Authentication Advice Collection

Hazel Murray and David Malone

March 13, 2023

Abstract

This document lists each piece of advice that was collected for our study of the Costs and Benefits of Authentication Advice. This illustrates which pieces of advice were contained under each category and in each advice statement how all the pieces of advice were categorized. A star (*) at the beginning of the advice means it contradicts the statement it is listed under.

The categories are shown in alphabetical order. There were 27 categories of advice in total. This document will list every piece of advice collected under these heading categories. The categories are:

- Administrator Accounts
- Backup Password Options
- Backup Work
- Composition
- Default passwords
- Expiry
- Generated Passwords
- Individual Accounts
- Input
- Keeping system safe
- Keep your Account safe
- Length
- Network: SNMP Community strings
- Password Auditing
- Password Manager
- Personal Information
- Personal Password Storage
- Phrases
- Policies
- Reuse
- Sharing
- Shoulder surfing
- Storage
- Throttling
- Transmitting passwords
- Two factor authentication
- Username

1 Administrator Accounts

Administrator account not for everyday use

1. Do not use an account with administrator privileges for everyday use.

Password different for administrators account than users' other accounts

1. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
2. Administrators must use different passwords for their administrative and non-administrative accounts.

Give administrator accounts extra protection

1. Give administrators, remote users and mobile devices extra protection.

2 Backup Password Options

Email up-to-date and secure

1. Make sure your backup password options are up-to-date and secure.
2. Make sure to regularly update your recovery email address
3. Make sure your email password is also strong.

Security answers difficult to guess

1. The answer shouldn't be something that someone can guess by scanning information you've posted online on blogs or social networking profiles.
2. If you have to choose a question from a list of options, such as the city where you were born, try to find a way to make your answer unique.
3. Verifiers also SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

Do not store hints

1. Do not hint at the format of a password
2. Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.

3 Backup work

Make digital & physical back-ups.

1. Make electronic and physical back-ups or copies of all your important work.

4 Composition

Must include special characters

1. Use a mix of letters, numbers, and symbols.
2. Include numbers, capital letters and symbols.
3. Numbers, symbols and combinations of upper and lower case can be used.
4. Use a combination of upper & lower case letters, numbers and keyboard symbols.
5. Passwords less than 12 characters long should contain mixed case letters, digits, and symbols.
6. Use lower case, upper case, a number, and a special character.
7. Use combinations of numbers, symbols, and letters (uppercase and lowercase).
8. *No special characters.
9. *Passwords must not contain non-English characters.
10. *No spaces
11. *Spaces shouldn't be used as some applications may trim them away.
12. *The password cannot contain the space character.

Don't repeat characters

1. Passwords should not contain more than two (2) consecutive repeated characters.
2. Passwords must not contain repeating strings of 3 or more identical characters.
3. The password cannot contain three or more repeated characters.

Enforce restrictions on characters

1. Include upper and lowercase letters, and at least one number.
2. Contain at least 1 letter. Contain at least 1 number.
3. Use a mix of alphabetical and numeric characters.
4. Do not choose any all-numeral passwords.
5. Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.
6. The password should contain a minimum of one (1) non-alphabetic character.
7. Passwords should contain at least one number and at least one special character.

8. Must contain at least one non-alphabetic character and at least four alphabetic characters.
9. Passwords between 12 and 15 characters long (inclusive) should contain mixed case letters and digits.
10. Use a mixture of upper- and lowercase.
11. Use a mixture of upper- and lowercase.
12. Passwords 20 characters or longer can contain just a single case of characters.
13. *Verifiers SHOULD NOT impose other composition rules (mixtures of different character types, for example) on memorized secrets.

5 Default Passwords

Change all default passwords

1. Change the manufacturer's default passwords on all of your software.
2. Change all default passwords.
3. All vendor-supplied default passwords must be changed before any computer or communications system is used.
4. Make sure that absolutely no default administrator passwords are used.

6 Expiry

Store history to eliminate reuse

1. Enforce Password History. Set how frequently old passwords can be reused. Users are not allowed to reuse any of the stored passwords.
2. A password history must be maintained for all domain level.
3. On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previous fixed passwords.
4. Passwords must not be the same as the previous password.
5. The password cannot match any of the last eight passwords.

Change your password regularly

1. Passwords should be changed periodically.
2. Enforce a Maximum Password Age, users should change passwords regularly.
3. Change your password regularly.
4. Have a minimum Password Age
5. Password expiration should be enforced on all accounts.
6. Change your passwords regularly (every 45 to 90 days).
7. All user-level passwords must be changed at least every six months.
8. All system-level passwords must be changed on at least a quarterly basis.
9. *The routine changing of passwords is not recommended.
10. *Don't change your passwords, unless you suspect they've been compromised.
11. *Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)
12. *Normally, there should be no reason to change your password or PIN.

Change password if compromise is suspected

1. If you think that someone else knows your password, change it immediately.
2. Unless the accounts to which they apply have been hacked, in which case they should be changed immediately.
3. If you suspect that someone else knows your password, you should change it immediately.
4. Don't change your passwords, unless you suspect they've been compromised.
5. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
6. Unless there is evidence of compromise of the authenticator or a subscriber requests a change.
7. Only ask users to change their passwords on indication or suspicion of compromise.
8. Whenever an unauthorised party has compromised a system the relevant Autonomous network manager or application administrator must immediately change every password on the involved system.
9. Passwords must always be changed if it is known or suspected that another person has become aware of the password.

10. If you notice something suspicious on your PayPal account. You suspect that someone you don't trust has your password.

7 Generated Passwords

Create using a random bit generator

1. SHALL be generated using an approved random bit generator.
2. Must be generated using the low order bits of system clock time or some other frequently changing unpredictable source.

Must aid memory retention

1. Choose a scheme that produces passwords that are easier to remember.
2. Offer a choice of passwords, so users can select one they find memorable.

Generated passwords must be issued immediately

1. Generated passwords and pins must always be issued immediately after they are generated.

Only valid for first login

1. Generated password valid only for the involved user's first on-line session.

Distribute passwords in an envelope.

1. Passwords must be concealed inside an opaque envelope that will readily reveal tampering.

8 Individual Accounts

One account per user

1. Everybody who uses a computer should be assigned their own user account.
2. Applications must support authentication of individual users, not groups.
3. Computer and communication system access control must have passwords unique to each individual user.
4. Do not allow password sharing.

Accounts must be password protected

1. Each user account should be accessible only by entering a username and password.
2. Computer and communication system access control must be achieved via passwords.
3. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

9 Input

Truncation should not be performed

1. Truncation of the secret SHALL NOT be performed.

All ASCII and UNICODE characters should be accepted

1. 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.
2. *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.

10 Keeping system safe

Implement Defense-in-Depth

1. Implement Defense-in-Depth: a layered defense strategy includes technical, organizational, and operational controls.
2. Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorized use of stored passwords,

Implement Technical Defenses

1. Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.

Update anti-virus

1. Update your system's anti-virus software daily.
2. All devices connected to the Internet must be equipped with the latest versions of anti-virus software

Regularly apply security patches

1. Regularly download vendor security "patches" for all of your software.

Monitor and analyze successful and attempted intrusions

1. Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.

Boot protection

1. All workstations, no matter where they are located, must use screen-savers with fixed-password-based boot protection along with a time-out-after-no-activity feature.

11 Keep your account safe

Check for encryption and SSL

1. Check for encryption and SSL.-when accessing account.

Manually type URLs

1. Log on manually by typing what you know to be the site's URL into your browser window.

Don't open emails from strangers

1. Do NOT open emails, links, or attachments from strangers.

Keep software updated

1. Make sure you're using up-to-date anti-malware software
2. Make sure that your operating system is up-to-date.

Log out of public computers

1. When using a public computer, always sign out when your session is complete to prevent other people from accessing your account.
2. Don't forget to log out on a cybercafe computer.

Password protect your phone

1. Use a "password" or fingerprints for your phone too.

12 Length

Minimum password length

1. Set a minimum password Length. At least eight characters.
2. Minimum password length should be 8 characters.
3. The minimum password length is 8 characters.
4. Eight or more characters.
5. Length of 6 to 40 characters.
6. Make the password at least 8 characters long.
7. At least 8 characters in length.
8. More than 8 characters long.
9. Minimum of 8 characters.
10. All passwords must have at least eight (8) characters.
11. Passwords must be at least 9 characters long.
12. Do not choose passwords of fewer than six characters.

13. Choose a password with at least eight characters. If you want greater security, set the minimum password length to 14 characters.

Maximum password length (¡40)

1. Passwords should be no more than fifteen characters in length.
2. Maximum password length 40.
3. Less than 20 characters long.
4. *Verifiers SHOULD permit user-chosen memorized secrets to be at least 64 characters in length.

13 Network: SNMP Community strings

Don't define community strings as the standard defaults.

1. The community strings must be defined as something other than the standard defaults of public, private, and system

Community string must differ from login passwords.

1. The community strings must be different from the passwords used to log in interactively.

14 Password Auditing

Try guessing passwords

1. Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates.

15 Password Managers

Use a Password Manager

1. If you have a difficult time remembering multiple passwords, a trusted password manager may be a good solution.
2. An alternative to writing down passwords is to use an online password vault or safe. Use a Password Manager
3. *Password management software can help users, but carries risks.

Create long random passwords with password manager

1. Configure your password manager to create 30-50 random characters with a mixture of upper- and lower-case letters, numbers, and symbols.

16 Personal information

Password should be unrelated to personal information

1. Create a unique password that's unrelated to your personal information.
2. Don't use family members' or pets' names. Or family birthdays. Or your favorite football or F1 team or other words easy to work out with a little background knowledge.
3. A car license plate number, a spouse's name, or an address must not be used.
4. Not a word or date associated with you (like a pet's name, family names, or birth dates).
5. Don't use any personal information. Even when combined with letters and numbers, someone who knows you, or can research you online, can easily guess a password with this information.
6. *Personal details such as spouse's name, vehicle license plate, PPS or social security number and birthday must not be used unless accompanied by additional unrelated characters.

Passwords must not match account information

1. Do not choose any ID number or user ID in any form, even spelled backwards.
2. Passwords can't contain the username.
3. Passwords must not contain your LoginID
4. Passwords must not contain any email address on record for the user profile.
5. The password cannot contain email address.
6. Can not match username.

7. Don't use your username or business name.
8. Do not choose part of your userid.

Do not include names

1. Do not choose your name in any form - first, middle, last, maiden, spelled backwards, nickname or initials.
2. Do not choose any common name, e.g., Sue, Joe.
3. Passwords can't contain parts of the user's full name such as his first name.
4. The password cannot contain your name.
5. Don't use your actual name
6. Do not choose part of your name.
7. *You could use someone else's mother's maiden name.

17 Personal Password Storage

Don't leave passwords in plain sight

1. Don't leave notes with your passwords to various sites on your computer or desk.
2. Don't post it in plain sight.
3. Do not write passwords down and store them anywhere in your office.
4. Passwords must not be written down and left in a place where unauthorised persons might discover them.

Don't store in a computer file

1. Don't store passwords in a document on your computer.
2. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without Encryption.
3. *If you decide to save your passwords in a file on your computer, create a unique name for the file so people don't know what's inside.

Write down safely

1. If you must write it down, hide the note somewhere where no one can find it.
2. If you must write passwords down in order to remember them, encrypt them in a way that is familiar to you but makes them indecipherable by others.
3. If you have to keep your passwords somewhere, it is safer to write them on a piece of paper and store that paper in a secure location, like a safe.
4. The display and printing of passwords should be masked, suppressed, or otherwise obscured.
5. Store unrecoverable passwords.
6. Allow users to securely record and store their passwords.
7. *Don't write down your password

Do not allow applications to remember your password

1. Don't save your passwords in a web browser.
2. Do not use the "Remember Password" feature of applications (for example, web browsers).
3. Don't save passwords or use "Remember Me" options on a public computer.

18 Phrases

Don't use patterns

1. Don't use keyboard patterns such as qwerty or qazwsx,
2. Dont use sequential patterns such as abcd1234
3. Don't use numerical sequences.
4. Don't use repetitive patterns on the keyboard.
5. Common character sequences must not be employed.
6. Do not use ascending or descending numbers (for example 4321 or 12345), duplicated numbers (such as 1111) or easily recognisable keypad patterns (such as 14789 or 2580).

Blacklist common passwords

1. Prohibit the most common passwords by blacklisting.
2. Verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised.

Don't use published phrases

1. Don't use song lyrics, quotes or anything else that's been published.
2. Do not choose names from popular culture, e.g., Harry_Potter, Sleepy.
3. *Choose a line of a song that other people would not associate with you.

Substitute symbols for letters

1. Consider using symbols and numbers in place of letters.
2. Replace a letter with another letter, symbol or combination, but don't be too obvious about it.
3. *Do not choose any word with any of the following substitutions: a → 2, a → 4, e → 3, h → 4, i → 1, l → 1, o → 0, s → $, s → 5, z → 5

Don't use a single word

1. Don't use a single commonplace dictionary word
2. Do not choose acronyms, geographical or product names, and technical terms.
3. Do not choose a single word either preceded or followed by a digit, a punctuation mark, up arrow, or space.
4. Passwords must not be a word found in the dictionary or some other part of speech.
5. Dont use Words like password or letmein
6. Don't use the word password
7. Compare the prospective passwords against a list of known commonly-used, expected, and/or compromised values.
8. Prohibit the most common passwords by blacklisting.
9. Pick a deliberately misspelled term
10. Words in a dictionary must not be employed.
11. User-chosen passwords must also not be any part of speech.
12. Pick an odd character in an otherwise familiar term, such as phnybon instead of funnybone
13. Choose an easily phonetically pronounceable nonsense word.
14. Combine random words.
15. Combine random words to create a passphrase.
16. Choose a combination of two unrelated words.

Insert random numbers and symbols

1. Do use a random word or phrase and insert letters and numbers into the beginning, middle, and end.
2. Chose a phrase and pad with symbols, uppercase letters and numbers.
3. Two words separated by a non-alphabetic, non-numeric, or punctuation character.
4. A combination of words with unusual capitalization, numbers, and special characters interspersed.
5. *Don't use passwords with combinations of random letters, numbers and symbols. e.g. jal43#Koo%a.

Take initials of a phrase

1. Use a phrase and use the initial of each word.
2. Pick a phrase known to you and take the first character from each word.
3. Take initials of a phrase and swap letters for numbers.
4. Initials of an easy to remember quote of phrase.

19 Policies

Establish clear policies

1. You should set account policies that define a secure password for your systems.
2. Establish clear policies and procedures for employee use of your organization's information technologies.

20 Reuse

Never reuse a password

1. Use a different password for every website
2. Don't use the same password twice
3. It's important to use unique passwords for each different online account.
4. Where possible, users must not use the same password for various access needs.
5. Avoid reusing old passwords.
6. Don't recycle passwords.

Alter and reuse passwords

1. Users must not use a basic sequence of characters that is then partially changed based on some predictable factor.
2. Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change.
3. Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.
4. *Incorporate the first few letters of the website name into your password so that every password is different.
5. *Add a couple of unique letters for each site.
6. *Select a single memorable base password and alter it to form derivations

Don't reuse certain types of passwords

1. Use a unique password for each of your important accounts.
2. Never use your Apple ID password with other online accounts.
3. Users must not use the same password for Company accounts as for other non-Company accounts.
4. Users should never reuse passwords between work and home.
5. Passwords used for Internet services should not be the same or similar to passwords used for services accessed within College.

21 Sharing

Don't share your password with anyone.

1. Don't share your Apple ID with other people, even family members.
2. Never give out your password to anyone.
3. Never disclose your passwords to anyone else.
4. Don't share your passwords.
5. Passwords must not be shared with anyone.
6. Do not share passwords with anyone,
7. Do NOT give any of your usernames, passwords, or other computer/ website access codes to anyone.
8. Never share your Maynooth University password with anyone.
9. Passwords must never be shared or revealed to anyone else besides the authorized user.

Don't send password by email

1. Do not send your password by email.
2. Don't send your password to anyone in an email.
3. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

Don't share passwords over the phone.

1. Passwords must not be revealed over the phone to anyone.

22 Shoulder surfing

Offer to display password

1. Verifier SHOULD offer an option to display the secret (rather than a series of dots or asterisks, typically) as it is typed.

Conspicuously enter password.

1. Make sure no one sees you typing your password.
2. Don't enter your password when others can see what you are typing.

23 Storage

Encrypt passwords

1. Store Password Using Reversible Encryption For All Users enable the option on a per-user basis and then only as required to meet the user's actual needs.
2. Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications system.
3. Passwords must always be encrypted (non-clear text) when held in storage for any period of time
4. Never store passwords as plain text.
5. The verifier SHALL use approved encryption.
6. Applications must not store passwords in clear text or in any easily reversible form.
7. Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover them.

Restrict access to password files.

1. Restrict access to files that contain passwords.
2. Ensure you protect files containing encrypted or hashed passwords from unauthorized system or user access.

Encrypt password files

1. Encrypt files that contain passwords.

Store password hashes

1. Store one-way cryptographic hashes for passwords instead of storing the passwords themselves.
2. Produce hashed representations of passwords using a unique salt for each account.
3. Store passwords in a hashed format
4. Secrets SHALL be hashed with a salt value using an approved hash function.

Don't hardcode passwords into software

1. To allow passwords to be changed when needed, passwords should not be hard-coded (incorporated) into software.

Contractual agreements should stipulate how credentials are protected

1. When outsourcing, contractual agreements should stipulate how user credentials are protected.

24 Throttling

Throttle password guesses.

1. Lock out a user account after a number of consecutive failed authentication attempts.
2. Have a fixed or exponentially increasing delay after each failed authentication attempt.
3. Verifiers SHALL implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account.
4. Allow users around 10 login attempts before locking out accounts.
5. The number of consecutive attempts to enter an incorrect password must be strictly limited.
6. The number of consecutive attempts to enter an incorrect password must be strictly limited.

25 Transmitting passwords

Do not transmit clear text password

1. Applications must not transmit passwords in clear text over the network.

Request passwords over a protected channel

1. The verifier SHALL utilize an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and man-in-the-middle attacks.

26 Two factor Authentication

Use for remote accounts

1. Consider implementing two factor authentication for all remote accounts.

Use multi-factor authentication

1. Consider using multi-factor authentication.

Enable two factor authentication using phone

1. Enable two step verification with your phone.

27 Username

Enforce Composition Restrictions

1. Lower case only, no spaces, no special characters. Contain a minimum of 3 letters and 3 numbers. Length of 8 or 9 characters

Don't reuse usernames

1. Any username used for the Internet services should not be the same or similar to a College username.