Keeper Security Special Edition

Password Management

for dummies®

A Wiley Brand

Protect yourself from cyber criminals

Secure your online accounts and assets

Learn best practices for password management

Compliments of

KEEPER®
Cybersecurity Starts Here™

Brian Underdahl

About Keeper Security

Keeper Security helps businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft and increase online productivity. Keeper is SOC 2 Certified and utilizes best-in-class encryption to safeguard its customers.

Password Management

Keeper Security Special Edition

by Brian Underdahl

for
dummies®
A Wiley Brand

Password Management For Dummies®, Keeper Security Special Edition

Publisher's Acknowledgments

Table of Contents

Introduction

Cyber crime such as theft and data breaches is increasingly putting both individuals and businesses at risk. Unfortunately, the method most often used to protect accounts — passwords — is the #1 cause of data breaches and cyber theft because using high-strength passwords often seems too difficult, frustrating, and error prone.

Individuals and businesses often deal with the password issue by using shortcuts. For example, they choose simple passwords that are easy to guess, they use the same password for every online account, or they write those passwords on sticky notes stuck to the side of their monitor. Such methods may seem like an easy way to avoid the work of creating and using secure passwords, but they make it easy for cyber criminals to do their damage. Clearly, people need a far more secure and convenient way to protect their online accounts and other online assets.

About This Book

Password Management For Dummies, Keeper Security Special Edition, shows you what you need to know about password management systems that can greatly improve your online security. This book shows how the right system can help you easily use extremely strong passwords to protect yourself and your assets without requiring extra effort or adding complications to your online life.

Icons Used in This Book

This book uses the following icons to call your attention to information you may find helpful in particular ways.

The information marked by this icon is important and therefore repeated for emphasis. This way, you can easily spot noteworthy information when you refer to the book later.

TIP

This icon points out extra-helpful information.

TECHNICAL STUFF

This icon marks places where technical matters, such as jargon and whatnot, are discussed. Sorry, it can't be helped; it's intended to be helpful.

WARNING

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Where to Go from Here

This book is designed to be modular. Although everything in this book is important and interesting, it's laid out so that you can jump to a specific chapter and gain some useful information quickly if you don't have the time right now to read everything. You'll probably want to go back later and read any chapters you skipped to make sure you don't miss any vital information, though.

As much as I try, it isn't possible to cram all the information you'll need into the limited space I have in a book of this size. For the latest news and information, please visit `https://www.keepersecurity.com/`.

Chapter **1**

Introducing Cyber Theft and Hacking

Cyber theft and hacking are making the online world a dangerous place. This chapter looks at the risks you face and considers some of the ways you can be attacked. Understanding these issues will help you to see how important it is to protect yourself and your business.

Understanding Your Risks

The number, size, and cost of data breaches and cyber theft is rapidly increasing. It doesn't matter whether you are an individual or a business — cyber criminals are out to get you.

Unless you're a computer security expert, you may simply not be aware of all the ways that you're at risk. Consider the following:

» **Legal liabilities:** If you run a business, you are responsible for protecting customer data including personal information, credit cards, and sensitive information such as products purchased. In most jurisdictions, the business, not the customer, is responsible for any costs resulting from a data breach.

- » **Lost business:** Companies that experience data breaches often struggle with trying to keep their customers. If people don't feel that they can trust a company to protect their data, they'll take their business elsewhere.

- » **Insecure devices:** Every device that can access your information holds the potential for unauthorized access. If you wouldn't leave your front door wide open so that anyone could come in anytime, even when you're not around, why would you use an unsecured device such as a smartphone or laptop to access your bank accounts?

- » **Identity theft:** A criminal who steals your identity can turn your life into a living hell. Sure, you'll likely be able to cancel any unauthorized accounts, but not before facing demands for payments and spending hundreds of hours trying to prove that it wasn't you who ran up those bills. And good luck getting your credit reports cleaned up!

- » **Intellectual property:** Your business may have patents, trademarks, trade secrets, or other confidential intellectual property that you wouldn't want in the hands of a third party. You need to make sure that such assets are properly protected.

REMEMBER

No matter how much you have to do to protect your assets, it's still much easier to prevent problems up front than it is to clean up the resulting mess if you are attacked. Recovering from a data breach or cyber theft is always more difficult and expensive than preventing such problems in the first place.

Seeing How You Are Vulnerable

To alleviate your risks, you need to understand where and how you're vulnerable. Unfortunately, in today's connected world, you can be attacked in many different ways. This section looks at some of them.

Malware

Malware is software designed to be malicious. Computer viruses, Trojan horses, and ransomware are some common examples of malware.

Regardless of the name, all types of malware are dangerous because they can damage your devices, steal your usernames and passwords, or encrypt your data so that you can't access it.

Malware can come from many different sources. Some common ones include:

- » Compromised software installations
- » Infected websites
- » Applications that pretend to be something useful for free

WARNING Never plug in a USB key that you find lying around someplace. Malware authors know that people will usually insert a USB key to see what it contains, and it's easy to create malware that automatically installs as soon as the key is inserted.

Account theft

Account theft can allow someone to access your confidential information, make large purchases, or even completely drain your bank accounts. Often, a great amount of damage is done long before you're aware that there's a problem. It only takes a few minutes!

Most online accounts control access by requiring a username and password. In many cases, your email address also serves as your username. But even when you have a separate username, the usernames are often public. Effectively, users typically log in with an easy-to-guess username and rely upon a pretty weak password to protect their accounts.

TIP Longer, more complex passwords are much more secure than simple, short ones. But even a strong password is less secure than a system that uses *two-step authentication.* Basically, two-step authentication adds a verification step such as entering the code that was sent by text message or another means of proving that you're really you.

TECHNICAL STUFF One type of malware that's often used in account theft is a *key logger,* a type of software that records a user's keystrokes. Some key loggers watch for login screens, record the user's input, and then send that information to a remote server.

Insecure connections

Information is often sent over the Internet as plain text. Anyone snooping on Internet traffic can read that information quite easily. If usernames, passwords, account numbers, or other confidential information is sent over this type of insecure connection, stealing that information is a simple matter.

TIP

Always look for *https* at the beginning of the URL in your browser's address box before entering any sensitive information. The *https* indicates that the connection is encrypted rather than being in plain text like addresses that start with just *http.* Most browsers also display a lock icon for secure encrypted connections.

WARNING

Ignoring available software patches or upgrades is another way to put yourself at risk. Software companies often issue fixes for vulnerabilities that have been discovered, but when a user doesn't apply those patches, the device running the software can be the target of attacks.

Chapter **2**

Understanding the State of Passwords

Protecting your online accounts and digital assets is absolutely vital in today's world. No one can afford to take the risk of going unprotected because plenty of people in the world don't give a second thought to stealing whatever they can.

In the vast majority of cases, most online assets are protected by a username and password. This chapter looks at the current state of password protection and shows you how common password practices are likely putting you at considerable risk.

Considering That Passwords Are the #1 Cause of Cyber Theft

In the early days of computing, passwords didn't matter very much. Computers were huge, centralized devices that most people never saw. To even get near one of those early computers, you needed to have physical access to a well-guarded, locked room. Once you got in, you needed to know some esoteric programming language to do anything. Now, compound that difficult

access with the fact that most early computers were completely stand-alone with no connection to the outside world. There was no Internet and no online access.

Today, of course, virtually all computing devices are connected. Your PCs, laptops, tablets, smartphones, and even some appliances now communicate via the Internet. This connectivity means that it's become absolutely vital to control the access to your digital resources.

Once controlling access became so important, the username and password seemed like the obvious solution. After all, the combination of a username and the correct password would have to be difficult to guess, wouldn't it?

The statistics show otherwise. A recent survey of small and medium-size businesses showed that more than half of them had been the target of a cyber-attack during the past year. These attacks wouldn't be successful unless the current state of protection — typically usernames and passwords — was so vulnerable.

REMEMBER

Although you might think that coming up with the right combination of both a username and password would be difficult, remember that one-half of that combination, the username, is often public information such as an email address or a user's online ID in public forums. In addition, it's extremely common for users to use exactly the same username across many different accounts. The result is that hackers likely only need to guess the user's password in order to gain full access.

Looking at the Challenges with Passwords

Protecting your online assets is obviously extremely important. You wouldn't think of leaving your unlocked car running in the parking lot while you went shopping at the mall, because you can probably guess the outcome. Likewise, you need to use methods that protect your accounts and other online assets in today's dangerous Internet world.

Unfortunately, using passwords to protect your online assets presents a number of major challenges.

Easy to guess or crack

Have you ever used something like "password" or "12345" as a password? If not, give yourself a pat on the back because those are some of the most common passwords that people use. In fact, lists are available online showing the passwords that people use most often, so someone trying to guess a password will probably have a pretty easy time of it in most cases.

Why do people use easy-to-guess passwords? It's simple, really. Few people take cyber security seriously, so to them, passwords are a nuisance. After all, who would want to steal their information? A password is just something they have to put up with. They don't want to put in any more effort than is absolutely necessary.

WARNING

Reusing a password for a number of different accounts also makes guessing someone's password very easy for a cyber thief. In fact, as soon as a thief discovers a password that works for one account, he'll try that same password to see if it will allow him access to other accounts. And, of course, if you use the same username for multiple accounts along with the same password, one lucky guess gives the thief access to every one of those accounts.

REMEMBER

Password policies are often not strictly enforced, and this oversight enables users to set up weak and easy-to-guess passwords. If you're running a business, you want to make sure that your password policy is enforceable and requires strong passwords. Use a system that allows you to set rules regarding minimum password length and complexity.

Hard to remember if complex and unique

Most experts recommend using long, complex passwords that contain a combination of uppercase letters, lowercase letters, numbers, and special characters. Every extra character in a password makes that password much harder to guess, especially if the password doesn't contain ordinary words. For example, something like joH8243_sMitH$mE would probably be virtually impossible for someone to crack (but now that I've used it here, it'll probably show up on a list, so you wouldn't want to use that exact sequence of characters).

Unfortunately, a password like joH8243_sMitH$mE is also extremely difficult to remember. You might be tempted to write it down on a sticky note that you placed on the side of your monitor (or the other favorite place for password sticky notes, one of your desk drawers). Of course, everyone knows to look for passwords on sticky notes, so that isn't a very secure method of keeping track of your passwords.

A good password manager system that encrypts all your data can make it much easier for you to use complex, difficult-to-crack passwords. Not only does the password manager keep track of those passwords, but it also keeps them private. The best password managers often also include features such as automatic secure password generation and automatic entry of your login information for various sites and accounts.

Difficult to use

Finally, strong passwords can be difficult to use because they're not only hard to remember, but also hard to type in correctly. If you use a long, complex password that contains a combination of characters, you can easily make a mistake entering the password.

Most sites hide the contents of password entry fields, so when you're informed that you've entered an incorrect password, you may not understand what error you're making. And if the site allows a limited number of attempts to enter the correct password, using a really complex password can be frustrating. Using a good password manager that automatically inputs your password is one effective way to avoid this frustration.

Don't fall into the trap of thinking that you can reuse the same complex password over and over. As mentioned earlier, if someone discovers your password, they'll likely try that same password on other sites where you have an account.

Chapter **3**

Considering Password Management

Anyone who is active on the web has dozens, if not hundreds, of usernames and passwords to keep track of. Trying to remember all of them quickly becomes a daunting task.

This chapter looks at some of the methods that people commonly use to keep track of their passwords and also considers why you may want to switch to a secure password management solution.

Looking at Common Password Solutions

People keep track of their passwords in a number of different ways. Often, those methods are completely insecure and almost invite theft or misuse.

Writing it down

Probably the most common method people use to keep track of passwords is to write them down on a piece of paper. Sometimes that paper is a sticky note stuck to the side of a computer monitor

or it may be a note stuck in a top desk drawer. Either way, anyone who happens to walk by can "accidentally" glance over and read the password.

TIP

An IT manager developed a method of discouraging users from leaving their passwords on a written note at their desk. He would walk around the office and look for these notes, and when he found them he would log into their account, change the password, and lock them out of their account. He then used their call to the help desk as an opportunity to deliver a lecture on password security.

Excel spreadsheet or data file

Another common method of keeping track of passwords is to create an Excel spreadsheet or data file containing usernames and passwords for various accounts. Although this method may seem slightly better than using written notes, those files are typically stored as plain text and often use an obvious file name such as "passwords."

WARNING

Because Excel spreadsheets and data files usually aren't encrypted, anyone who can access the file will have complete access to all your usernames and passwords. And they don't need to steal your laptop in order to get a copy of the file — especially if they can find it on your network or if you leave your device unlocked when you go for a cup of coffee.

Using a web browser to remember

Most modern web browsers conveniently offer to remember your usernames and passwords for the various sites that you visit. Although this feature may seem convenient, using it can place you at great risk because anyone who gains access to your computer can also gain access to your online accounts. This feature can also be inconvenient if you use more than one device because the information is only stored on the device where it was created (and may be stored as easily readable plain text, too).

REMEMBER

If you decide to allow your web browser to remember any account logins, it's vital that you set up your system to require a password or biometric scan in order to log in to your computer. In addition, make certain that you log out or at least lock your computer whenever you leave, even for a few minutes.

Password managers

An old saying goes "when all you have is a hammer, everything looks like a nail." If you want to do the job the right way, you'll get much better results using a tool specifically designed for the task.

When it comes to keeping your passwords secure, nothing beats an actual *password manager* — an application designed specifically to deal with passwords. In the next section, you see more about password managers.

Understanding Password Management Solutions

When you're ready to get serious about protecting yourself and your assets online, you need to consider a dedicated password management solution. Rather than some cobbled-together halfway measure, a true password manager incorporates all the features you need to ensure your safety and security.

Password managers provide secure, encrypted storage of usernames and passwords. They are available in a variety of configurations to meet the needs of individuals, families, and businesses of all sizes. Beyond storing usernames and passwords, a comprehensive password manager can also generate extremely strong passwords for each of your accounts. But a good password manager goes beyond simply generating great passwords by automatically recognizing sites and securely filling in your username and password.

A good password manager gives you the best of both worlds. You can easily create strong passwords, and you can easily use them. You don't have to remember your passwords, and you don't have to struggle trying to enter a complex password to log in to your account.

TIP

Look for a password manager that supports a broad range of platforms, operating systems, and storage capabilities. You want a solution that supports Android, iPhone, BlackBerry, Windows Phone, iPad, Microsoft Surface, Amazon Kindle, Mac, Linux, and Windows PCs. That way you won't be stuck with having to move to a different password manager when you add new devices.

TECHNICAL STUFF

Most password managers are encrypted and require you to log in to the application in order to access your passwords. Password managers store information in an encrypted digital vault. It's important that you choose a solution that's truly secure. An important factor in the security is something known as *zero knowledge*. This means that the user is the only person who has full control over the encryption and decryption of his or her data. The encryption key that's needed to decrypt the data always stays with the user. This requirement prevents anyone else, including the password management solution provider and the cloud storage provider, from decrypting the user's data.

The zero-knowledge approach is important because even if the data stored online is hacked, the hackers can't decrypt it. In addition, this approach ensures that data remains encrypted during transit, so even if someone manages to listen in to the data stream as it crosses the Internet, they can't decrypt the data.

In many organizations, the need to securely store data extends beyond passwords. This can include Secure Shell (SSH) keys, digital certificates, and a range of confidential business documents, files, videos, and photos. Therefore, a recommended feature of password management solutions is the ability to securely store these additional types of information.

TIP

Some of the better solutions also use *two-factor authentication,* which offers far better security than a simple username and password. Two-factor authentication adds a layer of security by requiring users to pass a biometric scan, enter a code sent as a text message, or provide a code from a physical or virtual one-time passcode generator, such as Google Authenticator.

Chapter **4**

Finding the Right Password Management Solution

F inding the right password management solution is important. Make sure to choose carefully and select a solution that protects you, fits your needs, is easy to use, and works with your budget. This chapter discusses what consumers and businesses should look for in password management.

Considering Password Management for Consumers

It isn't only businesses that need a good password management solution. Consumers need protection against cybercrimes like identity theft, too. When you realize that individuals and families don't have an IT staff to look after their online security needs, it's pretty clear that consumers need all the help they can get!

As a consumer, you may not have intellectual property such as patents, trademarks, and proprietary trade secrets to protect, but

you have bank accounts, medical records, online accounts, price-less family photos, and many other assets you want to keep safe. Consider, for example, that identity theft alone could cost you thousands of dollars and countless hours to correct. If a password manager can help you to prevent even a single such incident, isn't it worthwhile?

Finding the right password manager isn't too difficult, but you'll want to look for these features:

» **Remembering passwords:** Clearly, the number one reason for using a password manager is so that you'll never have to remember passwords again. And, if you don't have to remember your passwords, you can more easily use complex, strong passwords that will keep your accounts more secure.

» **Taking advantage of biometrics:** If your device has a fingerprint scanner, you'll want your password manager to take advantage of the biometric authentication feature built into your device. Not all password managers make use of these capabilities — check before you buy.

» **Password generation:** Let's face it, people are terrible at coming up with strong passwords full of random characters. You want a password manager that can create high-strength, random passwords that are virtually impossible to guess.

» **Easy log in:** A good password manager should be able to enter your login credentials for you automatically. This feature makes using strong passwords much easier because you have no chance of mistyping the entry and then having to figure out what's wrong or getting locked out of your account.

» **Digital vault:** You need to protect more than just pass-words, so you may want to consider a password manager that enables you to store private files, photos, and videos in a secure digital vault.

» **Multiple device support:** You need a password manager solution that works on all the types of devices you have now, and also has flexibility so that you aren't stuck with one platform. An important part of this multiple device support is automatic synchronization across those devices. If you add a new account and password on your desktop PC, you'll want to be able to access that information on your smartphone or tablet.

>> **Two-step verification:** It's much harder for anyone to break into your accounts if they need more than just your username and password, so you may want to consider a password manager that uses two-step authentication.

>> **Easy sharing:** Another nice feature to have is the ability to securely share files with friends and family members. Some password managers provide this option.

TIP

To protect all members of your family, you might consider looking for a password manager that offers a family plan. Not only will you be looking out for family members who might not otherwise take digital security very seriously, but a family plan will likely save you money, too. In addition, by including the whole family, you'll be teaching a valuable lesson about the importance of protecting your assets.

Finding Password Management for Businesses

If you run a business, you're already aware of many of the risks that face your employees, your customers, and your business assets. You probably also realize that cyber theft and data breaches affect businesses of all sizes. It's estimated that more than 60 percent of the data breaches affecting businesses result from weak passwords and policies. The right password management solution can help you minimize or avoid these problems and get back to doing business.

Most of the features mentioned earlier for consumer-grade password managers are also quite desirable in a solution aimed at businesses. Obviously, high-strength passwords, ease of use, secure authentication, and so on are features that you'll want in a password management solution for your business. But in addition to those, here are some features you may want to look for:

>> **A management dashboard:** You need a solution that enables you to enforce strong password policies and monitor employee compliance with those policies. You also need robust reporting and auditing capabilities, as well as notifications to alert you to any potential problems.

- » **Privileged account management:** Certain data, such as payroll records and other confidential information, must have restricted access. It's important that your password manager solution enables you to securely manage the life cycle of privileged account credentials, be able to set up role-based permissions, control credentials sharing, and enforce scheduled password changes.

- » **Reduced help desk costs:** You'll want a system that reduces the need to assist users with lost passwords.

- » **Easy scalability:** You don't want to be stuck with a system that can't grow with your business. You need a system that can easily accommodate your business needs now and in the future.

- » **Rapid deployment:** You have a business to run and can't afford to waste time trying to implement a poorly designed, complex system. Look for a system that's intuitive and easy to deploy, regardless of the size of your business now or in the future.

- » **Secure sharing:** You need to securely create, share, and manage both individual records and encrypted folders across teams with configurable permissions and policies that allow administrators to maintain compliance with company policies and internal controls.

- » **Alignment with company structure and policies:** Security solutions are only as good as their ability to adapt to your company's structure and policies. You need configurable roles, role-based permissions, and admin privileges, all assignable by a specific organizational hierarchy to ensure a perfect fit with your unique environment.

- » **Visibility into password hygiene and password usage reports:** Most businesses have limited visibility into the password practices of their employees, which greatly increases cyber risk. Password hygiene cannot be improved without critical information regarding password usage and compliance.

Chapter **5**

Ten Things to Remember about Password Management

This chapter gathers some brief facts that you'll want to remember about password management:

» **Your personally identifiable information (PII) and financial information are among your most valuable assets:** Financial accounts, Social Security numbers, sensitive documents, passwords, and identity are stored online and might be at risk of being hacked. Hackers target PII in virtually every single breach and earn billions of dollars per year from this information.

» **Cyber theft and data breaches against businesses and individuals are increasing:** You simply can't afford to assume that you won't be a target.

» **Passwords are the #1 cause of data breaches and cyber theft:** You need to use strong passwords that aren't easily guessed.

- » **Manual password management isn't working:** Manually generating, tracking, and managing high-strength passwords is difficult, time consuming, and error prone, and often leads to frustration and a lack of productivity.

- » **You need better security:** Common password solutions such as memorization, tracking via sticky notes, or storing in a spreadsheet are not secure and are inefficient.

- » **The growing number of accounts and devices adds complexity to password security:** It is becoming increasingly difficult to manage passwords and other personal information for a multitude of online accounts across multiple devices.

- » **Password managers can help:** Password managers such as Keeper solve the password management challenge and, in doing so, mitigate the risk of cyber theft and data breach while improving online productivity.

- » **Individuals need password management, too:** Individuals and families need a password manager to simplify and protect their digital lives as well as to provide an easier way to share passwords and other digital assets with friends and family.

- » **Businesses need protection:** Businesses need a password manager to significantly reduce the risk of data breaches, simplify secure password management and increase productivity in an increasingly bring-your-own-device (BYOD) workplace environment, and enable enforcement of password policies and proactive monitoring of password hygiene and practices within the workplace.

- » **Not all password managers are created equal:** Look for one that makes using strong passwords easy, enables you to use biometric authentication, enables automatic account logins, and supports a broad range of devices.

TIP

A free trial is of Keeper's password management solution is available at `https://keepersecurity.com`.

KEEPER®

The leading cybersecurity platform for preventing password-related data breaches and cyberthreats.

Protect yourself from cyber theft

Cyber crime increasingly puts both individuals and businesses at risk. Unfortunately, the method most often used to protect accounts — passwords — are the leading cause of data breaches and cyber theft. This book shows you what you need to know about password management systems that can greatly improve your online security and productivity. The right system can help you use extremely strong passwords without complicating your online life.

Inside…

- Understand online security threats
- Learn about password management
- Find a solution for business or home
- Create complex, strong passwords
- Protect yourself from identify theft
- Safeguard employees and customers
- Never memorize passwords again!

KEEPER®

Brian Underdahl is a well-known author and technologist who enjoys making complicated topics easy for ordinary people to understand.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT