Authentication Vulnerabilities

When it comes to protecting your information online, passwords are the most used form of website authentication. Password authentication requires users to create a key that only they (and the website) know as a way to access their online accounts.

The challenge: since passwords are so widely used, they’ve become obsolete. **Passwords are not only difficult to manage but also insecure because they can be easily guessed or cracked by hackers.**

Furthermore, if your business is using passwords to protect internal accounts and your user database, you and your user’s sensitive data could be at risk.

That’s why we’ve compiled a list of top password authentication vulnerabilities and ways your company can avoid them:

1. [Hackers can use brute-force attacks to crack password authentication.](https://swoopnow.com/password-authentication/#hackers)
2. [Password authentication is a user-generated security protocol.](https://swoopnow.com/password-authentication/#user-generated)
3. [Users have different password authentication credentials for every account.](https://swoopnow.com/password-authentication/#users)
4. [Password breaches make it difficult for users to protect their individual accounts.](https://swoopnow.com/password-authentication/#breach)

**1. Hackers Can Use Brute-Force Attacks to Crack Password Authentication**

**Password Authentication Vulnerability**



As technology evolves, so do the tools hackers use to crack people’s credentials. Aside from merely guessing your password, a brute-force attack is the most common technique hackers use.

**Simply put, a brute-force attack is when a hacker uses a computer program to run through every password combination until they find a match.** The system will run through all one-digit combinations, two-digit combinations, and so forth until it cracks your password.

To make matters worse, these systems are able to run through thousands of combinations in less than a second, which means that shorter passwords can be cracked in a very short time frame.

**Generally, hackers don’t use brute-force attacks to crack passwords on an individual level but rather to crack the key to the encryption code of a company’s user database,**[**compromising your website’s security**](https://swoopnow.com/passwords-wont-protect-websites/)**.** This method allows cybercriminals to obtain the credentials of multiple accounts all at once.

**Ways to Secure this Password Authentication Weakness**

The first thing your organization should do is ensure that hackers can’t use brute-force attacks for individual accounts. Companies can achieve this by limiting the number of login attempts and password reset requests for every account and IP address.

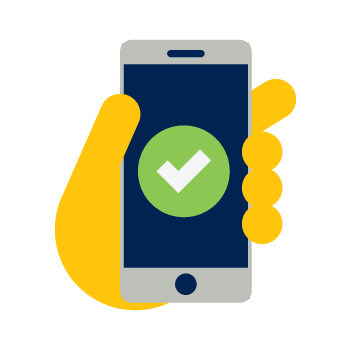
Your security team will need to establish a few standards before you can implement this process. For instance, you’ll need to ask yourself:

* **How many login attempts and password reset requests will each user and IP address receive?**The limit for IP addresses should be more than the limit for users. This is because multiple accounts could be using the same IP address like in an office setting.
* **How long will the account be temporarily blocked?**Once a user has reached the allowed number of requests, the account should be blocked for a short period of time. We recommend 10-15 minutes.
* **When should we block an IP address from making login attempts?**If there has been a lot of unusual behavior from a specific IP address, it might be in your website’s best interest to permanently block it from making login attempts.

In addition to making these changes, it’s also important that you encourage donors to create longer passwords. Credentials with more characters will take longer to crack.

## 2. Password Authentication Is a User-Generated Security Protocol

### Password Authentication Vulnerability

Since users have to create their own passwords, there’s always a chance they won’t create secure credentials. In fact, [around 90% of user-generated passwords](https://swoopnow.com/password-security-guide) are considered weak and easily vulnerable to hacking.

**Whether it’s because users want to have a password that’s easy to remember, aren’t up to date on password security best practices, or consciously (and subconsciously) use patterns to generate their passwords, this type of authentication has its flaws.**

Creating complex passwords is difficult because our minds are drawn towards patterns. Think about the passwords you create. It’s likely that they all follow a similar formula like using a word with numbers and a special character at the end. While these patterns make it easier for us to remember our credentials, cybercriminals are also aware of the common formulas people use to create passwords.

As a result, hackers can use this knowledge to input how their brute-force systems run through password combinations or crack your password making an educated guess.

**Another concern with user-generated passwords is that people don’t know if the passwords they’re using have already been compromised.** As a result, people continue to use weak and insecure credentials, and in many cases, passwords are the only thing protecting your users’ information.

### Ways to Secure this Password Authentication Weakness

Password authentication isn’t secure enough on its own because it puts the user in charge of protecting their information. Instead, organizations need to ensure their users’ data is protected in other ways.

If your website continues to use passwords in your [website authentication](https://swoopnow.com/website-authentication/), you should consider offering some alternative systems, like passwordless login social media sign-in options.

**Social media sign-in is an easy and effective way to offer your users a safer way to engage with your site.** Social media platforms already employ tighter security protocols than most other websites can offer, so the credentials tend to be relatively secure. Some users might shy away from these options, but offering them in addition to other authentication system will boost security all-around.

**Additionally, organizations should make a point to scan all newly created passwords through a list of commonly used or compromised credentials. When a user tries to create new credentials using a weak password, they’ll be asked to use a different credential.**

As a result, users are forced to create stronger passwords and avoid those that can be easily guessed.

**3. Users Need to Have Different Password Authentication Credentials for Every Account**

**Password Authentication Vulnerability**

Recent online security best practices suggest that users create passwords that are at least 8 characters (the ideal number is around 12 characters long) and use a combination of uppercase and lowercase letters, numbers, and symbols.

What’s more? Every password should follow these best practices and be unique to each account. This would be fine if users only had to juggle one or two accounts, but the reality is: people have an average of 27 online accounts and that trend is only projected to increase in upcoming years.

**The challenge with passwords is that in order for them to be secure, they need to be complex and unique. However, complex passwords are hard to remember, which means that passwords can’t be effective or user-friendly.**

Moreover, people can’t remember that many passwords, so they have to use other strategies store their credentials like a password management system. These tools allow users to store all their passwords in one place, generate new passwords, and auto-fill credentials when they land on a login screen.

**But, this solution has its risks as most of these tools require users to create an account with password-protection.**If a cybercriminal gets the password for your management tool, he’d have access to all your accounts.

**Ways to Secure this Password Authentication Weakness**

Password authentication is weak because of passwords themselves. As a result, organizations need to look into other ways to verify their users’ identities, also known as passwordless login options.

Passwordless login options allow organizations to remove passwords from the authentication process and require users to verify their identities using other methods.

**There are several different types of passwordless authentication, but three most common types are:**

* [Email authentication](https://swoopnow.com/password-alternatives/)
* [Token-based authentication](https://swoopnow.com/token-based-authentication/)
* [Biometric authentication](https://swoopnow.com/fingerprint-scanning/)

Swoop’s passwordless login technology uses email authentication to securely verify users. The process takes two steps:

1. After users press the login button, they’ll be redirected to a pre-written email that has instructions on their next steps and the details of their request.
2. To log in, users will have to hit “send” and wait for the system to grant them access.

Plus, our technology can be used to verify and confirm online payments, e-commerce purchases, and donations.

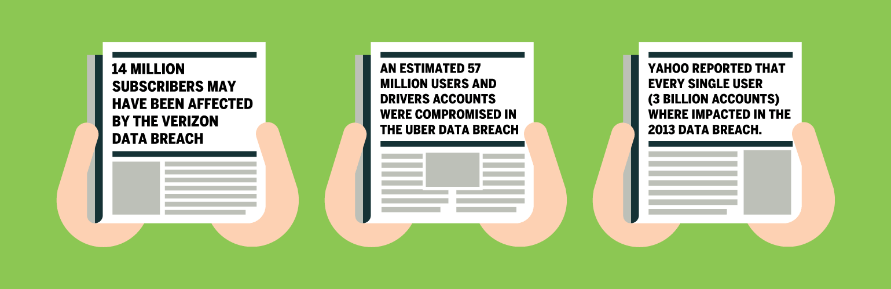
Behind the scenes, Swoop’s technology conducts three layers of security measures to determine if the email came from the correct user.**If the system suspects the request wasn’t made by the user, it will send a text message requesting the user to decline or approve the login attempt.**

**4. Password Breaches Make it Difficult for Users to Protect Their  Individual Accounts**

**Password Authentication Vulnerability**

As we mentioned earlier a hacker might attempt to crack an individual’s credentials, but the real goal is to get access to the website’s user database. Once hackers have cracked the code to your user database, they’ll have a list of all your users’ credentials, and as a result, no level of password security will be able to protect your users.

Password breaches are becoming a real concern for large and small organizations.



[Storing all of your users’ credentials puts you at risk](https://swoopnow.com/are-your-passwords-compromised/), and just encrypting the information isn’t enough.

**Organizations need to understand that weak internal passwords and storing credentials improperly could make a hacker’s job easier.**

Additionally, the password breaches of other companies could affect your organization’s security. Think about it: if you’re using a service from a company that recently had a password breach, your employees’ accounts could be compromised, which means your website’s users are also at risk.

**Ways to Secure this Password Authentication Weakness**

If your organization continues to use passwords as a [user authentication method](https://swoopnow.com/user-authentication/), it’s important that you store your passwords with more than use encryption. Credentials should be stored by:

* **Hashing your passwords.**Hash turns passwords into a random set of characters. Once the data has been hashed, it’s extremely difficult to decode the information. This is useful for passwords because they don’t need to be read back. When users log in, the same hashing will be applied and then compared to the information on file.
* **Salting your passwords.**This technique adds an extra value at the end of your passwords so that it’s harder to determine the actual password. For instance, the password “admin” would change to “admin+salt” when salt is added. For an additional security precaution, the salt added to each password should be random and unique. In general, salting occurs after a password has been hashed.

By salting and hashing your passwords, you’re adding another layer of protection to your database, which makes deciphering the information harder to achieve.

**Additionally, organizations need to implement the same password security best practices when creating internal accounts. In fact, using a passwordless login option isn’t just beneficial for your users.**

Since internal accounts are one of the common ways hackers gain access to user databases, your top priority should be making sure that these accounts can’t be easily cracked.

# Evaluting Strong authentication methods

But beyond that, why are companies still having this discussion? Usernames and passwords, on their own, are a vulnerable form of authentication. Passwords are forgotten, written down, and unintentionally disclosed to phishers adept at crafting email lures. Multifactor authentication ([MFA](https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA)) -- which requires verification from two or more independent credentials such as a password, security token or biometric identification -- may offer more layers of defense, but it is still not the norm. Why don't more enterprises adopt strong authentication methods? The answer may lie in uncertainty about the best technology options, [implementation strategies and costs](https://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-Procuring-multifactor-authentication).

### Strategic considerations

Start by understanding your use case. Is the user base small and focused on a small set of applications? A legal team within a large enterprise may have to deal with large volumes of confidential information stored in document management systems and e-discovery applications. A company may decide it wants to use, purchase and distribute a limited number of hardware devices for generating one-time passwords ([OTPs](https://searchsecurity.techtarget.com/definition/one-time-password-OTP)). A small number of users dealing with highly valuable data may justify more costly approaches than other scenarios.

Alternatively, companies that provide software as a service ([SaaS](https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service)) or have a large number of employees using [strong authentication methods](https://searchsecurity.techtarget.com/feature/Multifactor-authentication-products-CA-Strong-Authentication) may not find it practical to use specialized hardware and will opt for mobile device apps instead.

Consider how strong authentication will function with your existing authentication and identity management infrastructure. For example, if your enterprise has Active Directory Federation Services in Windows Server 2012, you can use certificate authentication or a third-party service, such as RSA SecurID Authentication Agent for Microsoft Active Directory Federation Services or Symantec Validation and ID Protection Service (VIP).

Cloud providers, such as Amazon Web Services and Microsoft Azure, are increasingly important components of enterprise infrastructure. Ideally, a strong authentication mechanism will work across on-premises and cloud platforms. Watch out for the need to support several MFA apps, such as [Symantec's VIP](https://searchsecurity.techtarget.com/feature/Multifactor-authentication-products-Symantec-Validation-and-ID-Protection-Service)for on-premises computer systems and Google Authenticator for AWS Multi-Factor Authentication.

Single sign-on (SSO) services, such as Okta and OneLogin, provide the benefits of [SSO](https://searchsecurity.techtarget.com/tip/What-factors-should-drive-your-choice-of-SSO-service) in cloud and SaaS environments. Consider how MFA will integrate with an SSO if you are using one. Does your SSO provider support your chosen MFA system? Do you want to deploy your MFA through the SSO provider if only a single application warrants MFA? This question can be especially important to ask if only a small number of users need access to sensitive applications and data that warrant MFA.

It is a well-understood practice in security to avoid proprietary algorithms related to encryption. Favor methods that are based on public standards, which have been subject to rigorous review. Proprietary algorithms may harbor unforeseen vulnerabilities.

Multifactor authentication will be new to many users who have become accustomed to working with usernames and passwords. They may be unfamiliar with MFA apps and devices, so support desks should be prepared for calls for assistance. Well-developed guides and tutorials on a self-service portal can help reduce the potential for a spike in support center calls.

An [MFA strategy](https://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-The-business-case-for-multifactor-authentication) complements passwords, it does not replace them. It is still important to enforce strong password policies. These policies should include limiting the lifetime of passwords, minimum length and character variety, limits on reuse and so on.

Strong authentication should be part of a broad set of information security practices that include separating and rotating duties, monitoring and logging events in identity management systems and performing routine audits.

### Authentication technology

Strong authentication methods typically involve dynamically generated OTPs or certificate- and context-based authentication.

The OTP employs a security device in the user's possession and a back-end server. The security device may be hardware-based, such as a tamper-resistant key fob, or software-based, such as a mobile phone app. One-time passwords may also be delivered to mobile phones using SMS. Both types of user device share a secret with the authentication back-end server. The secret is used to generate a time-limited OTP. Software-based devices have the advantage of easier distribution. Users simply need to download an app, and enterprises do not have the overhead of managing the physical inventory of key fobs.

There are two common approaches to OTP generation: time based and algorithm based. Time-based algorithms use the time, along with a shared secret or token, to generate a password. The [Time-Based One-Time Password Algorithm](https://tools.ietf.org/html/rfc6238) is an IETF standard for generating short-lived, one-time passwords. Non-time-based algorithms start with a seed value and hash function to generate passwords. After the initial password is generated, the prior password is used as input to generate the next password. Other OTP standards include the [S/KEY One-Time Password System](https://tools.ietf.org/html/rfc1760) (RFC 1760), [One-Time Password System](https://tools.ietf.org/html/rfc2289) (RFC 2289) and the [HMAC-Based One-Time Password Algorithm](https://tools.ietf.org/html/rfc4226).

Certificate-based authentication employs public key cryptography to generate public and private keys. Private keys may be stored on a portable device, such as a USB drive, or stored safely on a user's computer. Using a USB-based device mitigates the risk that a user will improperly secure a private key file, but adds the overhead of managing another physical device.

[Context-based authentication](https://searchsecurity.techtarget.com/definition/context-aware-security) uses information about a user, such as geographical location, to authenticate them. Context-based authentication is generally used in conjunction with other authentication methods. For highly secure environments, for example, a user may be required to provide a username, password, OTP and pass a verification on the geographical location of the device initiating the session. Other techniques include device registration or fingerprinting, source IP address reputation and behavioral analysis.

### Pitfalls to avoid

Authentication technology does not exist in a vacuum. Regardless of the mathematical rigor behind an authentication method, once it is deployed -- and is operating in the complex mix of users, applications and infrastructures -- vulnerabilities will be introduced. For example, [Trend Micro documented the case](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf) of attacks on European bank customers who were lured into downloading a malicious app purportedly designed to generate OTPs for their online banking accounts.