RESOURCE CENTER

Rapport sur l'état de la sécurité des mots de passe 2024

Comment les agences fédérales abordent la question de la sécurité des mots de passe

Get the full interactive view at
https://bitwarden.com/fr-fr/resources/the-state-of-password-security/

bitwarden

Assessing the State of Password Security within U.S. Federal Agencies

Recent years have brought an intense focus on cybersecurity across the United States Federal Government with many agencies leading the way in educating government organizations and businesses large and small, as well as consumers.

However, when it comes to password security, not every agency is singing the same tune. One of the foremost groups, the National Institute of Standards and Technology (NIST), "develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public."

The NIST cybersecurity page goes on to say that "some NIST cybersecurity assignments are defined by federal statutes, executive orders and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems."

Unfortunately, NIST's recommendations have not yet been universally accepted and implemented by all federal agencies. And while NIST sets the standards that agencies purport to follow, even it has its own weakness in the form of a disorganized website.

2024 marks the third year Bitwarden has conducted this analysis. Over the course of three years the NIST website has remained disorganized, although its content is very sound. There have also been a few positive developments. The White House has improved the dissemination of password security advice, going from a 'Room for Improvement' to a 'Good' rating. Other agencies that have trended in a better direction in terms of their password security recommendations and overall cybersecurity posture include the Cybersecurity and Infrastructure Security Association (CISA), the Federal Bureau of Investigation (FBI), the Federal Trade Commission (FTC), and the Small Business Administration (SBA).

This year, Bitwarden also added the Securities and Exchange Commission (SEC) to this report. Last year, the SEC adopted rules requiring companies disclose material cybersecurity incidents. Given the SEC's role in enforcing cybersecurity compliance, this report will assess the SEC's own password security advice.

Technology moves fast. For business and individuals, so much of our lives are now online in a myriad of accounts that range from fun entertainment sites to serious financial business like our bank accounts.

The goal of this assessment is to engage and educate everyone who uses passwords on the best practices coming from the federal government and where there is room for improvement. There are many within the federal government who have a solid educational approach to password security, and there are others that might need a bit of assistance to modernize.

Fortunately, consensus is building on best practices for password security. This report consolidates and assesses the details.

L'état de la sécurité des mots de passe : comment les agences fédérales abordent la question de la sécurité des mots de passe

Télécharger

View the State of Password Security Presentation

Table of Contents

Guideline to Password Security Ratings System

The rating system ranks agencies based on adherence to the following criteria:

Excellent

- Recommends use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is up-to-date and adheres to NIST guidelines
- Lays out password security recommendations in a clear, digestible, and easy-to-find manner

Very Good

- Recommends use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is up-to-date and adheres to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy-to-find manner

Good

- Does not recommend use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

Fair

- Does not recommend use of a password manager
- Calls out importance of strong passwords
- Does not consistently cite the need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

Room for Improvement

- Does not recommend use of a password manager
- Does not call out importance of strong passwords
- Does not cite the need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

National Institute of Standards and Technology (NIST)

NIST Risk Management Framework | IA-5(18)

Agency Advice:

- Authenticator Management | Password Managers
  - Employ [Assignment: Organization-defined password managers] to generate and manage passwords; and
    - Protect the passwords using [assignment: organization-defined controls].
    - For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords and storing the collection offline in a token.
- Reference

Digital Identity Guidelines

Agency Advice:

- Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed. A rationale for this is presented in Appendix A Strength of Memorized Secrets.
- Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well. To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length. Truncation of the secret SHALL NOT be performed. For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character.

- Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length and SHALL be generated using an approved random bit generator [SP 800-90Ar1].

- Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

- When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list MAY include, but is not limited to:
  - Passwords obtained from previous breach corpuses.
  - Dictionary words.
  - Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').
  - Context-specific words, such as the name of the service, the username, and derivatives thereof.

- If the chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret, SHALL provide the reason for rejection, and SHALL require the subscriber to choose a different value.

- Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret. This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets [Blacklists].

- Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.

- Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

- Verifiers SHOULD permit claimants to use "paste" functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets.

- In order to assist the claimant in successfully entering a memorized secret, the verifier SHOULD offer an option to display the secret — rather than a series of dots or asterisks — until it is entered. This allows the claimant to verify their entry if they are in a location where their screen is unlikely to be observed. The verifier MAY also permit the user's device to display individual entered characters for a short time after each character is typed to verify correct entry. This is particularly applicable on mobile devices.

- The verifier SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.

- Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function. Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. Examples of suitable key derivation functions include Password-based Key Derivation Function 2 (PBKDF2) [SP 800-132] and Balloon [BALLOON]. A memory-hard function SHOULD be used because it increases the cost of an attack. The key derivation function SHALL use an approved one-way function such as Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1], any approved hash function in SP 800-107, Secure Hash Algorithm 3 (SHA-3) [FIPS 202], CMAC [SP 800-38B] or Keccak Message Authentication Code (KMAC), Customizable SHAKE (cSHAKE), or ParallelHash [SP 800-185]. The chosen output length of the key derivation function SHOULD be the same as the length of the underlying one-way function output.

- The salt SHALL be at least 32 bits in length and be chosen arbitrarily so as to minimize salt value collisions among stored hashes. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator.

- For PBKDF2, the cost factor is an iteration count: the more times the PBKDF2 function is iterated, the longer it takes to compute the password hash. Therefore, the iteration count SHOULD be as large as verification server performance will allow, typically at least 10,000 iterations.

- In addition, verifiers SHOULD perform an additional iteration of a key derivation function using a salt value that is secret and known only to the verifier. This salt value, if used, SHALL be generated by an approved random bit generator [SP 800-90Ar1] and provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication). The secret salt value SHALL be stored separately from the hashed memorized secrets (e.g., in a specialized device like a hardware security module). With this additional iteration, brute-force attacks on the hashed memorized secrets are impractical as long as the secret salt value remains secret.

- Cybersecurity Awareness Month 2023 Blog Series
  - Agency Advice
    - Passwords are still the most widely used authentication mechanism for gaining access to resources of interest. Passwords are the frontline defense to protect data confidentiality and integrity against cybercriminals and data breaches. Good, strong passwords help people to stay secure and private online.

- Reference

NIST

bitwarden

National Institute of Standards and Technology (NIST)

Overall Bitwarden assessment: Very Good

- Recommends use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is up-to-date and adheres to NIST guidelines (NIST sets the standard for federal government security advice)
- Does not lay out password security recommendations in a clear, digestible, and easy-to-find manner

While advice is thorough and sets the standards for agencies accessing password guidelines via the website isn't intuitive. The advice is buried in very long PDFs and written in a way that isn't user-friendly.

The White House

A Proclamation on Cybersecurity Awareness Month, 2023

Agency Advice:

- "I call upon the people, businesses, and institutions of the United States to recognize and act on the importance of cybersecurity and to observe Cybersecurity Awareness Month in support of our national security and resilience. I also call upon business and institutions to take action to better protect the American people against cyber threats and create new opportunities for American workers to pursue good-paying cyber jobs. Americans can also take immediate action to better protect themselves such as turning on multifactor authentication, updating software on computers and devices, using strong passwords, and remaining cautious of clicking on links that look suspicious."
- Reference

Delivering a Digital-First Public Experience

Agency Advice:

- Agencies shall ensure websites that require the public to authenticate are compatible with commonly-used password managers, and shall not prevent the "pasting" of passwords or other automated, client-side assistive mechanisms.
- Reference

Readout of White House Multifactor Authentication Modernization Symposium

Agency Advice:

- "You need more than a password to stay safe online—and that's where multi-factor authentication steps in to ensure your data is better protected against malicious cyber actors," CISA Executive Director Brandon Wales said. "CISA has consistently urged organizations to implement MFA for all users to ensure any critical data is harder to access. Today's symposium is about coming together to map out the vision we are all striving towards making a reality."

- Reference

Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers

Agency Advice

- Acting under its authority to regulate wireless communication devices, the FCC is expected to seek public comment on rolling out the proposed voluntary cybersecurity labeling program, which is expected to be up and running in 2024. As proposed, the program would leverage stakeholder-led efforts to certify and label products, based on specific cybersecurity criteria published by the National Institute of Standards and Technology (NIST) that, for example, requires unique and strong default passwords, data protection, software updates, and incident detection capabilities.

- Reference

Good

bitwarden

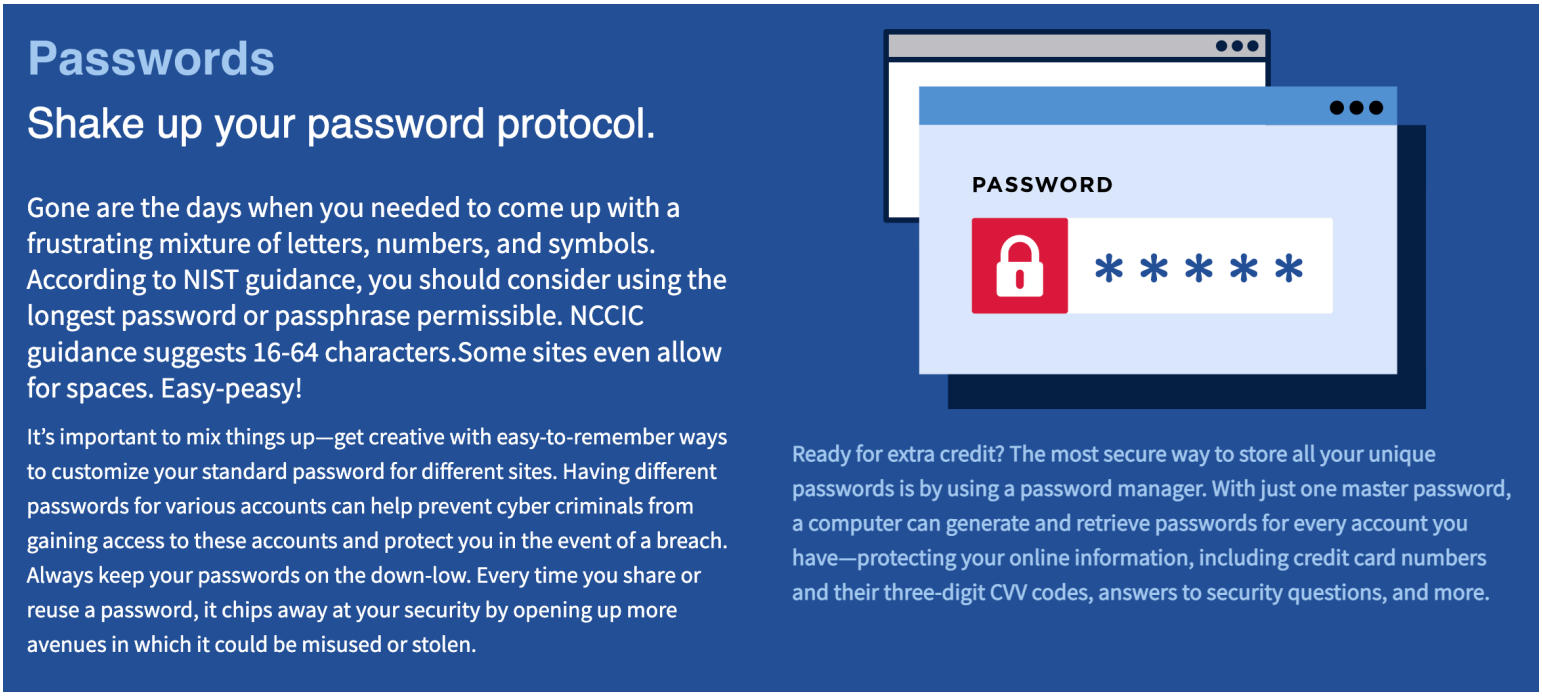
The White House

Overall Bitwarden assessment: Good

- Does not recommend use of a password manager
  - In a 2022 Cybersecurity Awareness Month communication, the White House recommended use of a password manager. The White House had the opportunity to do the same in the 2023 Cybersecurity Awareness blog. They did not. While the blog recommends 'using strong passwords', there is no mention of password managers.
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
  - In previous communications, the White House has recommended changing passwords, in contradiction to NIST advice. Passwords should only be changed if they are weak, reused, or have been compromised. A strong and unique password may never need to be changed unless you suspect it has been compromised.
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner
  - No dedicated cybersecurity page

Cybersecurity and Infrastructure Security Agency (CISA)

Cyber Lessons



Cyber lessons on passwords, CISA

- Reference

Stop Ransomware Guide

Agency Advice:

- Implement password policies that require unique passwords of at least 15 characters
    - Password managers can help you develop and manage secure passwords. Secure and limit access to any password managers in use and enable all security features available on the product in use, such as MFA.

- Reference

Secure Our World: Require Strong Passwords

Agency Advice:

- Small to medium businesses are a regular target for malicious hackers and a common entry point for digital thieves is stolen or weak passwords.
- But the good news is, you can keep your business safe by requiring employees to use strong passwords and password managers.
- Set the example by using long, random, unique passwords on all your personal and business accounts—and use a password manager to remember them! Then work with your IT staff or provider to require employees to use strong passwords to access your systems. This will keep your data safe and protected.
- Reference

Secure Our World: Weak Passwords

Agency Advice:

- Let a password manager do the work! A password manager creates, stores and fills passwords for us automatically. Then we each only have to remember one strong password—for the password manager itself. Search trusted sources for “password managers” like Consumer Reports, which offers a selection of highly rated password managers. Read reviews to compare options and find a reputable program for you.
- Reference

Very Good

bitwarden

Cybersecurity and Infrastructure Security Agency (CISA)

Overall Bitwarden assessment: Very Good

- Recommends use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is up-to-date and adheres to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy-to-find manner

The National Security Agency (NSA)

Stop Ransomware Guide

Agency Advice:

- Implement password policies that require unique passwords of at least 15 characters
  - Password managers can help you develop and manage secure passwords. Secure and limit access to any password managers in use and enable all security features available on the product in use, such as MFA.

- Reference

Cisco Password Types: Best Practices

Agency Advice:

- The rise in the number of compromises of network infrastructures in recent years is a reminder that authentication to network devices is an important consideration. Network devices could be compromised due to:
  - Poor password choice (vulnerable to brute force password spraying)
  - Router configuration files (which contain hashed passwords) sent via unencrypted email, or
  - Reused passwords (where passwords recovered from a compromised device can then be used to compromise other devices).

- Using passwords by themselves increases the risk of device exploitation. While NSA strongly recommends multi-factor authentication for administrators managing critical devices, sometimes passwords alone must be used. Choosing good password storage algorithms can make exploitation much more difficult.

- To provide as much protection as possible, use strong passwords to prevent them from being cracked and converted to plaintext. Comply with a password policy that:
  - Consists of a combination of lowercase and uppercase letters, symbols, and numbers;
  - Is at least 15 alphanumeric characters; and
  - Patterns that are not:
    - A keyboard walk
    - The same as a user name
    - The default password
    - The same as a password used anywhere else

  - Related to the network, organization, location, or other function identifiers
  - Straight from a dictionary, common acronyms, or easy to guess

- Reference

Keeping Safe on Social Media

Agency Advice:

- Secure and strengthen your passwords
  - Use unique and strong passwords for each online account. Reusing passwords across multiple accounts can expose data from all of the accounts if the password is discovered. Make sure that your password is of adequate length and complexity, using a combination of letters, numbers, and special characters. Where possible, implement multi-factor authentication using an authentication token or app so that someone can't access your account even if your password is compromised. Never share passwords and avoid using information that could be guessed based on your social media profiles or public information.

- Reference

Selecting Secure Multi-factor Authentication Solutions

Agency Advice:

- Single response, multi-factor authentication mechanisms require activation of the device, either with a PIN/password or biometric. The device provides 'what you have' and activation of the device implies that 'what-you-know' or 'what-you-are' has been verified.

- On the other hand, multi-step authenticators often include a password to provide 'what-you-know' and another authenticator that provides 'what-you-have'. U.S. Government agencies should consider requirements for PIN/password activation as well as for the passwords that are used directly to provide 'what-you-know'. Guidelines in SP 800-63-3 Part B indicate that memorized secrets (both for activation and as a single factor authenticator) must be at least 6-to-8 characters, and recommends higher password strength for user selected passwords. When determining password requirements, note that multi-factor devices should integrate strict thresholds to address password guessing attacks, whereas verifiers might employ less stringent threshold mechanisms that warrant passwords that are used directly have higher strength requirements.

- Reference

Good

bitwarden

The National Security Agency (NSA)

Overall Bitwarden assessment: Good

- Does not recommend use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and adheres to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy-to-find manner

Department of Homeland Security

CISA falls under the DHS

Cybersecurity page

Agency Advice:

- President Biden has made cybersecurity, a critical element of the Department of Homeland Security's (DHS) mission, a top priority for the Biden-Harris Administration at all levels of government.
- To advance the President's commitment, and to reflect that enhancing the nation's cybersecurity resilience is a top priority for DHS, Secretary Mayorkas issued a call for action dedicated to cybersecurity in his first month in office. This call for action focused on tackling the immediate threat of ransomware and on building a more robust and diverse workforce.
- In March 2021, Secretary Mayorkas outlined his broader vision and a roadmap for the Department's cybersecurity efforts in a virtual address hosted by RSA Conference, in partnership with Hampton University and the Girl Scouts of the USA.
- After his presentation, the Secretary was joined by Judith Batty, Interim CEO of the Girls Scouts, for a fireside chat to discuss the unprecedented cybersecurity challenges currently facing the United States. Dr. Chutima Boonthum-Denecke from Hampton University's Computer Science Department introduced the Secretary and facilitated a Q&A to close the program.
  - Overview of DHS Cybersecurity Sprints
  - Overview of Additional Ongoing Cybersecurity Priorities
  - Additional Information
- Reference

Room for Improvement

bitwarden

Department of Homeland Security

Overall Bitwarden assessment: Room for Improvement

- Does not recommend use of a password manager
- Does not call out importance of strong passwords
  - Offers inaccurate and misguided password security advice OR does not mention passwords or password security
  - Does not clearly call out password-related advice
- Does not consistently cite the need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

Federal Bureau of Investigation (FBI)

The Cyber Threat

Agency Advice:

- Internet-enabled crimes and cyber intrusions are becoming increasingly sophisticated and preventing them requires each user of a connected device to be aware and on guard.
- Keep systems and software up to date and install a strong, reputable anti-virus program.
- Be careful when connecting to a public Wi-Fi network and do not conduct any sensitive transactions, including purchases, when on a public network.
- Create a strong and unique passphrase for each online account and change those passphrases regularly.
- Set up multi-factor authentication on all accounts that allow it.
- Examine the email address in all correspondence and scrutinize website URLs before responding to a message or visiting a site
- Don’t click on anything in unsolicited emails or text messages.
- Be cautious about the information you share in online profiles and social media accounts. Sharing things like pet names, schools, and family members can give scammers the hints they need to guess your passwords or the answers to your account security questions.
- Don't send payments to unknown people or organizations that are seeking monetary support and urge immediate action.
- Reference

Scams and safety on internet

Agency Advice:

- **Keep your firewall turned on**

  A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

- **Install or update your antivirus software**

  Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

- **Install or update your antispyware technology**

  Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust.

- **Keep your operating system up to date**

  Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

- **Be careful what you download**

  Carelessly downloading email attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

- **Turn off your computer**

  With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

- Reference

Good

bitwarden

Federal Bureau of Investigation (FBI)

Overall Bitwarden assessment: Good

- Does not recommend use of a password manager
- Calls out importance of strong passwords
- Cites the need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

Federal Trade Commission (FTC)

Creating Strong Passwords and Other Ways to Protect Your Accounts

Agency Advice:

- Another option is to use a third-party password manager to create a strong password — and remember it. To find a reputable password manager, read expert reviews. Make sure the password you're using with the password manager is strong and secure. A web browser, mobile browser, and password manager all can save your passwords for you.

- A strong password is an important first step in protecting your account from hackers. But even strong passwords are vulnerable to cyberattacks. Using multi-factor authentication means a hacker who steals your password can't log in to your account without another authentication factor.

- The most common type of multi-factor authentication is a verification passcode you get by text message or email. This one-time passcode is typically six digits or longer and it expires automatically. But this is the least secure type of two-factor authentication, so choose a more secure method like an authenticator app or a security key for more protection, if you have the option.

- Reference

Password checklist

Agency Advice:

- **Make sure your password is long and strong.** That means at least 12 characters. Making a password longer is generally the easiest way to make it stronger. Consider using a passphrase of random words so that your password is more memorable, but avoid using common words or phrases. If the service you are using does not allow long passwords, you can make your password stronger by mixing uppercase and lowercase letters, numbers, and symbols.

- **Don't reuse passwords you've used on other accounts.** Use different passwords for different accounts. That way, if a hacker gets your password for one account, they can't use it to get into your other accounts.

- **Use multi-factor authentication when it's an option.** Some accounts offer extra security by requiring something in addition to a password to log in to your account. This is called multi-factor authentication. The "something extra" you need to log in to your account fall into two categories:
  - Something you have — like a passcode you get via an authentication app or a security key.
  - Something you are — like a scan of your fingerprint, your retina, or your face.

- **Consider a password manager.** Most people have trouble keeping track of all of their passwords. The longer and more complicated a password is, the stronger it is, but a longer password can also be more difficult to remember. Consider storing your passwords and security questions in a reputable password manager. To find a reputable password manager, search independent review sites, and talk to friends and family for ones that they use. Make sure to use a strong password to secure the information in your password manager.

- **Pick security questions only you know the answer to.** If a site asks you to answer security questions, avoid providing answers that are available in public records or easily found online, like your zip code, birthplace, or your mother's maiden name. And don't use questions with a limited number of responses that attackers can easily guess — like the color of your first car. You can even use nonsense answers to make guessing more difficult — but if you do, make sure you can remember what you use.
- **Change passwords quickly if there's a breach.** If a company tells you there was a data breach where a hacker could have gotten your password, change the password you use with that company right away, and on any account that uses a similar password.
- Reference

Excellent

bitwarden

Federal Trade Commission (FTC)

Overall Bitwarden assessment: Excellent

- Recommends use of password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is up-to-date and adheres to NIST guidelines
- Lays out password security recommendations in a clear, digestible, and easy-to-find manner

Department of Commerce

National Cybersecurity Month: Protecting Yourself Online

Agency Advice:

- Previously, the conventional wisdom was to create passwords using special characters, capitalization, numbers, letters, and a variety of arbitrary rules including forcing you to change your password multiple times per year. Research shows each of us did the same thing in response–re-used passwords or created variations of the same password because we'd been asked to memorize dozens of unique passwords for every site, log-in, or application.
- Our natural instincts created a weakness in our online security and cyber criminals took advantage. Research on the use of passwords has demonstrated the inherent weakness in expecting users to memorize arbitrarily complex passwords, and the importance of using multi-factor authentication (MFA) to safeguard our private information. Importantly, our thinking has evolved around this topic, and we've identified the following practices to better protect ourselves:
  - When you must use a password, use a longer password (15 or more characters) or even passphrases, as these provide greater protection than a shorter, arbitrarily complex password. Passphrases have the added benefit of being easy to remember.
  - Employing MFA (such as a one-time code emailed to you or an authenticator app on your phone) adds a second, critical layer to protect against a compromised password. MFA should be set up anytime it is available. It just takes a couple moments and will give you peace of mind.
  - Password managers, protected by one very strong, long password with MFA enabled, allow us to create unique passwords for each site without needing to memorize them all.
- Reference

NIST falls under the Department of Commerce

Agency Advice:

- Ensuring the security of our interconnected global networks, and the devices and data connected to those networks is one of the defining challenges of our era.
- The Department of Commerce is tasked with enhancing cybersecurity awareness and protections, protecting privacy, maintaining public safety, supporting economic and national security, and empowering Americans to better manage their safety online.
  - NIST Releases Version 1.0 of Privacy Framework
  - NIST Offers 'Quick-Start' Guide for Its Security and Privacy Safeguards Catalog
  - Small Business Cybersecurity Corner
- Reference

Department of Commerce

Overall Bitwarden assessment: Very Good

- Recommends use of a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Overall security advice is up-to-date and adheres to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy-to-find manner

Federal Communications Commission (FCC)

Cybersecurity tip sheet for small businesses

- Train employees in security principles. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.
- Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.
- Reference

10. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Fair

bitwarden

Federal Communications Commission (FCC)

Overall Bitwarden assessment: Fair

- Does not recommend use of a password manager
- Calls out importance of strong passwords
  - Links to content that focuses on password security
  - However, content is clearly outdated and could be more organized
- Does not consistently cite the need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
  - Against NIST guidelines, recommends changing passwords every three months
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

Small Business Administration (SBA)

Best practices for preventing cyberattacks

Agency Advice:

- Employees and their work-related communications are a leading cause of data breaches for small businesses because they are direct pathways into your systems. Training employees on basic internet usage best practices can go a long way in preventing cyberattacks.
  - Other training topics to cover include:
    - Spotting phishing emails
    - Using good internet browsing practices
    - Avoiding suspicious downloads
    - Enabling authentication tools (e.g., strong passwords, Multi-Factor Authentication, etc.)
    - Protecting sensitive vendor and customer information
- Reference

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone), and/or something that physically represents the user (fingerprint, facial recognition). Check with your vendors to see if they offer MFA for your various types of accounts (e.g., financial, accounting, payroll).

Good

bitwarden

Small Business Administration (SBA)

Overall Bitwarden assessment: Good

- Does not recommend use of a password manager
- Calls out importance of strong passwords
- Cites the need for 2FA/MFA to further support password security
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy-to-find manner

Securities and Exchange Commission (SEC)

In July 2023, the SEC "adopted final rules that will require public companies to disclose both material cybersecurity incidents they experience and, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance." Given the SEC's role in enforcing cybersecurity compliance, it seems prudent to assess the SEC's own password security advice.

A search for "password security" on the SEC.gov website reveals 12 documents, all of which appear to be from years ago. There is a page devoted to cybersecurity, but it offers fairly general recommendations repurposed from CISA. A cybersecurity risk alert from 2020 titled "Cybersecurity: Safeguarding Client Accounts against Credential Compromise" leads to a PDF that discusses credential stuffing. While the word "password" is used throughout, "password security is not explicitly mentioned. "Strong passwords" are referenced in the below context:

Cybersecurity: Safeguarding Client Accounts Against Credential Compromise

Agency Advice:

- As firms prepare for credential stuffing attacks, OCIE staff encourages firms to consider their current practices (e.g., MFA and other practices described above) and any potential limitations of those practices, and to consider whether the firm's customers and staff are properly informed on how they can better secure their accounts. Informed Customers Most firms require customers and staff to create and use strong passwords. However, the use of passwords is less effective if customers and/or staff re-use passwords from other sites. To be more effective, some firms have informed and encouraged clients and staff to create strong, unique passwords and to change passwords if there are indications that their password has been compromised.

> The Commission has noted that cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. In my view, artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate. All of these trends highlight investors' need for improved disclosure.

Fair

bitwarden

Securities and Exchange Commission (SEC)

Overall Bitwarden assessment: Fair

- Does not recommend use of a password manager
- Calls out importance of strong passwords
  - Links to dated content that acknowledges strong passwords but could be much more explicit
- Does not consistently cite the need for 2FA/MFA to further support password security
  - While 2FA/MFA is referenced in the PDF linked above, it is not prolific advice and requires some searching to find
- Overall security advice is not up-to-date and does not adhere to NIST guidelines
- Does not lay out password security recommendations in a clear, digestible, and easy to find manner

Summary

There are many steps you can take to stay safe online, but the simplest action with the most significant and immediate impact on your security is to use a password manager. Choose a cross-platform password manager with zero knowledge end-to-end encryption that can generate and store unlimited unique and strong passwords. You can get started with Bitwarden on a free account or opt for Premium for less than $10/year to get advanced features.

Additional Resources

- View the State of Password Security Presentation