Is Your Family Data Safe?

Tony Bandy looks at strategies for protecting your cloud-based data from intruders

© Oez, from Fotolia.com/Adobe

STOLEN IDENTITIES. HACKED PASSWORDS. FINANCIAL DATA GONE missing. One of our biggest fears today is keeping our online data safe. But did you ever stop to think about the security of your online ***family data***? These days, many of us with family history research keep it online, either through specialized genealogy services or online-hosted storage with the likes of Apple, Google, Microsoft or others. Yet this type of data is just as vulnerable as our passwords and financial accounts if not protected properly.

Is there anything we can do? Are there safer online ways to use and store our family history data? While nothing is ever completely foolproof, I've put together a quick list of things to know and a baseline checklist that you can use when thinking about securing this type of information. First, let's start by examining some online security issues.

Security Considerations

One of the first things you need to do before purchasing or using any online service is be aware of the ways in which your data is held. The three factors include:

- Your data held locally on your network and devices
- Your data in-transit to your service of choice
- Your data held by the service itself

Let's take a quick look at what each of these means.

Data on Our Own Networks & Devices

Most security experts all agree that local storage of data and information is a flashpoint of potential problems. End-user security is a big deal and something to be aware of. How secure is your machine and software? What are your everyday computer-using habits? Do you keep your machine up to date with BIOS flashing and operating system updates?

Do you keep your family data on a separate drive, away from the main computer hard drive and operating system? Have you upgraded your house Wi-Fi? Have you checked it to see if it is locked down to prevent strangers from accessing your network (and data)? When was the last time you checked your telecommunication providers's router (or your own)? Knowing this is the first step towards safe data use.

Your Data In-Transit to The Service

The security of our genealogical data in-transit to our chosen service simply means, "How is the data secured from your personal devices to the final point at the online service?" Is the data encrypted before it leaves your machine? Is the encryption level high enough to prevent hackers from easily breaking in? When your information flows from your Internet provider through the Internet itself, how many machines does it go through – and is the encryption at that data level high enough as well? If secure routing is enabled, are the security certificates up to date and strong enough to deter hackers? This is the second step you need to take.

Data Storage @ The Service Level

The last step to think about is how your data is stored and used at your online service of choice. Does it reside in separate server farms away from any Internet-facing public websites? Do employees have access to your data? Where is your data stored? Another country? Locally within your country of residence? Is it kept in encrypted formats? Are your accounts password protected? Are the security certificates held by the service up to date and at the correct encryption levels they should be?

Your Security Checklist

Given the above questions, if you are considering any online family genealogy or storage service, it pays to put together a comprehensive planning document about how to secure your personal and family data. For myself, this involved sitting down at my desk with a blank sheet of paper and writing out where my data was stored now, what I was going to need in the future, and then what cloud-based services and sharing options would work best. Doing a bit of mind mapping with these questions, I was able to put together my own personal security checklist.

If you haven't yet done this, then you should. Hackers and thieves are out there, and any cloud-based data has the potential to be at risk. Take a few moments and create a planning document, or checklist, and think about all the places you currently have your family data. Ask the hard questions and don't forget to factor in things that you might do in the future, such as mobile genealogy search from local history sites, gravestone research or libraries. This can influence the purchase of any service you decide to use. Make up your own security questions or consider the following as baseline options to help you in this process.

© magraphics, from Fotolia.com/Adobe

Your Baseline Data Security Needs:

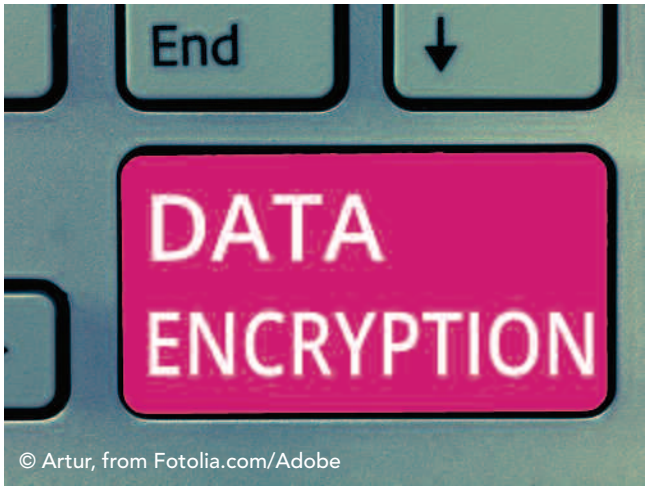
(A) Your data. What types do you already have and how much storage does it need? Consider multiple drive setups for security (RAID). This link can help if you are a Windows 10 user: ***www.windowscentral.com/how-use-storage-spaces-windows-10.***

(B) For your local storage, do you have a backup strategy? Multiple drives, safe deposit box off-site, etc.? See this link for details: ***www.howtogeek.com/242428/whats-the-best-way-to-back-up-my-computer***.

(C) Is your data encrypted if held in local external or USB-based drives? If you are using Microsoft as your operating system, consider BitLocker (***http://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview***) as a starting point. If not, look online for safe encryption software to secure your data. Ensure it is from a reputable source or find other genealogists who have had success with this previously.

(D) If your data is on a laptop or other mobile device, what security measures have you put in place to prevent it from being stolen? See this link for tips: ***http://med.stanford.edu/irt/security/protecting/laptops.html***. Also remember to never leave your computer equipment unattended, regardless of how safe you think the situation is. Thieves work best when they know our guard is down.

(E) When was the last time you updated your computing device? Regular updates to the software operating system and hardware level BIOS (***http://en.wikipedia.org/wiki/BIOS***) are essential these days. Contact your device manufacturer for details if you are unsure. Quite often, hackers find the end-user data much easier to break into than online or in-transit data because of the lack of these updates.



© Artur, from Fotolia.com/Adobe

Your Data In-Transit Essentials:

(A) For any service you are considering, is the connection to the service encrypted? Is there the ***https***: symbology and the lock icon in your web browser tool bar? See these links for changes and background information: ***http://security.googleblog.com/2016/09/moving-towards-more-secure-web.html*** and ***www.searchenginejournal.com/google-is-requiring-https-for-secure-data-in-chrome/183756***.

(B) As a follow-up, is the encryption level used by your service a newer form of the encryption known as ***SHA-2***? See this link for additional information: ***www.csoonline.com/article/2879073/encryption/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html***. If your provider has not yet updated to this standard, this should raise your concern. See this link for a description of this encryption level and what it means: ***http://en.wikipedia.org/wiki/SHA-2***.

Data Held Online Considerations:

(A) How much do you need to put online? Consider sharing only the essential information. Sharing is good, but given the rampant rise in identify theft, etc. perhaps less is better? Go over your current accounts you already have in place and consider removing non-essential data or closing accounts you no longer need. Try this link for a bit more background: ***www.csoonline.com/article/2134092/network-security/social-engineering—how-over sharing-information-can-lead-to-disaster-online.html***.

(B) Is my data encrypted while on the service's network? See these links for more information: ***http://digital guardian.com/blog/data-protection-data-in-transit-vs-data-at-rest***. This is a good thing if possible.

(C) Does my family data reside offline or in a different location that the main server? In other words, if possible, make sure your data is not on the main server(s) that host the service's website. This way if the site goes down either via hardware fault or hack, your family data stays safe.

(D) How are day-to-day security operations performed? Do staff have access to or can read your personal data and/or photos? Hint: They should never have access to this unless authorized by you or the person you designate. What information can you ask about via FAQ or customer service about how their network is configured?

(E) Where does your data reside? Is it in your home country? Given the vastly differing international laws on government access to consumer data, this should be a factor. See this link for background story: ***http://thehackernews.com/2018/02/icloud-data-china.html***. Although geared for business, this link is very informative about these practices: ***www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located***.

(F) At what encryption levels is your data stored? While somewhat technical, the following link can be useful: ***http://cloud.google.com/storage/docs/encryption***.

While no service can ever be completely foolproof, you are the paying customer, so it's in your best interest to find these things out if possible. Most services, be they genealogical in nature or otherwise, should make this information known to you up front. A good example of this can be seen in Google's online FAQ about how they store your personal data: *http://privacy.google.com/your-security.html*. An example for data access rules used by FamilySearch.org for developers access to data can be found here: *www.familysearch.org/developers/docs/guides/private-spaces*.

Look for online FAQ (frequently-asked-questions) or send an email directly to customer service asking these things if you cannot find them online. If you do not see any mention of this or are rebuffed by customer service, be cautious!

Further Reading

So far in this article, I've shared questions to ask, how basic online security works and then some best practices and links that you can use when using and considering both sites and services. However, this is just the tip of the proverbial iceberg of the knowledge and skills that you need to be aware of. For a bit more help, consider the following outbound links to get started.

- Cloud Computing and Security (Wikipedia Overview): ***http://en.wikipedia.org/wiki/Cloud_computing_security***
- Dick Eastman's Privacy Blog: ***http://privacyblog.com***
- Federal Trade Commission, Online Security Information: ***www.consumer.ftc.gov/topics/online-security***
- Lehigh University Guide to Evaluating Cloud Services: ***http://lts.lehigh.edu/services/explanation/guide-evaluating-service-security-cloud-service-providers***
- Online Photo Privacy Issues: ***www.makeuseof.com/tag/exif-photo-data-find-understand***
- Security Considerations from the National Cyber Security Alliance: ***http://staysafeonline.org***

Final Thoughts

Let's face it: The Internet is both a strange and wonderful place. One minute we find online clues about our family's heritage, and the next we found out we've been victims of an online hack. It can drive one crazy! However, the solution is not to give up on what many of us have found to be a great resource for our families, but instead become wise by asking questions, planning, and then following a set of basic practices that we can use across all the sites and services we access. Investigate, have fun, but stay informed!

TONY BANDY is a regular contributor to *Internet Genealogy*.