3 Steps to Stronger Passwords

By Lisa Traina, Partner

I once heard a speaker say that passwords are like underwear: change them often, keep them long, don't leave them lying on your desk, and don't share them.

As a security professional, I have been discussing the need for strong passwords for almost 20 years, and not much has changed during that time. Each time I made a presentation, I noted that there is no silver bullet. The best solution was complex passwords that users change frequently and don't share.

Yet weak passwords remain a top cybersecurity risk, as highlighted by recent large hacks and breaches, including the Equifax breach. The media has reported that Equifax was using "admin" for both the username and password of an employee portal in Argentina. And after the 2014 Sony hack, it was discovered that the company kept thousands of passwords to the company's internal computers, servers, and email and online accounts in a digital folder labeled "Password."

So why does this keep happening, and what can your organization do to reduce the risk? Here are three steps to stronger passwords.

1. Understand the challenges.

The National Institute of Standards and Technology (NIST) made headlines when it issued password guidelines that steer away from requiring complexity and frequent password changes.

NIST noted that while the previous guidelines were intended to create more secure passwords through criteria such as complexity, this has been circumvented over time by several issues:

- The number of systems individuals access via a username and password has grown tremendously. Not too many years ago, we didn't have passwords for travel sites, online bank accounts, health records, and more — not to mention the growing number of work-related passwords. There are just too many to commit to memory.
- Users have difficulty remembering complex passwords, especially when they change frequently. As a result, many people use ineffective variations of common passwords (e.g., Password1!). The most common breached passwords are published annually and it is surprising how many versions of "123456" and "password" continue to make the list.
- Because complex passwords are hard to remember, users also store them in unsafe ways, such as in a document on their computer, on a sticky note on their desk or, even worse, in the Notes app on their unsecured cellphone.
- Password-cracking software has become more sophisticated, and keylogger software and social engineering have emerged as effective means of compromising lengthy, complex passwords. Millions of compromised passwords are in circulation due to cyber breaches.

These factors make complex, expiring passwords far less effective, thus new the new guidelines.

2. Understand the new guidelines.

Rather than complex passwords that expire frequently, the new NIST guidelines focus on layered security, which we have long advised.

NIST recommends:

- Comparing passwords against a "blacklist" that rejects passwords:
  - Used in previous compromises,
  - Based off dictionary words,
  - Containing repetitive or sequential characters, and
  - Based off items such as user name, system name, etc.
- No forced composition rules (like alphanumeric and special characters) or required arbitrary changes.

- Limiting the number of password attempts before a user is locked out.
- Multi-factor authentication (MFA), which involves an addition to the username and password, typically when a system is accessed from a different device or location. You are likely familiar with receiving a text code that must be used to access an account from a different computer.

With these criteria, simple passwords still cannot be used, and the recommended minimum number of characters is still eight for user-chosen passwords or six for randomly generated passwords or PINs. While the recommendation is not to impose composition rules, alphanumeric or special characters may still be used in an effort to create a memorable password that is not a dictionary word. Limiting the use of dictionary words definitely slows down password-cracking systems.

3. Take a layered approach.

It's important to note that the new guidelines are extensive, and this is just a summary of one aspect of them. While it may seem that the new guidelines make passwords easier for end users, there is much more to the authentication process than passwords.

And regardless of new recommendations, don't expect to see things change quickly. Many organizations use systems configured and managed by third parties, and it will take time to see industry-wide changes in response to these revised standards. Even if your organization wants to forego complex passwords for your users, it may not be an option until your systems catch up.

In the meantime, there are several steps you can take to protect your organization from weak passwords. These include:

- Layered security controls – With layered controls, if one fails, others are in place to help protect your organization. Many industry experts consider these "must have" additions to passwords for high-risk systems.
- Multi-factor authentication – Among security professionals, MFA has become a must-have layered control. The use of MFA for cloud-based systems is particularly critical because these systems can be accessed from any device through a browser. Thus a compromised password, whether discovered through a dictionary attack, keylogger or other spyware, or observed on a sticky note, can be used from just about anywhere.
- Ongoing training and communication – Make sure all network users understand why they:
  - Need to use strong passwords
  - Should not share passwords
  - Should not save passwords in an easily accessible location
  - Should not use the same password for multiple accounts

Even as cyberattacks have become increasingly sophisticated, the humble password remains a vital defense. The steps above will help you improve password security at your organization.

CapinTech offers expert cybersecurity services to organizations assess their information security controls and identify and address any risks and vulnerabilities. More information is available at capintech.com.

Weak passwords remain a top cybersecurity risk, as highlighted by recent large hacks and breaches.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA