PRIVACYSAFE™ FOUNDATION

FLASH CARDS

Passwords and passphrases

Terminology and quiz cards for the Take Back Your Bytes lesson on strong passwords and passphrases.

What is in this set

40 cards: **24 term cards** (term on the front, definition on the back) and **16 quiz cards** (question on the front, answer on the back). Bracketed numbers on the backs, like [1], match the reference list on the last page and in the instructor guide.

How to print

1. Print double-sided on US Letter at 100% scale (no "fit to page").
2. Choose **flip on the long edge**. The backs are arranged so each answer lands behind its card.
3. Cut along the dashed lines. Each card is 3.75 by 2.5 inches.

How to use them

- **Self-test:** read the front, answer aloud, flip to check.
- **Pairs:** one reads the front, the other answers. Swap every five cards.
- **Boxes:** keep a "missed" pile and a "got it" pile. Re-test the missed pile after a break, then again the next day.
- **Warm-up:** deal a few quiz cards at the start of the next session.

Facts checked October 27, 2026. Tools and models change quickly, so confirm details against the current documentation. These materials are dedicated to the public domain under CC0 1.0 and shared for the public good. The PrivacySafe and PrivacySafe Foundation names and logos are trademarks and are not included in that dedication.

TERM

1 / 40

Password

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

2 / 40

Passphrase

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

3 / 40

Bit

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

4 / 40

Entropy

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

5 / 40

Pool (keyspace)

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

6 / 40

Random

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

7 / 40

Wordlist

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

8 / 40

Delimiter

Say it in your own words, then flip.

Passwords and passphrases

PrivacySafe Foundation | CC0 1.0

TERM

2 / 40

A secret made of several random words. Easier to remember and type than random characters.

[2]

PrivacySafe Foundation | CC0 1.0

TERM

1 / 40

A secret string of characters used to prove who you are to a service.

[1]

PrivacySafe Foundation | CC0 1.0

TERM

4 / 40

A measure, in bits, of how unpredictable a secret is. It assumes the secret was chosen at random.

[3]

PrivacySafe Foundation | CC0 1.0

TERM

3 / 40

A unit for counting possibilities. One more bit doubles the number of guesses needed.

[3]

PrivacySafe Foundation | CC0 1.0

TERM

6 / 40

Chosen by chance with no pattern. Strength numbers only hold for random choices.

[2] [3]

PrivacySafe Foundation | CC0 1.0

TERM

5 / 40

The set of choices for each position, such as 26 lowercase letters or a list of 7,776 words.

[3]

PrivacySafe Foundation | CC0 1.0

TERM

8 / 40

The character or space that joins the words in a passphrase.

General

PrivacySafe Foundation | CC0 1.0

TERM

7 / 40

A list of words a passphrase generator picks from. The EFF long list has 7,776 words.

[2]

PrivacySafe Foundation | CC0 1.0

TERM

9 / 40

Brute force

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

10 / 40

Dictionary attack

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

11 / 40

Credential stuffing

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

12 / 40

Phishing

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

13 / 40

Data breach

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

14 / 40

Hash

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

15 / 40

Offline guessing

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

16 / 40

Password manager

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

10 / 40

Trying common passwords and words from lists first.

[5]

PrivacySafe Foundation | CC0 1.0

TERM

9 / 40

Trying many possible secrets until one works.

[3]

PrivacySafe Foundation | CC0 1.0

TERM

12 / 40

Tricking you into typing a secret into a fake page. Strength does not stop it.

General

PrivacySafe Foundation | CC0 1.0

TERM

11 / 40

Trying passwords leaked from one site on many other sites.

[7]

PrivacySafe Foundation | CC0 1.0

TERM

14 / 40

A one-way scrambled form of a password that a service stores instead of the password.

[6]

PrivacySafe Foundation | CC0 1.0

TERM

13 / 40

When an attacker steals data from a service, such as its password hashes.

[6]

PrivacySafe Foundation | CC0 1.0

TERM

16 / 40

An app that stores and fills long random passwords so you remember only one.

[4] [8]

PrivacySafe Foundation | CC0 1.0

TERM

15 / 40

Guessing stolen hashes on the attacker's own machines, with no login limits.

[6]

PrivacySafe Foundation | CC0 1.0

TERM

17 / 40

Master password

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

18 / 40

Multi-factor authentication

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

19 / 40

Passkey

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

20 / 40

Composition rules

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

21 / 40

Blocklist check

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

22 / 40

CSPRNG

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

23 / 40

Client-side

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

24 / 40

Have I Been Pwned

Say it in your own words, then flip.

PrivacySafe Foundation | CC0 1.0

TERM

18 / 40

Signing in with something more than a password, such as a code or a security key.

[9]

PrivacySafe Foundation | CC0 1.0

TERM

17 / 40

The one secret that unlocks a password manager. A random passphrase suits it.

[2]

PrivacySafe Foundation | CC0 1.0

TERM

20 / 40

Rules that force symbols, digits or capitals. Current guidance discourages them.

[1]

PrivacySafe Foundation | CC0 1.0

TERM

19 / 40

A phishing-resistant sign-in method that replaces the password with a cryptographic key.

[10]

PrivacySafe Foundation | CC0 1.0

TERM

22 / 40

A cryptographically secure random number generator, the kind needed to make secrets.

[11]

PrivacySafe Foundation | CC0 1.0

TERM

21 / 40

Rejecting passwords that are common or known to be breached.

[1] [5]

PrivacySafe Foundation | CC0 1.0

TERM

24 / 40

A service for checking whether a password or email appears in known breaches.

[5]

PrivacySafe Foundation | CC0 1.0

TERM

23 / 40

Running on your own device, in your browser, instead of on a server.

[11] [12]

PrivacySafe Foundation | CC0 1.0

QUIZ

25 / 40

Name four ways passwords are attacked.

PrivacySafe Foundation | CC0 1.0

QUIZ

26 / 40

How do you estimate bits for a random password?

PrivacySafe Foundation | CC0 1.0

QUIZ

27 / 40

What does one extra bit do?

PrivacySafe Foundation | CC0 1.0

QUIZ

28 / 40

About how many bits does each random word add?

PrivacySafe Foundation | CC0 1.0

QUIZ

29 / 40

How many random words match 16 random lowercase letters?

PrivacySafe Foundation | CC0 1.0

QUIZ

30 / 40

About how many bits are 8 random lowercase letters?

PrivacySafe Foundation | CC0 1.0

QUIZ

31 / 40

Why is a famous quote a poor passphrase?

PrivacySafe Foundation | CC0 1.0

QUIZ

32 / 40

Does a strong password stop phishing?

PrivacySafe Foundation | CC0 1.0

QUIZ

26 / 40

Length times log2 of the pool size.

[3]

PrivacySafe Foundation | CC0 1.0

QUIZ

25 / 40

Common passwords, reuse across sites, offline guessing after a breach, and phishing.

[6] [7]

PrivacySafe Foundation | CC0 1.0

QUIZ

28 / 40

About 12.9, from a 7,776-word list.

[2] [3]

PrivacySafe Foundation | CC0 1.0

QUIZ

27 / 40

It doubles the number of guesses an attacker needs.

[3]

PrivacySafe Foundation | CC0 1.0

QUIZ

30 / 40

About 38 bits, since 8 x 4.70 is about 37.6.

[3]

PrivacySafe Foundation | CC0 1.0

QUIZ

29 / 40

About 6 words, roughly 78 bits, versus about 75 bits.

[2] [3]

PrivacySafe Foundation | CC0 1.0

QUIZ

32 / 40

No. A fake page can capture any password. Use a second factor or a passkey.

[9] [10]

PrivacySafe Foundation | CC0 1.0

QUIZ

31 / 40

It is a known pattern, not a random choice, so it can be guessed.

General

PrivacySafe Foundation | CC0 1.0

QUIZ

33 / 40

Why is password reuse dangerous?

PrivacySafe Foundation | CC0 1.0

QUIZ

34 / 40

What does a password manager do?

PrivacySafe Foundation | CC0 1.0

QUIZ

35 / 40

What do current NIST guidelines favor?

PrivacySafe Foundation | CC0 1.0

QUIZ

36 / 40

When should you change a password?

PrivacySafe Foundation | CC0 1.0

QUIZ

37 / 40

Where does a good generator run, and why?

PrivacySafe Foundation | CC0 1.0

QUIZ

38 / 40

What should you not do with a secret generated on a shared screen?

PrivacySafe Foundation | CC0 1.0

QUIZ

39 / 40

Which is better for a master password: 8 random characters or 6 random words?

PrivacySafe Foundation | CC0 1.0

QUIZ

40 / 40

Name one step in the password plan.

PrivacySafe Foundation | CC0 1.0

QUIZ

34 / 40

It stores long random passwords for every account, so you remember one master passphrase.

[4] [8]

PrivacySafe Foundation | CC0 1.0

QUIZ

33 / 40

One breach lets attackers try the same password on many other sites.

[7]

PrivacySafe Foundation | CC0 1.0

QUIZ

36 / 40

After a breach or other reason to think it is exposed, not on a schedule.

[1]

PrivacySafe Foundation | CC0 1.0

QUIZ

35 / 40

Length, long passwords, no forced symbols or scheduled changes, and breach checks.

[1]

PrivacySafe Foundation | CC0 1.0

QUIZ

38 / 40

Do not use it for a real account. Others saw it.

General

PrivacySafe Foundation | CC0 1.0

QUIZ

37 / 40

On your own device, so the secret need not be sent anywhere. Check who runs it and whether its source is public.

[11] [12]

PrivacySafe Foundation | CC0 1.0

QUIZ

40 / 40

For example: use a manager, make each password unique, turn on a second factor, check for breaches.

General

PrivacySafe Foundation | CC0 1.0

QUIZ

39 / 40

6 random words: about 78 bits versus about 50 bits for 8 characters from all four sets.

[2] [3]

PrivacySafe Foundation | CC0 1.0

Reference list

Links were checked on October 27, 2026.

#	SOURCE	WHAT IT SUPPORTS
[1]	NIST, SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (2025) https://pages.nist.gov/800-63-4/sp800-63b.html	Current US guidance on memorized secrets: favor length, allow long passwords, avoid composition rules and scheduled changes, and check against known-compromised passwords.
[2]	Electronic Frontier Foundation, EFF Dice-Generated Passphrases https://www.eff.org/dice	The long wordlist of 7,776 words, the advice to use six words, and the 77-bit figure.
[3]	Electronic Frontier Foundation, Deep Dive: EFF's New Wordlists for Random Passphrases (2016) https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases	How passphrase strength is measured: about 12.9 bits per word, and each extra bit doubles the guesses.
[4]	EFF Surveillance Self-Defense, Creating Strong Passwords https://ssd.eff.org/module/creating-strong-passwords	Plain-language advice on strong passwords and password managers.
[5]	Have I Been Pwned, Pwned Passwords https://haveibeenpwned.com/Passwords	A service for checking whether a password appears in known breaches.
[6]	OWASP, Password Storage Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html	How services should store passwords as salted hashes, and why stolen hashes can be guessed offline.
[7]	OWASP, Credential Stuffing Prevention Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html	How attackers reuse leaked credentials on other sites, and defenses including multi-factor authentication.
[8]	CISA, Secure Our World: Use Strong Passwords https://www.cisa.gov/secure-our-world/use-strong-passwords	Consumer advice on long, random, unique passwords and password managers.
[9]	CISA, Secure Our World: Turn on MFA https://www.cisa.gov/secure-our-world/turn-mfa	Consumer advice on multi-factor authentication.
[10]	FIDO Alliance, Passkeys https://fidoalliance.org/passkeys/	An overview of passkeys, a phishing-resistant way to sign in.
[11]	MDN Web Docs, Crypto.getRandomValues() https://developer.mozilla.org/en-US/docs/Web/API/Crypto/getRandomValues	The browser's cryptographically secure random number source.
[12]	PrivacySafe Bot https://privacysafe.bot	The password and passphrase generator shown in the video. Its own pages describe how it runs and what it estimates.
[13]	Music credit in the video's caption file video/privacysafe-bot-demo_en.vtt	The background music, "Mall" by Komiku, is dedicated to the public domain under CC0 1.0.
[14]	PrivacySafe Foundation https://privacysafe.foundation/	The Take Back Your Bytes education campaign and the Foundation's other work.
[15]	Creative Commons, CC0 1.0 Universal https://creativecommons.org/publicdomain/zero/1.0/	The public-domain dedication that covers these lesson materials.