The State of Password Security

A report and assessment of security advice from U.S. Federal Agencies
First published February 8, 2022

TABLE OF CONTENTS

Assessing the State of Password Security within U.S. Federal Agencies 3
Guideline to Password Security Ratings System 4
National Institute of Standards and Technology (NIST) 5
The White House 8
Cybersecurity and Infrastructure Security Agency (CISA) 11
Department of Homeland Security 13
Federal Bureau of Investigation (FBI) 15
Federal Trade Commission (FTC) 18
Department of Commerce 20
Federal Communications Commission (FCC) 22
Summary 24
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), offers excellent advice but its recommendations have not yet been universally accepted.

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.
Guideline to Password Security Ratings System

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

**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
- Lays out password security recommendations in a clear, digestible, and easy-to-find manner

**GOOD**
- 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

**FAIR**
- Calls out need for password security but does not mention 2FA/MFA
- Overall security advice is up-to-date and adheres to NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner

**ROOM FOR IMPROVEMENT**
- Offers inaccurate and misguided password security advice OR does not mention passwords or password security
- Does not adhere to NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner
# National Institute of Standards and Technology (NIST)

| ⊕ | Recommends use of password manager |
| ⊕ | Recommends best practices for securing passwords in a password manager |
| ⊕ | Calls out importance of strong passwords |
| ⊕ | Cites need for 2FA/MFA to further support password security |
| ⊕ | Sets the standard for federal government security advice |

- 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.

- Digital Identity Guidelines
  - Agency Advice:
    - 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.
    - 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.

- 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.

The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

- Something you know (e.g., a password).
- Something you have (e.g., an ID badge or a cryptographic key).
- Something you are (e.g., a fingerprint or other biometric data).

  ○ MFA refers to the use of more than one of the above factors. The strength of authentication systems is largely determined by the number of factors incorporated by the system — the more factors employed, the more robust the authentication system. For the purposes of these guidelines, using two factors is adequate to meet the highest security requirements.

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.

**National Institute of Standards and Technology (NIST)**

**Overall Bitwarden assessment: Very Good**

- Recommends use of a password manager and best practices for securing passwords within a password manager
- Calls out importance of strong passwords
- Cites need for 2FA/MFA to further support password security
- Sets the standards for federal government security advice
- While advice is solid, 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 consumer-friendly.
The State of Password Security 2022

The White House

- No clear tips for password security
- No guidance on how to generate and safely store strong & unique passwords
- Doesn’t adhere to NIST guidelines
- Information isn’t laid out in a clear, digestible, or easy-to-find manner
- No dedicated cybersecurity page

- Federal Zero Trust Strategy
  - Agency Advice:
    - MFA will generally protect against some common methods of gaining unauthorized account access, such as guessing weak passwords or reusing passwords obtained from a data breach.
    - Agencies are encouraged to pursue greater use of passwordless multi-factor authentication as they modernize their authentication systems. However, when passwords are in use, they are a “factor” in multi-factor authentication. If outdated password requirements lead agency staff to reuse passwords from their personal life, store passwords insecurely, or otherwise use weak passwords, adversaries will find it much easier to obtain unauthorized account access—even within a system that uses MFA.
    - Consistent with the practices outlined in SP 800-63B, agencies must remove password policies that require special characters and regular password rotation from all systems within one year of the issuance of this memorandum. These requirements have long been known to lead to weaker passwords in real-world use and should not be employed by the Federal Government. These policies should be removed by agencies as soon as is practical and should not be contingent on adopting other protections.

- Protecting against malicious cyber activity
  - Agency Advice:
    - Change Passwords and Mandate Multi-Factor Authentication (MFA). Ask your IT staff how long it has been since employees changed their passwords. Many criminals use stolen credentials, so forcing a reset (with
adequate length and complexity) before the holidays can deny malicious actors access to your systems. At the same time, confirm that your organization has implemented MFA and that it is required without exception. If you have MFA available, but are not requiring it, change that – require all staff to use the security technology that you have already acquired. MFA significantly reduces your risk from almost all opportunistic attempts to gain entry into key systems.

- **Fact sheet: Initiatives to bolster nation's cybersecurity**
  - **Agency Advice:**
    - Amazon announced it will make available to the public at no charge the security awareness training it offers its employees. Amazon also announced it will make available to all Amazon Web Services account holders at no additional cost, a multi-factor authentication device to protect against cybersecurity threats like phishing and password theft.

- **Memo to nation's leaders**
  - **Agency Advice:**
    - Implement the five best practices from the President's Executive Order: President Biden's Improving the Nation's Cybersecurity Executive Order is being implemented with speed and urgency across the Federal Government. We're leading by example because these five best practices are high impact: multifactor authentication (because passwords alone are routinely compromised), endpoint detection & response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses). These practices will significantly reduce the risk of a successful cyberattack.
Implement the five best practices from the President’s Executive Order:
President Biden’s *Improving the Nation’s Cybersecurity* Executive Order is being implemented with speed and urgency across the Federal Government. We’re leading by example because these five best practices are high impact: multifactor authentication (because passwords alone are routinely compromised), endpoint detection & response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses). These practices will significantly reduce the risk of a successful cyber-attack.

Screenshot 2: “Five Best Practices from the President’s Executive Order”
Reference

The White House

Overall Bitwarden assessment: Room for Improvement

- Lacking clear tips for password security
  - Highlights benefits of MFA and discourages password rotation, but does not offer guidance on how to generate and safely store strong and unique passwords.
  - Ransomware memo inaccurately states “passwords alone are routinely compromised” and does not clarify that only weak and reused passwords are routinely compromised.
  - No mention of password security in the May 2021 Executive Order on Improving the Nation’s Cybersecurity.
- Does not adhere to NIST guidelines
  - Still recommends 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.
- Information is not laid out in a clear, digestible, or easy-to-find manner.
  - No dedicated cybersecurity page
Cybersecurity and Infrastructure Security Agency (CISA)

- 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
- Could improve overall layout so password security advice is clear, digestible, and easy-to-find
- Relies on news releases (versus web page) to disseminate advice

● Reminder for critical infrastructure
  ○ Agency Advice:
    ■ Identify IT security employees for weekends and holidays who would be available to surge during these times in the event of an incident or ransomware attack.
    ■ Implement multi-factor authentication for remote access and administrative accounts.
    ■ Mandate strong passwords and ensure they are not reused across multiple accounts.
    ■ If you use remote desktop protocol (RDP) or any other potentially risky service, ensure it is secure and monitored.
    ■ Remind employees not to click on suspicious links, and conduct exercises to raise awareness.

● Preparing for and mitigating cyber threats
  ○ Agency Advice:
    ■ Increase organizational vigilance by ensuring there are no gaps in Information Technology (IT)/Operational Technology (OT) security personnel coverage and that staff provides continual monitoring for all types of anomalous behavior. Security coverage is particularly important during the winter holiday season when organizations typically have lower staffing.
■ Prepare your organization for rapid response by adopting a state of heightened awareness. Create, update, or review your cyber incident response procedures and ensure your personnel are familiar with the key steps they need to take during and following an incident. Have staff check reporting processes and exercise continuity of operations plans to test your ability to operate key functions in an IT-constrained or otherwise degraded environment. Consider your organization's cross-sector dependencies and the impact that a potential incident at your organization may have on other sectors, as well as how an incident at those sectors could affect your organization.

■ Ensure your network defenders implement cybersecurity best practices. Enforce multi-factor authentication and strong passwords, install software updates (prioritizing known exploited vulnerabilities), and secure accounts and credentials.

■ Stay informed about current cybersecurity threats and malicious techniques. Encourage your IT/OT security staff to subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

■ Lower the threshold for threat and information sharing. Immediately report cybersecurity incidents and anomalous activity to CISA and/or the FBI.

Ensure your network defenders implement cybersecurity best practices. Enforce multi-factor authentication and strong passwords, install software updates (prioritizing known exploited vulnerabilities), and secure accounts and credentials.

Screenshot 3: “Preparing For and Mitigating Potential Cyber Threats”

Reference

Cybersecurity and Infrastructure Security Agency (CISA)

Overall Bitwarden assessment: Good
- 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
- Could improve overall layout so password security advice is clear, digestible, and easy-to-find; relies on news releases (versus web page) to disseminate advice
# The State of Password Security

## Department of Homeland Security

<table>
<thead>
<tr>
<th>Room for Improvement</th>
<th>Doesn’t mention passwords or password security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Doesn’t promote NIST guidelines</td>
</tr>
<tr>
<td></td>
<td>Information is not laid out in a clear, digestible, or easy-to-find manner</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity web page is not conducive to security education</td>
</tr>
<tr>
<td></td>
<td>Directives or releases are fragmented and directed at specific industries</td>
</tr>
</tbody>
</table>

### 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](#)
Department of Homeland Security
Overall Bitwarden assessment: Room for Improvement

- Does not clearly call out password-related advice
- Doesn't promote NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner
  - Cybersecurity webpage is not conducive to security education
  - Directives or releases issues are fragmented and directed at specific industries
Federal Bureau of Investigation (FBI)

- Offers inaccurate and misguided password security advice
- Doesn't call out password advice on business and personal security web pages
- Mentions 2FA, but advice could be more clear and straightforward
- Minimal password advice
- Lack of alignment with NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner

● 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.

---

### How to Protect Your Computer

The same advice parents might deliver to young drivers on their first solo journey applies to everyone who wants to navigate safely online. A special agent in our Cyber Division offered the following:

- “Don’t drive in bad neighborhoods.”
- “If you don’t lock your car, it’s vulnerable; if you don’t secure your computer, it’s vulnerable.”
- “Reduce your vulnerability, and you reduce the threat.”

---

**Scams and Safety Business Emails**

- **Agency Advice:**
  - Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
  - Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
  - Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
The State of Password Security

Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.

Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.

Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.

Be especially wary if the requestor is pressing you to act quickly.

Federal Bureau of Investigation (FBI)

Overall Bitwarden assessment: Room for Improvement

- Offers inaccurate and misguided password security advice OR does not mention passwords or password security
  - Does not appear to clearly call out password-related advice on web pages that deal with business and personal security. As the 'lead federal agency for investigating cyberattacks and intrusions', one would expect that a major source of those attacks - password breaches - would be addressed
  - While it does mention 2FA, advice could be more clear and straightforward
- Minimal password advice
- Lack of alignment with NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner

1 https://www.fbi.gov/investigate/cyber
Federal Trade Commission (FTC)

- 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

● **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.

**Federal Trade Commission (FTC)**

**Overall Bitwarden assessment: Very good**

- 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-related recommendations in a clear, digestible, and easy-to-find manner
The State of Password Security

2022

Department of Commerce

Links to NIST guidelines, which emphasize passwords and password security

While easy-to-find, wading through links and PDFs means information is not easily digestible

NIST falls under the Department of Commerce

- Cybersecurity
  
  - 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

Cybersecurity

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.
Department of Commerce

Overall Bitwarden assessment: Fair

- Links to NIST guidelines, which emphasize passwords and password security
- While easy-to-find, wading through links and PDFs means information is not easily digestible
Federal Communications Commission (FCC)

- Calls out need for password security and mentions MFA
- Links to outdated and unorganized content that focuses on password security
- Recommends changing passwords every three months, against NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner
- Calls out threats, but does not offer solutions

- **Cybersecurity and network reliability**
  - **Agency Advice:**
    - The FCC’s responsibility is to ensure the reliability and resiliency of the Nation's communications network and to promote public safety through communications. The FCC, because of its relationship with the nation’s communications network service providers, is particularly well positioned to work with industry to secure the networks upon which the Internet depends.
    - Over the years, the FCC has worked through its Federal Advisory Committee, the Communications Security, Reliability, and Interoperability Council – CSRIC – to develop voluntary industry wide best practices that promote reliable networks, including for 911 calling. CSRIC and its working groups are made up of industry leaders, academics, and innovators in communications, Federal partners, public safety entities, state and local government officials, and Internet registries.
    - CSRIC will release a series of recommendations in March 2012 to address the most pressing threats to our cyber security, and suggest frameworks for possible solutions. We believe the most pressing cyber security threats are botnets, domain name fraud, and Internet route hijacking.

- **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 multifactor 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 multifactor authentication for your account.

**Federal Communications Commission (FCC)**

**Overall Bitwarden assessment: Fair**

- Calls out need for password security and mentions MFA
  - Links to content that focuses on password security
  - However, content is clearly outdated and could be more organized
- Recommends changing passwords every three months, against NIST guidelines
- Information is not laid out in a clear, digestible, or easy-to-find manner
  - Calls out threats, but does not define solutions
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 like 2FA and Emergency Access.