PASSWORD SECURITY

THE GOOD, THE BAD &
THE NEVER SHOULD HAVE HAPPENED

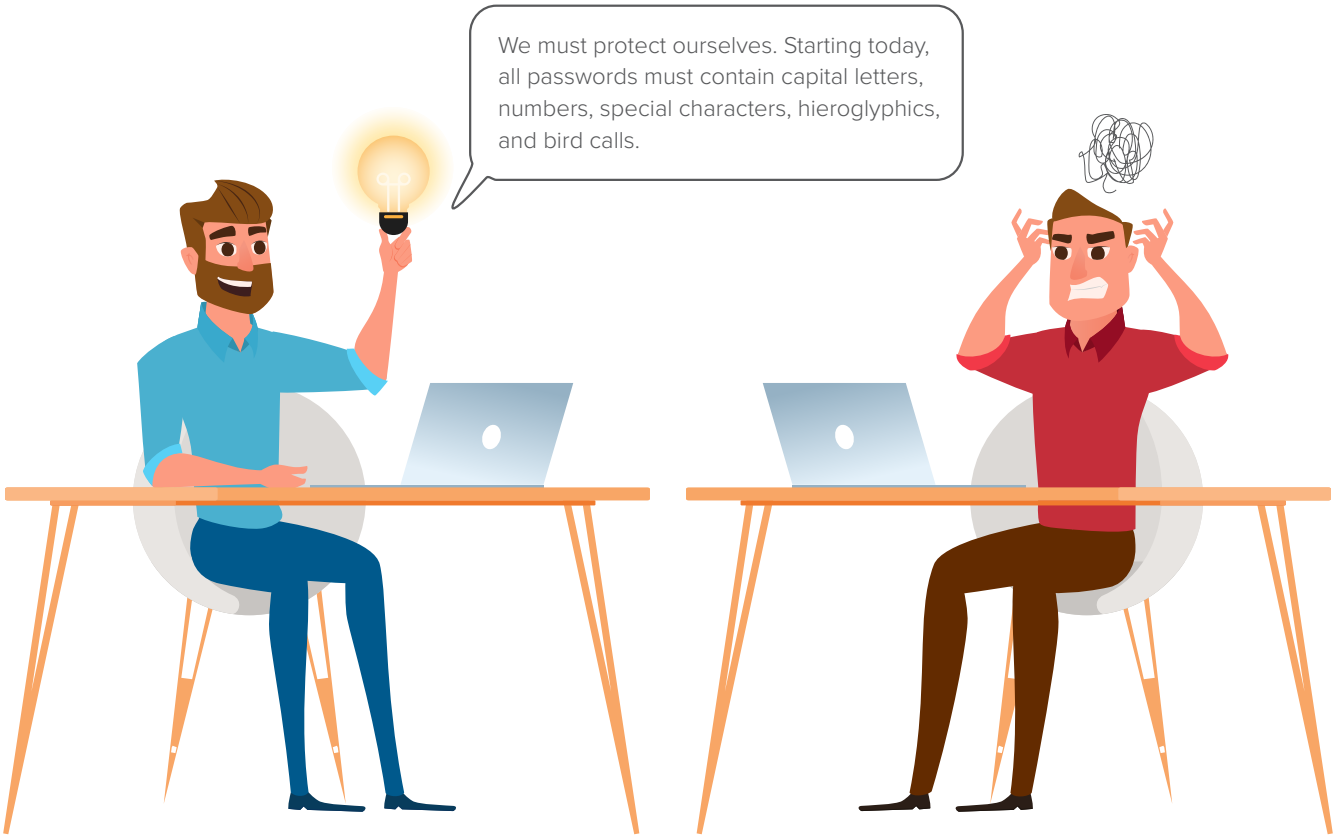
CONTENTS

INTRODUCTION

While most organizations have a password policy that sounds technically secure, hardly any have a policy that benefits the organization, encourages strong passwords, and improves overall security. It's time to stop requiring capital letters, numbers, special characters, and frequent password updates. We are here to correct the outdated, misleading, and muddled logic when it comes to what makes a password secure.

IN THIS GUIDE, YOU WILL LEARN:

- The changes organizations should make to improve their password security
- Some recommendations for ways to help support these new changes
- Exceptions and customizations for creating a new password policy to ensure it works for your organization



A HISTORY LESSON ON PASSWORDS

As passwords became prevalent with the increased adoption of computers and the internet in the late 90s, the tech industry started looking for guidance on what makes a good password. Enter: NIST Special Publication 800-63B: Digital Identity Guidelines, the official government list of recommendations regarding passwords. The first edition of this document by the National Institute of Standards and Technology (NIST) covered requirements for passwords, including the use of capital letters, numbers, and special characters, and the need to change them approximately every three months. The author has since come out and apologized about the first iteration of the NIST guidelines, stating, "In the end, it was probably too complicated for a lot of folks to understand very well, and the truth is, it was barking up the wrong tree." The author and others worked to improve the document, and it has been updated regularly since then. It is now an excellent industry standard, but many organizations still follow advice from the original version and have not had a chance to catch up with the latest recommendations.

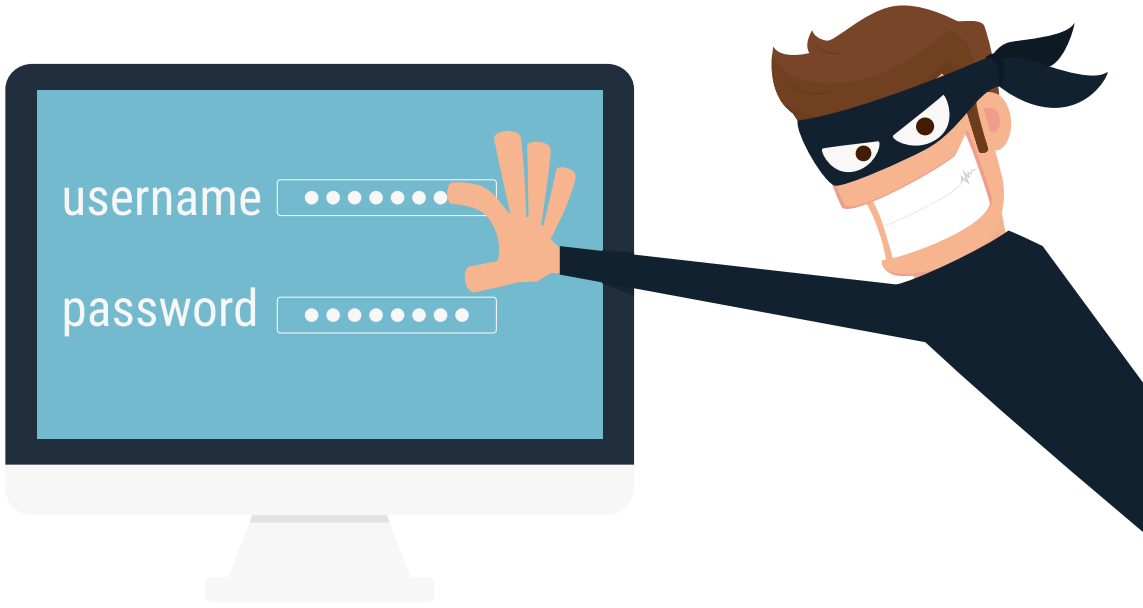
Let us take this chance to apologize on behalf of the entire security community for making you comply with those older requirements. We have learned, we have grown, and we know better now. With these new requirements, we are glad to say that passwords should become easier to remember and more secure in the future.

HOW PASSWORDS WEAKEN ORGANIZATIONS

Before we dive into best practices, it's important to understand how hackers can use poor passwords against your organization. It's easy to think that that you will never be targeted, but the first thing a hacker needs before compromising an organization is a foothold into the network. Once they get access into a network, they can usually use that foothold to access practically anything. This has a lot to do with how networks are designed and accessed, but we won't dive into that here.

When Bishop Fox consultants need to guess passwords during an engagement, we don't pick one employee and focus our efforts on compromising their identity. Instead, we learn the email pattern of an organization (e.g., first.last@company.com) and pull a list of employees off a social media or directory website. From there, we try each email with one common password (e.g., Company123!). Almost every time, this method will work for at least a few accounts, and we gain the foothold we need.

For this reason, it doesn't matter who you are; you are a potential target.



RECOMMENDED POLICY CHANGES

STRONG RECOMMENDATIONS FOR CHANGES TO A PASSWORD POLICY:

RULE 01

REQUIRE LONG PASSWORDS

Password length is the most important aspect to a strong password. When implemented correctly, a 15-character password is essentially impossible for hackers to brute-force. (Refer to section 5.1.1.2 in NIST 800-63B for technical details on what a correct implementation requires.) If your organization can implement the recommendations outlined in the rest of this section, we recommend that your password policy require at least eight characters; if the organization can't implement all the requirements, we recommend the minimum length be made longer to compensate.

RULE 02

DON'T REQUIRE NUMBERS, CAPITAL LETTERS & SPECIAL CHARACTERS

Research shows that when password policies dictate that users must include capital letters, numbers, and special characters, frustrated users are likely to take shortcuts and use the same pattern for every password they create. While users should still be able to include uppercase letters, numbers, and special characters, they should not be forced to include them. Also, there will always be people who do only the bare minimum. For example, Company123! fits almost every common character requirement, but it's still a poor password. Ultimately, requiring multiple character sets is unnecessary, only makes things more complicated, and still allows for poor passwords.

RULE 03

DON'T REQUIRE UNNECESSARY & REGULAR PASSWORD CHANGES

The policy of changing passwords on a regular cycle is old-school logic and perpetuates the use of weak passwords. Instead, have your employees create one strong password and use it for the duration of their career at your organization. The only times you should ask employees to update their passwords are when passwords are breached or otherwise compromised. Without this requirement, there is no reason for employees to use passwords based on the season or other minor variations of the same password.

RULE 04

IMPLEMENT SINGLE SIGN-ON (SSO) WHERE POSSIBLE

Implement an identity provider that supports a single sign-on protocol (such as SAML) so that a user can log into a single ID to gain access to connected systems. This will help reduce the number of separate credentials employees have to memorize to access their accounts. When employees must remember the credentials for multiple accounts, many will use small variations of the same password, keep all their passwords in a file on their computer, or use the old classic: a sticky note next to their monitor.

RULE 05

BAN YOUR COMPANY NAME & ALL RELATED WORDS

One of the most important aspects of a good password policy is that it is enforceable. You can have the best fine print in the world encouraging people not to use common words, but if you don't hold people to it, they will do so anyway. We highly recommend that you have a system in place that will allow you to ban certain passwords from being used.

THIS SHOULD INCLUDE:

- All the words in the dictionary
- Your company name
- Names of all your products
- Company or product names combined with numbers
- Seasons or years
- Other words or vocabulary related to what your company does
- Generated lists of the most popular passwords

There are several data sources, e.g., SecLists, that regularly compile large lists of common passwords. You can download the list and then add items specific to your company.

OPTIONAL IMPLEMENTATIONS FOR ORGANZATIONS:

RESOURCE 01

USE A PASSWORD MANAGER

There are many password managers, like LastPass, 1Password, and KeePass. They all have advantages and disadvantages. Some are web-based and attached to your browser, whereas some are downloaded directly on your machine. A password manager is designed to only require one master password to access all your passwords. The password manager generates strong passwords that are stored and, if attached to the browser, auto-populated into known websites so that you can easily log in.

AS EFFORTLESS AS THIS SOUNDS, THERE ARE SOME CAVEATS:

- Password managers must have strong master passwords
- Some password managers do not support multi-factor authentication (MFA). Choose one that supports MFA.
- Do your research to understand each provider's pros and cons.
- Password managers cannot populate passwords for the computer itself, so have a policy for this password.

RESOURCE 02

IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA)

MFA makes logging in a two-step process. The most common practice is to enter your password and receive a push notification on your phone that you would accept. Mobile applications like Duo, Microsoft Authenticator, and Authy make adding MFA simple. We think MFA is great, and absolutely recommend organizations to implement it. While MFA is not a magic bullet, it does make it much harder for an attacker to exploit a bad password.

You might be thinking to yourself: But what if my system doesn't allow me to put these types of enforcements in place? An excellent question.

MAKING A PASSWORD POLICY WORK

The recommendations in this document were written for professional organizations and for those who are creating and enforcing password policies. There will be exceptions to these suggestions since every organization is different and handles different data. Please consider the following cases and include exceptions and customizations when updating your organization's password policy:

OFF-THE-SHELF SOFTWARE DOESN'T ALWAYS SUPPORT WHAT YOU DO.

Many companies use off-the-shelf software that don't allow certain flexibilities when it comes to enforcing password policies.

SOLUTION 01

IDENTITY PROVIDER IMPLEMENTATION

SSO can act as a gateway to your network and various platforms that you ask employees to log into. Identity providers tend to be security-focused, so you can find an SSO solution that allows the password controls you desire to help enforce better security and password policies.

If SSO is not possible, encourage your employees to rely on a password manager. If you can't deploy and support a password manager, have employees memorize one strong password and use it for all accounts on corporate-owned systems. However, users must remember to use separate and unique passwords for third-party accounts since you cannot verify how the third-party protects or stores account credentials. This is a good reason to encourage and support the use of a password manager; this lifts the burden of keeping track of which services are safe to use the same password on.

SOLUTION 02

EMPLOY GET-BADPASSWORDS[4] OR SIMILAR SERVICE.

Get-bADpasswords is a free PowerShell script available in GitHub that allows Active Directory (AD) administrators to scan directories and compare them against lists of compromised, weak, or non-compliant passwords. The software is designed to work with AD, but a similar idea could be adopted to work with other programs. Get-BadPasswords

RECOMMENDATIONS CANNOT BE IMPLEMENTED EVERYWHERE

If your company has been around for over 40 years, chances are you have some old homegrown systems that might not allow you much flexibility when it comes to implementing user-friendly password policies. Even some more recent solutions may not completely implement recommendations such as MFA. Additionally, some situations may not easily allow the implementation due to their nature, such as company email accounts that do not have an associated user (e.g. contact@company.com).

SOLUTION

POLICY EXCEPTIONS

Always allow room for exceptions in your policy and put in mitigating controls to minimize the risk. For example, consider placing legacy systems on their own separate network or behind a VPN. For shared email accounts, forward email from those accounts to the individual accounts of users responsible for them and disable regular access to the shared accounts. Finally, increase monitoring of systems and accounts that cannot implement the normal recommendations.

TYPE OF INPUT DEVICE

A blanket password policy should always be device-specific. When we talk about password policy in this document, we are referring to any device that has a keyboard. Don't accidentally force your employees to use a 15-character code to go the bathroom.

SOLUTION

DETAILED DEVICE SPECIFICATIONS

Specify the type of devices the policy refers to and avoid any confusion.

USER ACCESS

The recommendations in this document may not apply in the case of privileged users with access to highly critical data or systems, such as system administrators with back-end access who manage accounts related to security, safety, or military weapons.

SOLUTION

POLICY ADJUSTMENTS

Consider risks associated with these accounts when creating policies and adjust the policy as necessary.

MOST EMPLOYEES ARE NOT SECURITY EXPERTS

Employees should not be expected to be security experts on top of their day-to-day job. Each employee is hired to be an expert in a certain area, and they have their own stresses and priorities. Just as you wouldn't expect the security team to understand marketing analytics, you can't expect your sales or human resources departments to know the difference between a secure and insecure password.

SOLUTION

CYBERSECURITY EDUCATION

Make policies easy to understand and educate employees on the policies on a regular basis.

EMPLOYEES MAKE MISTAKES

Employees have a vested interest in protecting their reputation and their job. When an employee feels like they have done something to put either of those at risk, such as doing something to compromise their corporate account, they are likely to keep it quiet. Employees should feel comfortable going to IT when they think they've done something to put the organization's security at risk.

SOLUTION

CONSTRUCTIVE DISCIPLINARY ACTION

Do not punish or shame employees when they are compromised, so they feel encouraged to notify security or IT when something happens.

CONCLUSION

Password policies are often overly complicated and based on antiquated logic. It's time to update those outdated beliefs around passwords, password policies, and what constitutes a secure password. Just because we've been doing something for years doesn't make it right.

MEET CANDIS ORR

ABOUT
THE AUTHOR

Candis Orr (CISSP) is a Security Associate at Bishop Fox, a security consulting firm providing services to the Fortune 500, global financial institutions, and high-tech startups. In this role, she focuses on vulnerability management, security policies and processes, and social engineering assessments.

Additional core competencies include risk assessments, gap analyses, and mergers and acquisitions (M&As). She also is heavily experienced with social engineering tactics and tools, security process documentation, and mapping controls and requirements to processes. Candis has been quoted in publications such as Threatpost and CSO. Additionally, she has presented at Brigham Young University, Georgia Tech University, and Aaron's Day of Cybersecurity Awareness on the subject of social engineering.

Candis holds a Bachelor of Science from Arizona State University with a major in Computer Science and a concentration in Information Assurance.

BISHOP FOX®

We provide security consulting services to the Fortune 1000 and high-tech startups.

We help our clients secure their businesses, networks, cloud deployments, applications, and products.

Find out more at bishopfox.com.
Keep in touch with the foxes on Twitter @bishopfox and on LinkedIn Bishop Fox.