The CENTRE for EDUCATION
in MATHEMATICS and COMPUTING

Password Hygiene

A CS and Society resource addressing social and economic issues within the realm of digital technology and computing

This resource will:

- emphasize the importance of having good password habits, and
- provide you with suggestions and strategies to strengthen your online credentials.

Passwords

A password is a secret string of characters that is used to verify your identity when accessing an account or a device.

Passwords are important because they:

- Prevent unauthorized access
- Keep personal and sensitive data safe
- Protect against theft and fraud

Password Hygiene

A set of habits for creating and managing secure passwords. Good password hygiene can reduce the risk of cyberattacks, similar to how good personal hygiene can reduce the risk of illness.

Password Trivia

Are you a password pro? This quiz will put you to the test through surprising password statistics and quirky fun facts such as the first recorded password in written history and the most commonly used password worldwide.

QUIZ

Weak Passwords

A weak password is one that is vulnerable to being discovered, either through theft, through guessing, or through advanced hacking techniques. A password is weak if:

- It is short in length
- It is unchanged from a default password (such as admin)
- It can be found in a dictionary
- It is a predictable sequence of numbers (such as 123456)
- It is a keyboard swipe (such as qwerty)
- It lacks complexity (such as only using letters)
- It contains personal information (such as names or dates)
- It is reused across multiple accounts
- It is written down in an easily noticeable place

Password Cracking

Cybercriminals have many tools at their disposal to crack user passwords and gain unauthorized access to accounts and private information.

The following article describes 12 different techniques used by modern day hackers. After reading the article, complete the *Password Cracking Crossword* found under additional materials.

ARTICLE

Strong Passwords

When it comes to passwords, length equals strength! The current recommendation is to use a password that is at least 16 characters long.

Password	Description	Time to Crack
ku9$@f	6 characters	?
8gt##v2D	8 characters	?
CFsz76.Deb*	11 characters	?
aE:2HsX3-pMn!	13 characters	?

Use Bitwarden's *Password Strength Testing Tool* to examine how the following passwords perform against a brute force attack.

Bitwarden

Memorable Passwords

Creating a long and strong password that is also memorable is a challenge. One strategy is to design a password around a memorable sentence by taking the first letter of each word. For added complexity, you can include numbers and symbols as well.

Starting with this quote from Shakespeare's *Hamlet*:
"Alas, poor Yorick! I knew him, Horatio: a fellow of infinite jest"

A password could be: `A,pY!Ikh,H:afo8j`

Don't be too obvious! If you are a Taylor Swift fan, basing a password on her songs becomes guessable.

Password Match-Up

In small groups, try to match these passwords to the inspirations behind them.

`Ihadtm4lcw1dlianwtwnbjbtcotsbbtcotc.`	Alfred, Lord Tennyson
`@1stIwa,Iwp.Kt'Icnlwubms.`	Dr. Martin Luther King Jr.
`Lilaboc.Ynkwygg.`	Gloria Gaynor
`Uslucawal,0ig2gb.In.`	Inigo Montoya
`'Tb2hl&ltn2hl@a.`	Forrest Gump
`H.MniIM.Ykmf.P2d.`	The Lorax

Password Match-Up (Answers)

In small groups, try to match these passwords to the inspirations behind them.

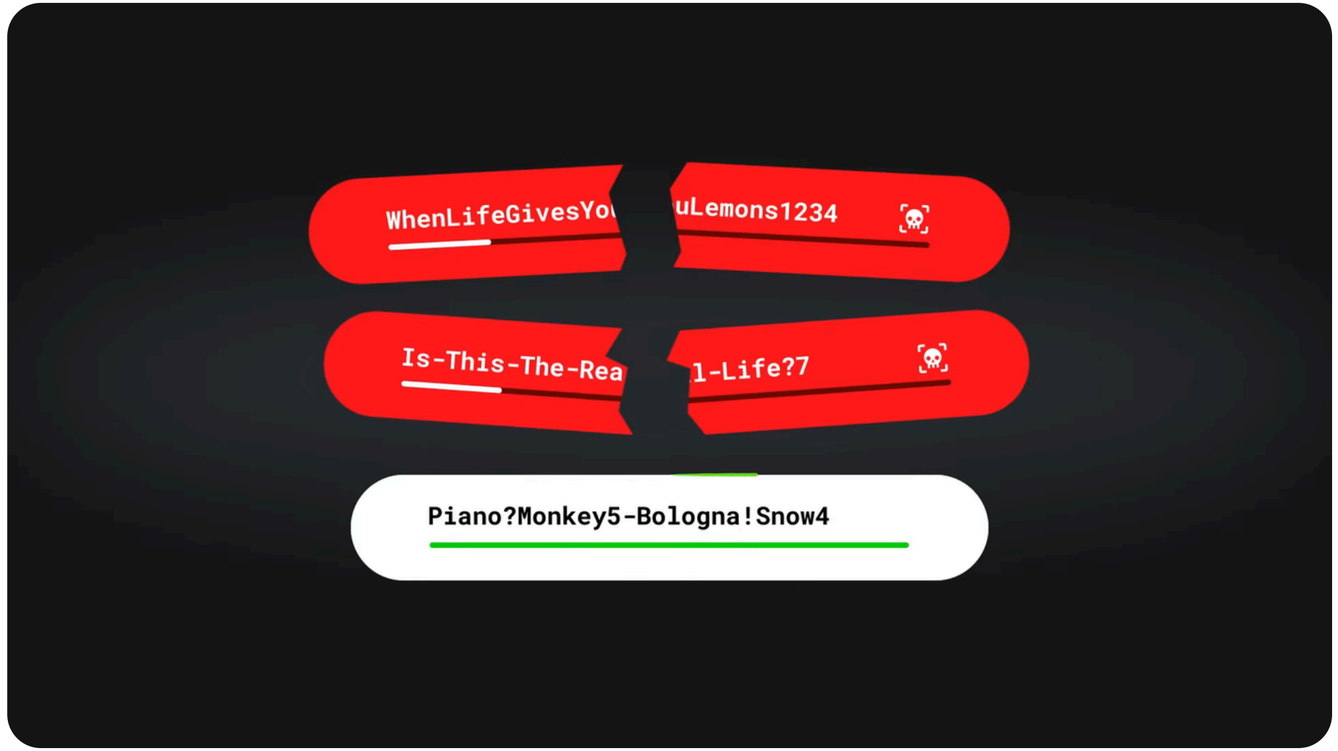
`Ihadtm4lcw1dlianwtwnbjbtcotsbbtcotc.`	Dr. Martin Luther King Jr.
`@1stIwa,Iwp.Kt'Icnlwubms.`	Gloria Gaynor
`Lilaboc.Ynkwygg.`	Forrest Gump
`Uslucawal,0ig2gb.In.`	The Lorax
`'Tb2hl&ltn2hl@a.`	Alfred, Lord Tennyson
`H.MniIM.Ykmf.P2d.`	Inigo Montoya

- I have a dream that my four little children will one day live in a nation where they will not be judged by the color of their skin but by the content of their character. (Dr. Martin Luther King Jr.)
- At first I was afraid, I was petrified. Kept thinkin' I could never live without you by my side. (Gloria Gaynor)
- Life is like a box of chocolates. You never know what you're gonna get. (Forrest Gump)
- Unless someone like you cares a whole awful lot, nothing is going to get better. It's not. (The Lorax)
- 'Tis better to have loved and lost than never to have loved at all. (Alfred, Lord Tennyson)
- Hello. My name is Inigo Montoya. You killed my father. Prepare to die. (Inigo Montoya)

Passphrases

Another type of long, memorable password is a passphrase. The following video provides some great tips on how to create passphrases that provide strong security.

VIDEO



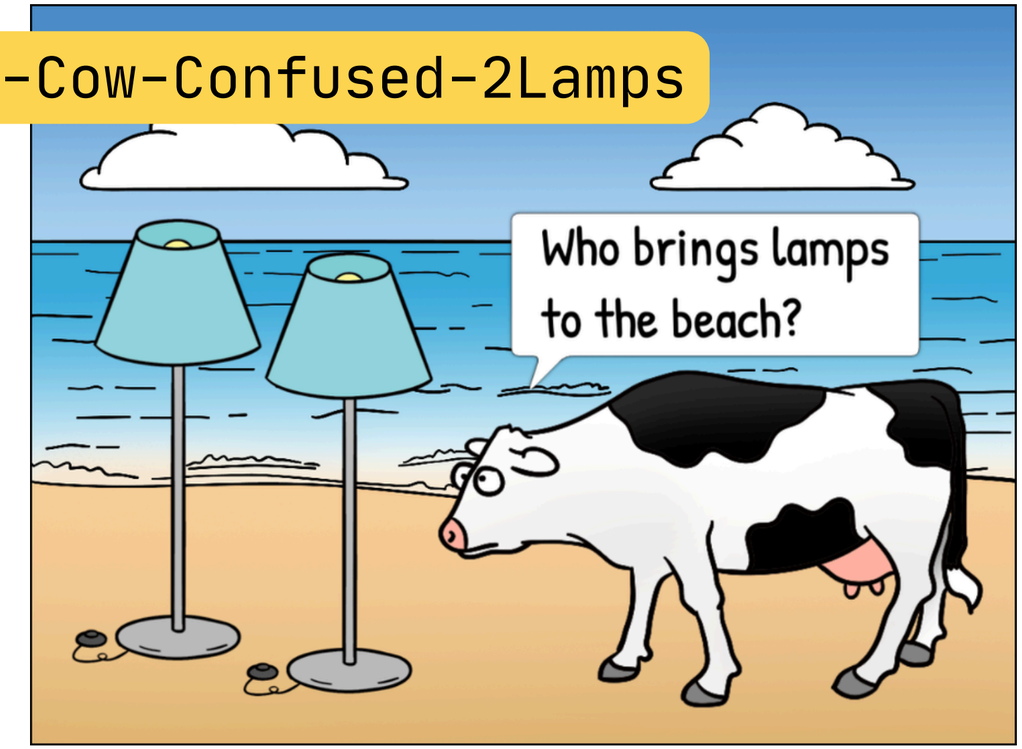
DID YOU KNOW?

Spaces count as characters too!

Create a Passphrase

In the *Create a Passphrase* activity found under additional materials, practice creating a long passphrase and a corresponding image that can help you remember it.

`@Beach-Cow-Confused-2Lamps`



The passphrase you design for this activity will be shared within your class. Do not use this passphrase for any of your real-life accounts!

Best Practices

Security starts with strong passwords (or passphrases), but they need to be combined with good password hygiene habits to offer true protection.

- Set a unique password for each of your accounts
- Do not save passwords on shared devices
- Do not share your passwords with others
- Avoid logging in to accounts while using public Wi-Fi
- Always log out of accounts when done
- Never click on suspicious links or attachments

BONUS TIP!

Use a Password Manager with Two-Factor Authentication

Damage Control

If you suspect that a password of yours has been compromised, here are some action items to help you minimize the impact. **The most important step is to act quickly!**

LOCK Immediately change the password, and update any other accounts that use the same one. Add an extra layer of security by enabling Two-Factor Authentication (2FA).

CLEANSE Make sure your antivirus software is up to date and scan your devices for the presence of malware.

AUDIT Monitor your account activity. Look for unrecognized logins, password reset requests that you did not initiate, or messages that you did not send.

ALERT Notify your contacts about the breach so they don't fall for scams coming from your account.

The Future of Passwords and Security

Multi-Factor Authentication (MFA)

2FA uses 2 pieces of identification. Typically those are something you *know* (password) and something you *have* (a code sent to your phone). MFA adds more pieces. These can include something you *are* (biometrics) or *somewhere* you are (geolocation data).

Security Questions

Personal questions such as your mother's maiden name are becoming less useful. They can be easily guessed or discovered. Instead, on-the-fly questions based on recent user activity may be asked instead. For example, "which website did you visit earlier today?"

Passkeys

Passkeys are 'wordless' and 'typeless' ways to log in. Your device itself becomes the key necessary to enter your account. The device may use biometric markers such as asking for your fingerprint, or an embedded pin code such as your screen unlock pattern.

Behaviour Profiling

This trend relies on patterns to verify your login. It can monitor things such as your typing speed and rhythm, how you hold your phone, and the way you swipe and scroll. When an account detects a deviation from your usage patterns it triggers an automatic lockdown.

Questions for Continued Discussion

1. Is it ever ethical to crack a password?
2. When choosing a password, do you gravitate more towards convenience or more towards security?
3. Many browsers offer to save your passwords for you. Is this a good idea?
4. Is two-factor authentication a failsafe method for identifying someone? What about multi-factor authentication?
5. How accurate are biometric markers? Can they be spoofed?
6. Can password managers be trusted? How do you feel about putting all your credentials in a single place behind a single password?
7. When someone has died, how should their passwords be handled?

Further Resources

Explore the Government of Canada's Get Cyber Safe campaign.

In particular:

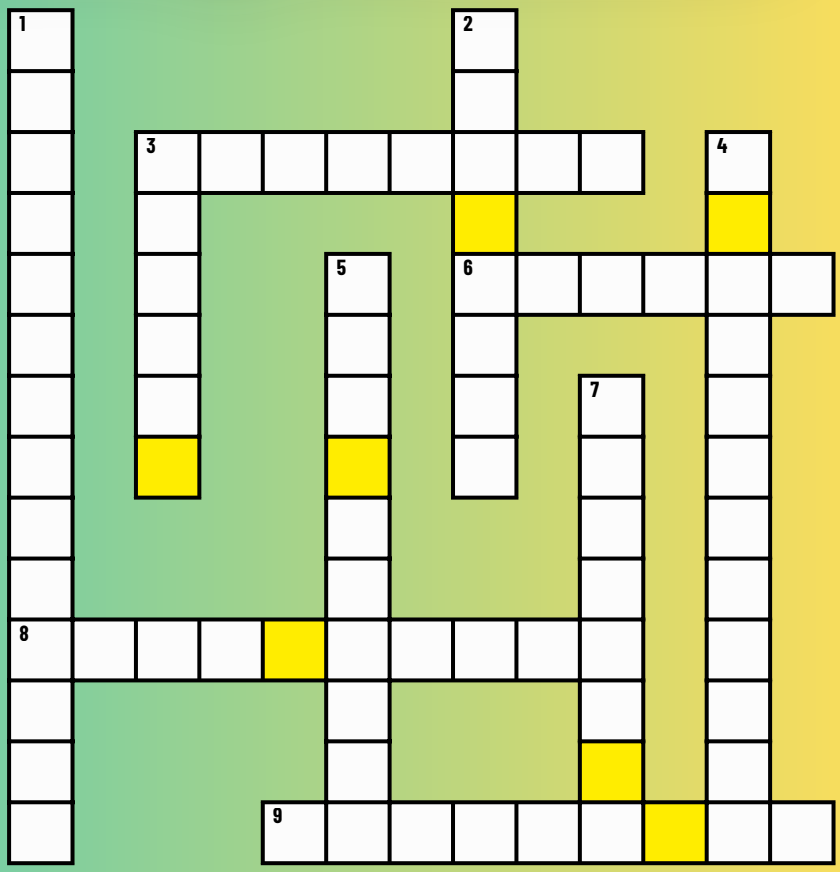
- Passphrases, passwords and PINs
- Multi-factor authentication
- Password managers
- Social media

Discover how easy it can be to guess someone's password by playing Passwordle.

Check whether your personal data has been exposed in a data breach using Have I Been Pwned.

Additional Materials

Password Cracking Crossword



ACROSS

[3] Credential ____ is when a stolen username and password combination is tested across multiple different websites.

[6] This type of attack starts with a known base word and then tests variations of the base word by appending or prepending numbers and symbols.

[8] This type of attack guesses likely passwords using the fact that humans tend to use common words and patterns.

[9] A ____ is a device that secretly records keystrokes.

DOWN

[1] Password credentials that are shared over an unsecured Wi-Fi network are vulnerable to ____ attacks.

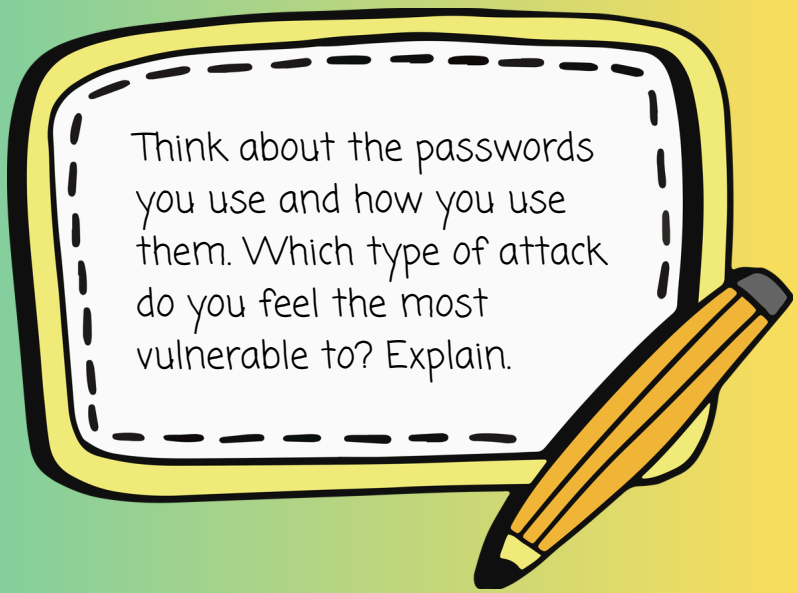
[2] Sending a fake message that tricks users into revealing their account credentials is called ____.

[3] Calling an IT help desk and pretending to be a legitimate account holder who needs a password reset is an example of a ____ engineering attack.

[4] This type of attack uses a precomputed table that maps hashes to passwords in order to quickly reverse a stolen hash.

[5] This type of attack involves trying every possible combination of characters.

[7] Trying a single, common password against multiple user accounts is called password ____.

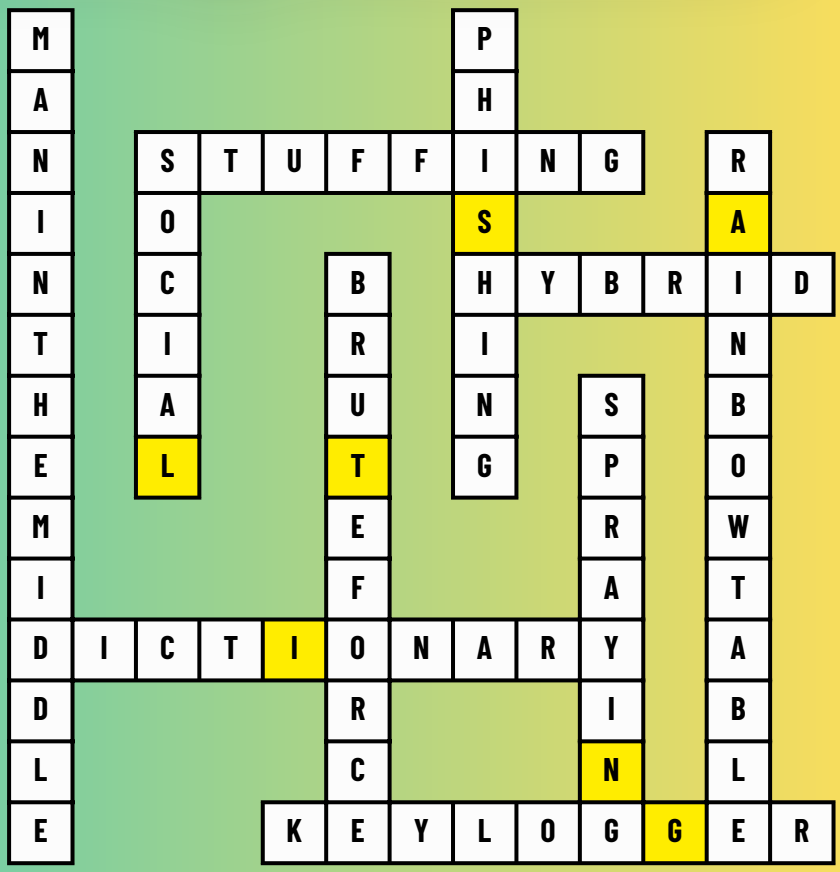


BONUS CLUE

Adding random characters to a password before it is hashed is known as ____.

Activity to accompany slide: *Password Cracking*

Password Cracking Crossword



ACROSS

[3] Credential ____ is when a stolen username and password combination is tested across multiple different websites.

[6] This type of attack starts with a known base word and then tests variations of the base word by appending or prepending numbers and symbols.

[8] This type of attack guesses likely passwords using the fact that humans tend to use common words and patterns.

[9] A ____ is a device that secretly records keystrokes.

DOWN

[1] Password credentials that are shared over an unsecured Wi-Fi network are vulnerable to ____ attacks.

[2] Sending a fake message that tricks users into revealing their account credentials is called ____.

[3] Calling an IT help desk and pretending to be a legitimate account holder who needs a password reset is an example of a ____ engineering attack.

[4] This type of attack uses a precomputed table that maps hashes to passwords in order to quickly reverse a stolen hash.

[5] This type of attack involves trying every possible combination of characters.

[7] Trying a single, common password against multiple user accounts is called password ____.

BONUS CLUE

Adding random characters to a password before it is hashed is known as **SALTING**.

Activity to accompany slide: *Password Cracking*

Create a Passphrase

The goal of this activity is to create a long passphrase and a corresponding image that can help you remember it.

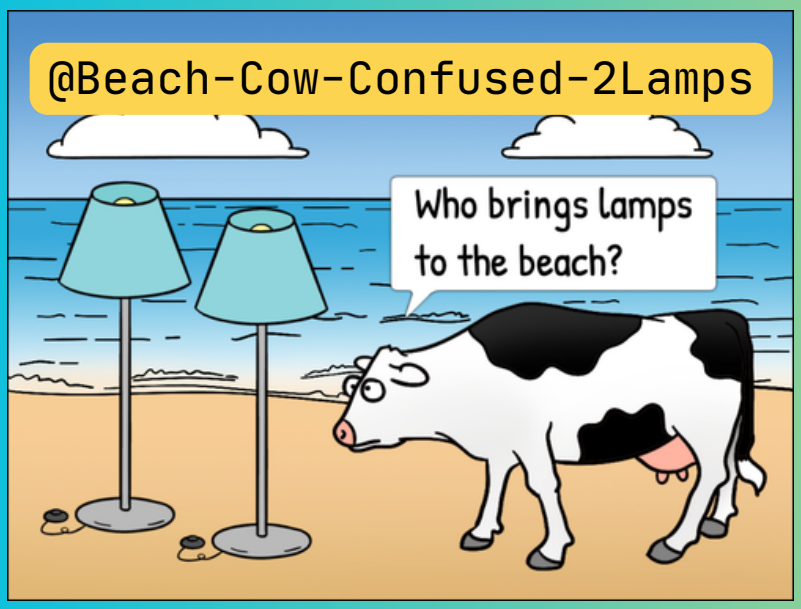


Image created using ToonyTool

Passphrase Creation Ideas:

- Look around your space and pull words from your environment
- Roll some dice and select words from a word list
- Randomly pick words out of a dictionary or other book
- Use an online generator