Sticky Notes

That Impenetrable Fortress for your Password might not be that secure…

Howard Globus

IT on Demand

In the modern world, passwords are required for everything. For added security everything should have a unique password, as we've been advised by professionals and pundits. We need a way to create unique, complex passwords and manage them. As a home user this is important but as a business owner password management is deemed a critical risk point.

Taking a step back, you may ask "Why do we care about passwords and password management?" Studies done every year have shown that password security is perhaps the biggest threat to an organization or family's online and financial security. That may sound like an extreme statement. However, if you consider that stolen and weak passwords are responsible for over 80% of the security breaches, you can see that this is an area where we really need to figure out how to alleviate this vulnerability.

Where Does This Information Come From?

To give a bit of background and history, in 2015, the Federal Government's Office of Personnel Management was breached and the personnel data of over 22 million current and former employees was released. This information was not limited to names or addresses, but also social security numbers, drivers licenses, and in some cases, password information. The background check details of 19.7 million individuals was breached, along with data related to 1.8 million non-applicant spouses or cohabitants, and 5.6 million fingerprint records.

Imagine a database as group of spreadsheets with each tab of the spreadsheet a group of indemnifying information (like "first name", "last name", "address") in columns across the top and rows down the side with individual's information filling out the specific information.

A database's information is often stored in several different layers. To extend the analogy think of the different layers or tables as another tab on a spreadsheet. One tab might contain only a table with an identification number—something known as a "key record" – and a name. Other tabs of the databased may only be identified with this number or key record. Without that topmost layer, it would be difficult to know what social security number is connected with which person in the database. We call this a "relational database." The key record is literally the key that unlocks the treasure of the database's information.

What made the Office of Personnel Management's breach so significant is that these "key records" were obtained. For employees of the federal government, background checks are extensive, so this database contained massive records of each employee's life, replete with information they were required to submit in order to be issued security clearances. Beyond names, addresses, telephone numbers and personal social security numbers, it also included things like spouses' names, children's names, and parents' names, dates and places of birth… as well as every address at which the employee has ever lived.

Consider if you've ever had to reset a password or had a clue listed on a website where you have forgotten your login details. Most websites and financial institutions offer ways for you to access your account through "security questions". When armed with bits of critical personal information hackers can leverage the stolen data to reset account passwords for every email address ever used. This in turn can allow them to confirm password changes on other sites like American Express, Wells Fargo, the Small Business Administration, amongst other sites.

To round out this line of attack, when a database holding sensitive information like usernames, passwords, current address, mother's maiden name, and date of birth is paired with a list of all your previous addresses and spousal information, the hacker is no longer stymied by a security question like "What street did you live on in the 3rd grade?"

How to Protect Yourself

What does a password management system do to protect you from this? People tend to use very simple passwords. The most used password in 2019 and 2020 was "password." Further, people often use the same password for their banking app, mortgage app, and even their children's remote-learning platform. Why? Simply put, if there is a complex password in use, using it in multiple places makes it easier to remember. A password management system allows you to remember the "one password to rule them all" while still maintaining highly secure passwords that are unique to each site.

If we start with the belief that every website and application should have its own unique and complex password, the question that naturally follows is "How the hell do I remember them all?

Short of writing passwords on a sticky note and putting them under your keyboard—which is done more often than you may imagine—there is another way. Using more complex passwords of 10, 15, even 20 characters with a mix of uppercase, lowercase, and alpha-numerics becomes much easier when stored in a password management system. You then only need to remember one master password to gain access to all the others.

With the number of websites and tools online and on our computers we may use tens and even hundreds of unique passwords once a month, once a quarter, once a year, or once every five years. For example, I created a password to sign up for my daughter's student loan, then four years later when I had to sign up for my son's student loan, I had no idea what that earlier password was. I had only used it once.

When using a password management tool, that system doesn't care how complex each password is. Whether it's five characters or 50, we only have to worry about remembering the master password and setting the rules of complexity for any passwords stored in the system. You can even use a pass-phrase which may be a common line of dialogue bantered about between you and your spouse, as long as it meets the rules you've established.

Even if your vital key record information is compromised, this additional step makes it less likely that your various accounts can be hacked.

Sometimes It's Okay to Lie

You can also protect yourself by adapting your responses when setting up security questions/answers. For example, rather than using your mother's real maiden name, you could use your mother-in-law's maiden name. For me though, I go even further and use a completely fictitious name. But I don't have to remember what it is, because I have it stored in my password management system.

Likewise, you don't have to use the real city of your birth, or the city where your parents met, or the year you actually graduated high school. Instead, use the password management tool to save not only your various complex and secure passwords, but also the specific answers used for security questions.

Again, even if your key records get compromised in a massive data leak at a state or national level, if your answers to security questions were fictitious, it is an added level of obfuscation and makes it more difficult to have your passwords reset without your knowledge or consent.

What Else Can a Password Management System Do?

Another feature of a password management tool is the ability to change a large number of passwords quickly. If someone leaves or is fired from your company, you can change all the passwords that person had access to within your business. From an audit standpoint, you can access forensic information to learn who logged in using what password and when. Even if you use a shared password amongst a dozen people in your company, you can track usage at the individual level. You can also scan the dark web to see if those passwords are in use, and to what extent.

Use It or Lose It

Password Boss is a password management tool that stores encrypted credentials on a cloud-based service where you retain the key to unlock the system. It has plugins that can be used on multiple operating system platforms and all major web browsers that doesn't compromise its security for ease of use.

One of the key features that sold me on the product was the ability to create an offline master password that can be used to unencrypt the data. Why is this so important? Password Boss, as a company, will not retain a master key to your encrypted data, which is what makes it secure and a preferred solution. Only you have access to your stuff.

I feel so strongly about this product I've struck a special arrangement with Password Boss to offer readers free month's trial. Go to **https://keepmesafe.club/password** to claim your gift now.

Please, please, please…

Whatever you do, do not write your master password down on a sticky note and put it on your monitor!

Security Evangelist Howard Globus has more than twenty years of experience designing, installing and supporting Windows server and workstation products in industries where security and reliability are critical. System engineering and administration experience includes customized Windows Server and Workstation installs, designed to be deployed using the latest automated technology available and managed using products found onsite at most Fortune 500 firms to ensure a wide variety of potential personnel to support the products in the future.

www.it-on-demand.com