC on which your children play games is generally a bad idea, as a lot of those 'free' downloads kids (and some adults) try can be attack vectors exploited by malware writers (aka, "bad guys"). So, unless you're ready to set down some stricter rules for access (separate logins, monitor activity, etc.) it's best to keep work devices separate from the family fun PC.

9. **Accessing services over HTTP**
   Only use HTTPS to access any of your data or files stored online. Otherwise, you run the risk of exposing your password, along with any potentially sensitive information, to strangers. This is especially important to consider when using public Wi-Fi hotpots such as those at your local coffee shop or airport terminal. The easiest way to tell if you are accessing via HTTPS? Look for that little lock icon at the bottom of your browser.

10. **Blowing off the "fine print."**
    Just like you are wary of a blind date, regardless of your friend's intentions, always look for 3rd party validation of your cloud provider's commitment to security. You have the right to know what security controls are in place before you blindly trust your data to any cloud services provider. If you find a security statement on their web site that looks like it was written by a team of lawyers, call your provider and ask them to explain, in plain English, how your data is stored, how secure it is when it's in transit and what the provider does to back up your data.

Meet Brandon and Michael

Brandon Dunlap, Managing Director – Brightfly
Brandon has more than 15 years of experience managing business technology risk in large and small organizations. He has served in a variety of roles across heavily regulated industries, successfully leading all aspects of IT security programs, including policy and procedure management, oversight and control, strategy, architecture, development, and training. Follow Brandon @bsdunlap

Michael Webb, Chief Technology Officer – SmartVault Corporation
SmartVault provides businesses and accounting firms the ability to store and share business documents securely online. As Chief Technology Officer, Michael is responsible for the design and delivery of SmartVault's Software-as-a-Service (SaaS) platform, managing the R&D group at SmartVault, and ensuring the overall security of SmartVault's platform. In addition, Michael is a founding member of SmartVault. Drop Mike a note at mwebb@smartvault.com

To continue the conversation about how you can work in the cloud without biting yourself in the a**, check out our security and compliance resource center.