

ANSWER KEY

Answer Key

Every page for this day is keyed. Nothing is left as "answers will vary."

Bell Ringer — Which One Takes Longer to Guess?

Look for

- Picks Password B.
- Says no, because length does more work than symbols, or because A follows a common pattern.

Model response

Password B would take far longer to guess, because it's much longer and made of random words. Password A is short and follows a pattern guessing lists already try: a word with a capital, a symbol and a number.

Also accept: Any answer that picks B and mentions length, randomness or the pattern in A.

Do not accept: An answer that picks A because it has more kinds of characters.

Guided Notes

Blanks are shown filled in, in order.

How do attackers break a password?

Trying every possible combination until one works is a **brute-force attack**.

Trying the most likely passwords first, from lists of real leaked ones, is a **dictionary attack**.

A cap on how many wrong guesses anyone can make at the sign-in page is **rate limiting**.

What does a careful site actually store?

A one-way scramble of a password that can't be turned back into it is a **hash**.

A random value added to each password before it's hashed is a **salt**, so two people with the same password get different hashes.

Guessing against a stolen file of hashes, with no limit on tries, is **offline cracking**.

That's still guessing, so a long, uncommon password is very hard to crack.

What do the current rules say?

Forced mixes, like a capital, a number and a symbol, are **composition rules**, and the current rules say sites shouldn't require them.

A list of passwords a site refuses because they're common or already leaked is a **blocklist**. The current rules also drop security questions, because the answers are easy to find or guess.

When a password is the only thing protecting an account, the rules say it should be at least 15 characters.

The rules also say sites shouldn't make you change a password on a schedule, only when there's a sign it leaked, so change it when a site tells you it was breached.

A site should let you use a password of 64 characters or more, so long passphrases fit.

What makes a password hard to crack?

A password made of several random words is a **passphrase**.

An app that creates, stores and fills in a different strong password for every account is a **password manager**.

Reusing a password means one leak can open every account that shares it.

Exit Ticket

1. Correct: (A) Sites shouldn't require it, because people meet it in predictable ways.

The current rules say sites shouldn't force composition rules. People meet them the same predictable ways, like a capital first and an exclamation point at the end.

2. Correct: (B) Guess it, by hashing guesses until one matches her hash.

A hash can't be turned back into the password. The attacker has to guess, which is why a long, uncommon password is so hard to crack.

Item 3 — written response

Look for

- Says Monica's password is more likely to be cracked.
- Says cracking a hash is still guessing, or that a long, uncommon password takes far more guesses than a common pattern.

Model response

The attacker is more likely to crack Monica's password. Cracking a hash is still guessing, and hers is a word, a year and a symbol, a pattern guessing lists try early, while Rhett's six random words take far more guesses.

Also accept: Any answer that picks Monica's password and says cracking is guessing or that hers follows a common pattern.

Do not accept: An answer saying a stolen file makes both passwords useless, or that passphrases can never be cracked.

Points: give 1 point for each line under Look for, 2 in all.