
# The Monthly Brief

Volume 5 Issue 4 April 2017

## Passing On Passwords

No one likes to think about this but what would happen if you weren't here tomorrow?

In the past family members could locate important information in a file at your home. But have you stopped to consider just how much of your important life information is now digital?

Banking, insurance, business, real estate and even vehicle titles are all maintained online. What about all your photographs, videos and even social media accounts?

But writing down accounts, passwords and login information is a risky practice.

A better way is to keep your passwords where loved ones can only access them under certain circumstances. There are both online services and software that help you do this, and some tools that give you a lot of control.

These services will act like digital safety deposit boxes where you can upload documents, photos and other information that your loved ones need to have, including passwords. To get your files, the loved ones you specify will need to meet the standard you designate. Some services also allow your heirs to get the information if you're incapacitated.

We don't endorse any company and you should carefully investigate before doing business but examples are Estate Map, Assets In Order and Everplans

**WWW.SA18.ORG**

Subscribe: philarcher@sa18.org

## HAVE I BEEN PWNED?

**Pwned** is slang for the word 'owned' and refers to being taken advantage of. The **'Have I Been Pwned'** site reveals if your email address was among lists of those leaked during recent security breaches at major companies such as Adobe, Dropbox and LinkedIn.

Typing an email into the site reveals which, if any, breach affects you or if it's been detected on the "dark web" where private information is made available to cybercriminals.

To search these pwned sites, type in the email address on the site's homepage and hit enter. If the address is discovered on one of the leaked lists, the screen will turn red and give you more information on which data breach was involved.


If the email address is not found on any pwned sites, the screen will turn green. Users of the site can choose to sign up to be notified if their email address ever appears online.

## Facebook Like-Farming

Have you seen posts saying you can win a free car, vacation or some large sum of money? All you have to do is "like" and "comment" on a picture and then share it on your wall. You're skeptical but since it only takes a few minutes you complete the steps just in case it's legit.


These social media hoaxes are known as **like-farming scams.** Based on the way Facebook works, the more likes and shares a post has, the more likely it is to show up in people's News Feeds.

This gives the scammer more viewers for posts that boost their Facebook status, create targets for spam and phishing attacks or to insert malicious downloads aimed at later visitors to the page.

Remember once you've "liked" a page on Facebook, the person who runs the page receives a notification and can view your profile, any publicly shared information including your friends list. This can lead to them being targeted as well.

Don't get tricked into helping promote a scam and avoid giveaway prize posts. Review your Facebook Privacy settings to find out how much information you are sharing publicly and make changes as needed.