



4 Password Risks and How to Handle Them

eBook

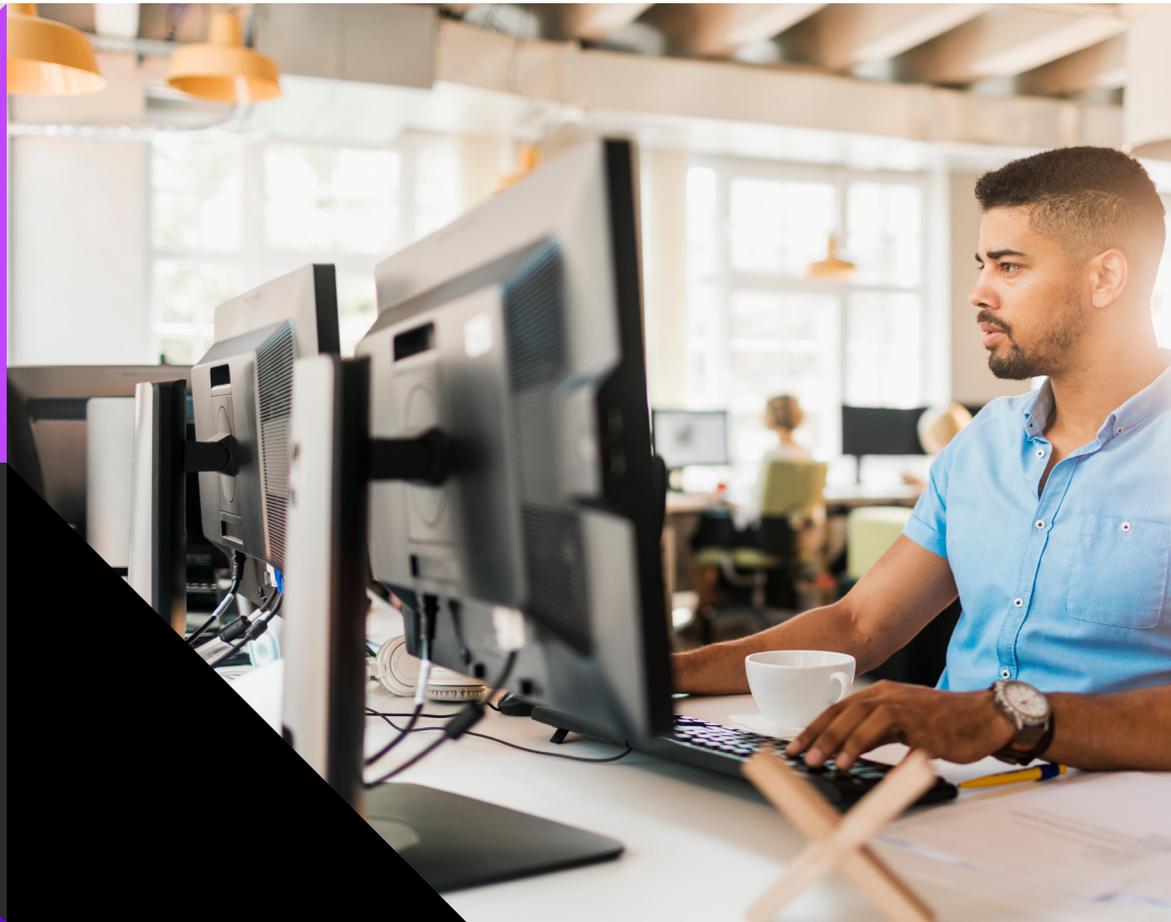




Table of Contents

4 Password Risks and How to Handle Them	3
The Trouble with Passwords	3
Password Management Can Be Time-Consuming and Difficult	4
People Often Use Easy-to-Guess Passwords.....	4
Criminals Use Multiple Tools to Guess Passwords.....	5
Password Reuse.....	5
Securing the Keys.....	6
Safeguarding the Keys to the Kingdom	7
About N-able	8

4 Password Risks and How to Handle Them

Willie Sutton was a long-time American bank robber. It took years for authorities to catch him, during which time he made off with a killing.

Once caught, the authorities asked him why he chose to rob banks. He replied, “Because that’s where the money is.”

Crime hasn’t changed much since it went virtual. Cybercriminals look for high-value targets that net them a tidy sum for little work. Just like Sutton robbed banks instead of individuals because they held everyone’s money, cybercriminals have increasingly focused on MSPs because they hold all the passwords, data, and systems for multiple businesses.

As an MSP, you have the “keys to the kingdom.” Criminals know you have insider access to applications, devices, networks, and sensitive data for multiple businesses. They hit you once but can profit numerous times. Your job is to keep your customers safe, and that means using strong password policies for your own team. Today, we’ll discuss some of the challenges organizations face concerning passwords and password management—and ways you can reduce your risk.

The Trouble with Passwords

Passwords were originally used as an authentication method well before the days of the internet. Back then, you often had to authenticate only to your own workstation and a mainframe, and rarely was it necessary to remember many passwords. Times have changed. People use more services than ever, often memorizing an incredible amount of username/password combinations.

Today, if not handled correctly, passwords can open businesses to significant damage. If you fail to protect your customers, you could lose them, face brand reputation damage, or grapple with fines.

Unfortunately, there are serious challenges when it comes to password management. This eBook shares four of the main challenges and how to handle them.

1. Password Management Can Be Time-Consuming and Difficult

Managing user credentials across multiple customer environments can quickly become a sizeable undertaking. You must be able to grant or revoke access, expire passwords periodically, and demonstrate due diligence to auditors. These can easily become complex, time-consuming tasks.

Beyond that, many technicians have bad habits around storing passwords. They may write them down on paper or post-its where people can easily see them. They may keep them in spreadsheets, which can introduce human error and quickly become unmanageable as your MSP takes on more clients. It's not uncommon to store these spreadsheets in multiple locations, such as a local work machine, cloud storage, a personal USB drive, or even on a personal computer (for those after-hours calls), making it hard to truly revoke access if a technician leaves. Neither paper nor spreadsheets make storage and management easy, let alone secure.

2. People Often Use Easy-to-Guess Passwords

Most users find it difficult to remember passwords, so they fall back on creating easy-to-remember passwords. This, unfortunately, also makes them easy to guess. Even technicians who know better can practice bad cyberhygiene around their passwords. Here are some common no-no's:

- **Common passwords:** There are a number of passwords people commonly use. In 2018, for example, a most-commonly-used-passwords list reported that a significant number of people use the words "password," "iloveyou," "football," "admin," and "monkey," for their accounts¹.
- **Short passwords:** Some systems force lengthy, strong passwords, but many are lax on the requirements. Longer passwords take exponentially longer to crack than shorter ones².
- **Keyboard patterns:** Using a straight keyboard pattern, like "123456" or "qwerty," can easily be picked up in automated attacks. These often show up on the lists of the most commonly used passwords as well.
- **Reverse spellings:** It might seem like a more secure pattern, but spelling your password in reverse order won't help. For example, "drowssap" (password spelled backwards) has appeared frequently in data breach dumps.
- **Easy-to-find information:** If someone actively wants to pick a high-value target—say a CFO of a company or an IT admin—they can do some reconnaissance to find personal information on the person. For this reason, avoid using information that can easily be found, like your birthdate, your name, a pet name, or anything too personal.

¹"'123456,' 'donald,' and Other Terrible Passwords People Used This Year," Mashable. <https://mashable.com/article/most-common-passwords-2018/> (Accessed July 2019).

²"Estimating Password-Cracking Times," BetterBuys. <https://www.betterbuys.com/estimating-password-cracking-times/> (Accessed July 2019).

3. Criminals Use Multiple Tools to Guess Passwords

As mentioned previously, people often create passwords that are easy to remember, even if they're not inherently secure. If you use an easy-to-guess password, you could open yourself up to one of the following attacks:

- **Password spraying:** This involves gathering a list of known email addresses and trying out a list of common passwords to see if they get a match. These attacks are automated and sometimes highly successful. Cybercriminals have it even easier if you choose a commonly used password or passphrase, as mentioned in the previous section.
- **Brute-force attacks:** This involves attempts to crack a password using email addresses or usernames and combining them with words from dictionaries (often called a “dictionary attack”) or common variations on these words. These attacks are also automated. They can be resource-intensive and time-consuming, but cybercriminals still see success against weaker passwords.
- **Credential stuffing:** This involves gathering stolen username/password combinations from a large-scale data breach, then using them on other sites to see if there's a match. For example, hackers could buy (or find) breached username/passwords from a major hack like the Collection #1 data dump from early 2019, which contained more than a billion breached email and password combinations³. They can then use this information and try it against other accounts.

Cybercriminals have multiple tools at their disposal to crack or steal passwords. This puts you at a disadvantage if you're not using proper cyberhygiene for your passwords.

4. Password Reuse

Finally, many people reuse the same passwords across multiple accounts, leaving customers open to credential stuffing attacks like those mentioned in the previous section. For example, let's say you have a username/password or email address/password combination to a compromised social media site. Your information will likely appear on the dark web in a data dump, and cybercriminals can then try that on multiple banking institutions' websites, hoping to get a match. If you use one of those institutions and reused your credentials on that site, bad things can happen.

Password reuse doesn't even have to lead to major consequences. It could just lead to a major nuisance. For example, many Pizza Hut® customers had their loyalty points stolen by cybercriminals. Pizza Hut wasn't breached—the points were vulnerable due to users reusing passwords across accounts⁴.

³“Collection 1 Breach – How to Find Out if Your Password Has Been Stolen,” Forbes. <https://www.forbes.com/sites/kateofahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#7e1b09562a2e> (Accessed July 2019).

⁴“To Members of Pizza Hut's Loyalty Scheme: You Really Knead to Stop Reusing Your Passwords,” The Register. https://www.theregister.co.uk/2019/06/06/pizza_hut_hacked_tells_rewards_users_to_change_passwords/ (Accessed July 2019).

Securing the Keys

Fortunately, you can stay ahead of the bad guys with a few tips.

DON'T LIMIT YOURSELF TO LETTERS

Many users think of passwords as literal words. This limits users to passwords that can easily be guessed using an automated dictionary attack, where hackers attempt to guess passwords by searching through words in the dictionary. Adding numbers or symbols to passwords greatly increases the strength, making them harder to crack.

However, don't fall into the trap of using "obvious" strings of letters or symbols. For example, you may want to avoid using "@" to replace the letter "a" or adding "1" or "123" to the end of your password. Criminals know these patterns and often structure their attacks to look for them.

PASSPHRASES ARE YOUR FRIENDS

Using a phrase can help boost the strength of your password since entire phrases don't appear in dictionaries (preventing them from being used in dictionary-style attacks, for the most part). For example, "MyCat!Isn'tHappy8WithMe" is far stronger than "catfood789." Check commonly used password lists to make sure you don't use one like "iloveyou." Many news outlets post articles each year on the most commonly used passwords, so periodically reviewing these articles can also prove beneficial.

GO RANDOM

An even better practice is to create a random string of numbers, characters, and letters. These can be harder to remember at first, but they certainly are stronger. You can generate these passwords using an automated generator, or you can create one yourself. One possible way of achieving this—and still making passwords memorable—is to convert a passphrase into a string using a specific letter in the phrase while also adding in numbers, symbols, and capitalization. For example, you could take the phrase, "I really love products by N-able," and make a phrase out of the final letters in each word. This could look like "IYESYS." Then, you could add in other numbers or symbols to end up with "I#Y7Es3Ys." This appears random, but you have an underlying logic to make it easier to remember.

USE MULTIFACTOR AUTHENTICATION

You're probably already familiar with multifactor authentication (MFA). MFA requires users to have several elements to prove their identity before allowing access to a system. Each element is considered one "factor." Factors include username/password combinations; security questions; a verification code sent via text or email; biometric elements, like fingerprints or face scans; applications, like Google® Authenticator or Authy®; or a physical device, such as a USB stick designed for authentication purposes.

MFA can reduce the likelihood of unauthorized access as few criminals will have access to each factor. If someone guesses your password, they're unlikely to have your USB authenticator as well.

USE A PASSWORD MANAGER

These tips can certainly help secure your passwords and accounts; however, what you gain in security could cost you in usability. Compound this with the sheer number of passwords MSPs and technicians have to remember, and you have a pretty unsustainable model on your hands.

Enter password managers. A password manager, like N-able™ Passportal™ + Documentation Manager, can help you:

- Reduce memorization: Technicians shouldn't have to remember multiple passwords, write them down on sheets of paper, or maintain spreadsheets. N-able Passportal + Documentation Manager lets technicians log in once using one strong password, then enables them to access user accounts with auto-generated strong passwords.
- Revoke passwords easily: N-able Passportal + Documentation Manager makes it easy to revoke access for technicians who leave, which can help protect you against former employees leaving with passwords and holding a grudge.
- Enforce strong password policies: With N-able Passportal + Documentation Manager, you can ensure passwords get expired and updated periodically to help keep them fresh and secure. You can even set passwords to expire on a daily basis if you want maximum protection.

Safeguarding the Keys to the Kingdom

Cybercriminals see MSPs as high-value targets. All they need to do is successfully hit you once to compromise multiple businesses. As an MSP, you need to take your password policies seriously, or you could end up on the wrong end of a breach.

N-able Passportal + Documentation Manager is built to help you manage risk around passwords, shorten incident resolution times, and assist customers in meeting compliance guidelines.

[Learn more and request a demo](#)



About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com

© 2021 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein.