West Virginia Executive Branch
Privacy Tip

This week's tip is brought to you by www.sans.org. Reprinted with permission.

January 2020 • The Monthly Security Awareness Newsletter for Everyone
Digital Inheritance



Overview
Have you ever thought about the uncomfortable question, What happens to our digital presence when we die or become incapacitated? Many of us have or know we should have a will and checklists of what loved ones need to know in the event of our passing. But what about all of our digital data and online accounts? Should we consider some type of digital will? Should we create a "digital inheritance" plan?
Think about your digital presence. Bank and retirement accounts, home mortgages, family photos and videos, smart home accounts, email, and social media are just some of the many examples that make up our digital footprint. In the event of your death or the death of a close family member, family and loved ones may need prompt access to those accounts or data. In addition, legacy data and online accounts left behind could become vulnerable over time to hackers, thus placing family and friends at risk.

Creating a Plan
It is a good idea to discuss your desires with your trusted family or friends, like other end-of-life details. In addition to having these conversations, take inventory and document your digital assets and online accounts. If you do not provide access to your accounts after you die, it can be very difficult for family members to access or close them. For example, would you want your family members to be locked out of all those years of family photos and videos you have stored online?
One idea is to document your online presences in a password manager. This is a program that securely stores all your logins and passwords, credit cards, and other sensitive information. It's designed to make creating, storing, and accessing passwords and security questions vastly simpler. In many ways, this is a powerful tool to catalog your digital presence. With many password managers you can even configure them to share all or certain passwords with other trusted family members. If you are uncomfortable with that, document access to your password manager and seal that in an envelope; then have that sealed envelope opened after your passing by an executor or trusted family member. This way, they will have access to your password manager and be able to access your accounts and information stored in there.
In addition, some sites provide the option to identify legacy or trusted contacts. Facebook, for example, allows participants to determine in advance if they would like their account deleted or memorialized after passing. Memorializing creates a space that's only visible to existing friends, where memories can be shared. Finally, you may want to consider dealing with a lawyer or estate planner who specializes in digital inheritance.

Inheriting Digital Assets
You may find yourself in the situation where you have to recover or access the online accounts of a recently deceased friend or family member. We recommend you first coordinate with a lawyer and other family members before taking action. Other family members could quickly become upset if they see you taking action without consulting them first. Then start with identifying any passwords you can find. Did the family member write them down or store them anywhere? If that is not an option, can you access any computers or mobile

devices they used and are still logged into? If not, you most likely will have to reach out to each site for access to the deceased member's account. This often includes having to provide both a death certificate and proof you are directly related to the family member. In some cases, you will not be able to access the account or data stored in the account but only delete it. Every site handles these situations differently, which can be a time-consuming process.

In today's digital world, we should not only consider physical assets but also digital assets in our future estate planning.

Subscribe to OUCH! and receive the latest security tips in your email every month. Do you think you've got what it takes to get into the cyber security industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

---

Resources

Password Managers

Making Passwords Simple

OUCH! is published by SANS Security Awareness and is distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.