Password SAFE

Are You Frustrated with Too Many Passwords?

Every E-commerce website wants you to set up an account, which is controlled by a password. Then there are the sites you visit to manage your finances, pay your bills, and read your Email. The list never stops. You probably have dozens or even hundreds of online accounts.

If you use one password for all hosts you login to, or for all E-commerce sites, or for all financial websites, you make yourself vulnerable. If one of them has a security breach, the attackers will have your password for many sites.

If you use a different password for each host and website, however, you have a memorization problem that would challenge a professional mnemonist. You can just memorize a handful of accounts you use most often. But then, you waste time resetting your password every time you want to access the other accounts.

Do You Solve This Problem by Writing Down Passwords?

Cyber security experts control access to system with three types of information: what you know, what you have, and what you are. A password is an example of the first type. But if you write your passwords down, they become what you and potentially others know. It doesn’t matter whether you put them on sticky notes on your computer monitor, in a notebook you keep in your purse, or on a paper you keep with your laptop. Once they can be read, they aren’t just what you know, but what someone else might know.

The solution to password overload is the Password Safe™. You enter one PIN number and have instant access to up to 400 accounts. You’ll never forget another password again and never have to reset another password.

Password Safe™ is the Solution

The Password Safe™ has a large back-lit LCD screen and a full QWERTY keyboard. The PIN passcode can be any combination of 4 to 16 digits. You can enter the name of the site or host, the user ID, the password, and optional notes for each account.

To look up the user ID and password for a given host or site, just enter the site/host name in the search function. You can also scroll through your accounts using the directional buttons.

The Password Safe™ automatically locks for 30 minutes after 5 consecutive incorrect PIN attempts. If it has been inactive for 3 minutes, it will sleep to protect your passwords and preserve the life of the 3 AAA batteries.

The menu allows you to select View, Add, Edit, Delete, or Settings. The last choice allows you to turn the Sound on and off, change your PIN passcode, or change the Auto-off time.

One of the most important security features that the Password Safe™ offers is what it **doesn’t have**. It doesn’t have any form of network connectivity. In order to see the passwords that the Password Safe stores, you must physically type in your PIN number and read the display. What isn’t connected can’t be hacked, unless the attacker has physical access to your premises.

Advanced Model

The Password Safe Plus™ has two important improvements over the basic model. The first improvement is a standard slot for a laptop cable lock. So, you can physically attach the Password Safe Plus to your desk, and not have to worry about having it “walk away.” This makes it much more suitable for use outside the home.

The second improvement is a slot for a micro-SD card. If you are going to save the passwords that control access to every aspect of your digital life on a device, you need a way to back up those passwords. With the original model, all you could do if you forgot your PIN number was clear the memory. If you insert a micro-SD card into the device after it is turned on, it will write a file of your passwords to the card. The file is encrypted using advanced AES 256 encryption to ensure that your passwords are safe. If the Password Safe Plus™ is turned on with the SD card already inserted, it will read the file of passwords back into the device.

Case Study #1

I’m an information security professional. My dad is in his mid-eighties. I convinced him that he should have long pass phrases to secure all of his many online accounts.

Recently, he called me to complain that he was having trouble accessing his online accounts, because he couldn’t remember the passwords. So, I bought him a Password Safe and told him that it was the solution to his password problems. I told him to put all of his passwords in it, and put his PIN number on paper in his security box at the bank.

Then my dad had a stroke and I had to take care of his finances. Fortunately, he had taken my advice. I got the paper out of the security box, and to my great relief, the Password Safe had all of the accounts and all of the passwords I needed to access. He had even put the answers to his backup security questions in the notes section for many accounts. I managed his online banking, paid all of his bills online, and even monitored his investments. The Password Safe was a great help to me in caring for my dad while he was unable to care for himself.

Case Study #2

I’m the CISO of our company. One of our competitors suffered a well-publicized breach last year, which resulted in major financial losses. One of the root causes for the success of the attack was an easily guessed password for a privileged account. So, based on input from the auditors, our board has pressured our CIO to aggressively enforce password rules.

We issued a Password Safe Plus™ to all of our employees. We made it policy that they must put all passwords that they use at work in the device. Once a month, an IT employee comes to people’s offices and dumps the contents of the Password Safe Plus™ to a memory card. Also, once a month, we run a sweep of every server and workstation. It collects the usernames of everyone who has access to each system. We check that the owner of every account listed really needs access to the system in question. The accounts are sorted by employee, and compared to the results of collecting the passwords from each user. Any account on a host which does not correspond to the user’s Password Safe Plus™ is immediately locked out.

What we find with our password procedures is access creep and policy violations. However, we also have found what we believe were two early stage Advanced Persistent Threats. The Password Safe Plus™ helps protect our shareholders’ assets.

Copyright © 2017 RecZone LLC