Is the Cloud Secure Enough for Me?

Presented by Joe Lamoglia, ChFC®

Have you ever used Dropbox or Box.com? How about web-based mail, like Gmail, Yahoo! Mail, or Hotmail? If you consider that all of these are clouds—as are most Google apps—it's hard to find an Internet user who doesn't have *some* information in the cloud.

As cloud-based services become more prevalent, you might be wondering: Is the cloud secure enough for storing and sharing my own information?

Cloud security implications

The perks. Before we dive into the risks involved, let's start with the perks of using a cloud:

- Your information is accessible from anywhere you have an Internet connection.
- You can easily share files with others.
- You don't have to worry about managing external hard drives, USB sticks, or other storage hardware.

The potential drawbacks. On the other hand, when you give your information to a cloud provider, you're ceding a good deal of control of that information.

- You may not know exactly where that information will be stored or how it will be secured.
- The perk of easy accessibility from the Internet for you is also true for attackers. If a criminal were to guess your password, he or she could potentially gain access to your information.

In the end, we do have to trust *something* with our information. And many cloud providers try to stand out by practicing sound security. So, if you've made the risk-based decision to move your information to the cloud, be sure to look out for the security features described below.

Cloud provider security features to watch for

1) Multifactor authentication. This extra layer of protection can help make your login process much more secure. Multifactor authentication is a system that requires a second form of verification in addition to your password, such as:

- A passcode that you receive on your smartphone
- A digit that you press after receiving a phone call

This ensures that, even if your password were compromised, an attacker couldn't access your account because he or she wouldn't have that second piece of identifying information.

2) HTTPS connection. Check the beginning of the URL you visit to access your cloud.

- If you see **https://**, all your information will be encrypted while it's in transit between you and the cloud. An attacker trying to intercept your connection won't be able to see the information.
- If your cloud—or any website, for that matter—begins with **http://**, keep in mind that any information you transmit could potentially be compromised. In this situation, we'd strongly recommend finding an alternative.

3) Encryption at rest. Not only should your information be encrypted in transit (https), but it should also be encrypted at rest—while it's sitting in the cloud. That way, if anyone were to get access to that information, he or she would still need your password in order to make any sense of it. (Encrypted information appears unreadable when it hasn't been decrypted by its encryption key/password.)

4) File version history. It's always possible that something can go awry when syncing or making changes to files in the cloud. A service with *versioning* allows you to dig back into the various revisions of a file over time and choose to restore an older one if needed. This can be a life-saver in terms of protecting your information, especially in cases where information is accidentally erased or files are corrupted.

The forecast is looking cloudy . . .
Years ago, the idea of entrusting your information to someone far, far away in a place you couldn't even see would've sounded ridiculous. But today, many Internet users are migrating their information and services to the cloud for cost savings, ease of use, and security benefits.

In the end, careful research can make all the difference. Deciding which service to trust is the most important part of the cloud that's in your control.

Joe Lamoglia is a financial consultant located at Potomac Financial Private Client Group, LLC, 6723 Whittier Ave., Suite 305, McLean, VA 22101. He offers securities as a Registered Representative of Commonwealth Financial Network®, Member FINRA/SIPC. Joe can be reached at 703.891.9960 or at joe@potomacfinancialpcg.com.