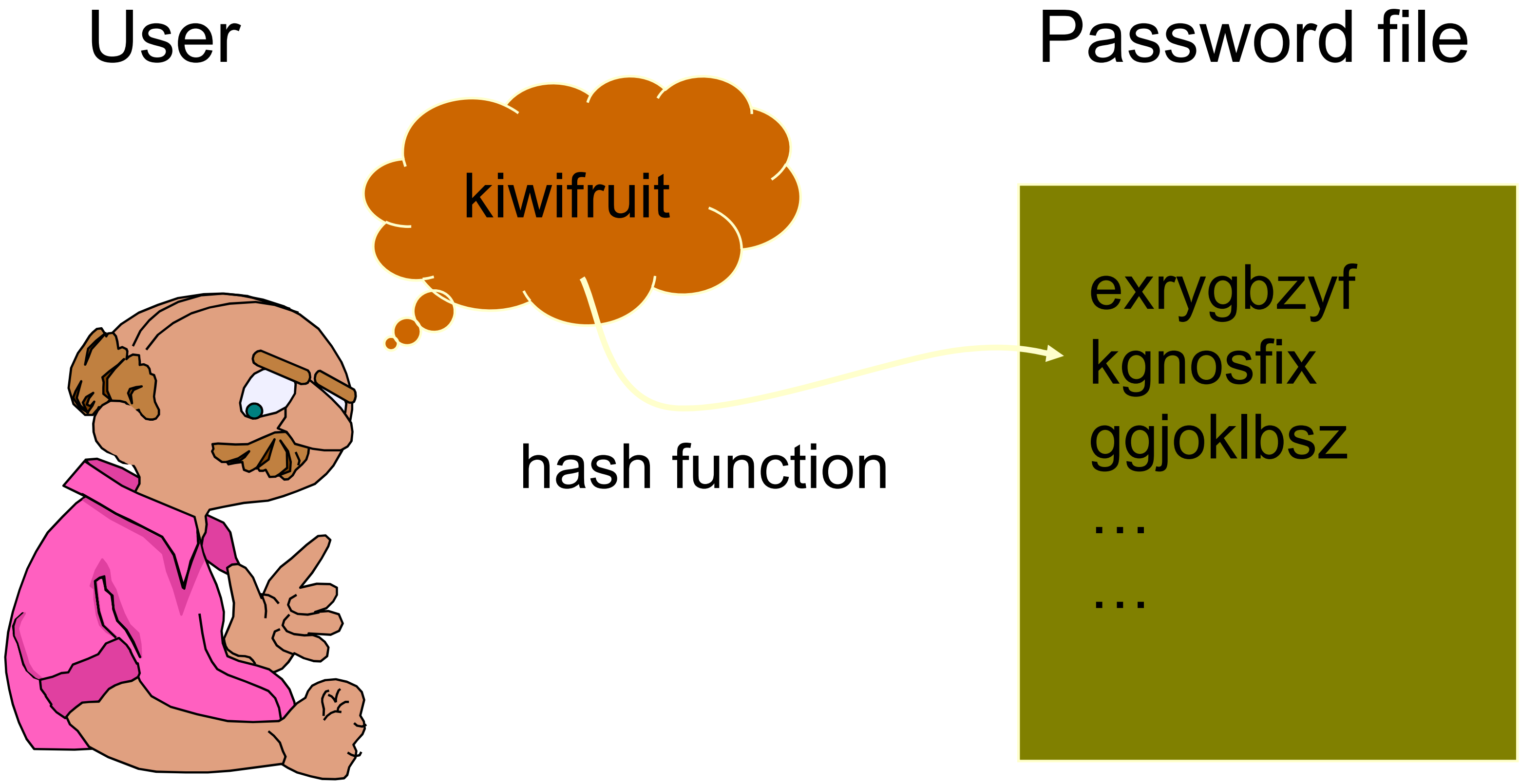
Password Management

Passwords We Use Today

- PINs, smartphone unlock codes, computer accounts, websites
- Passwords are used to protect against unauthorized access and privilege escalation (ex. Super user privilege on UNIX)

Basic Password Scheme



User

Password file

kiwifruit

hash function

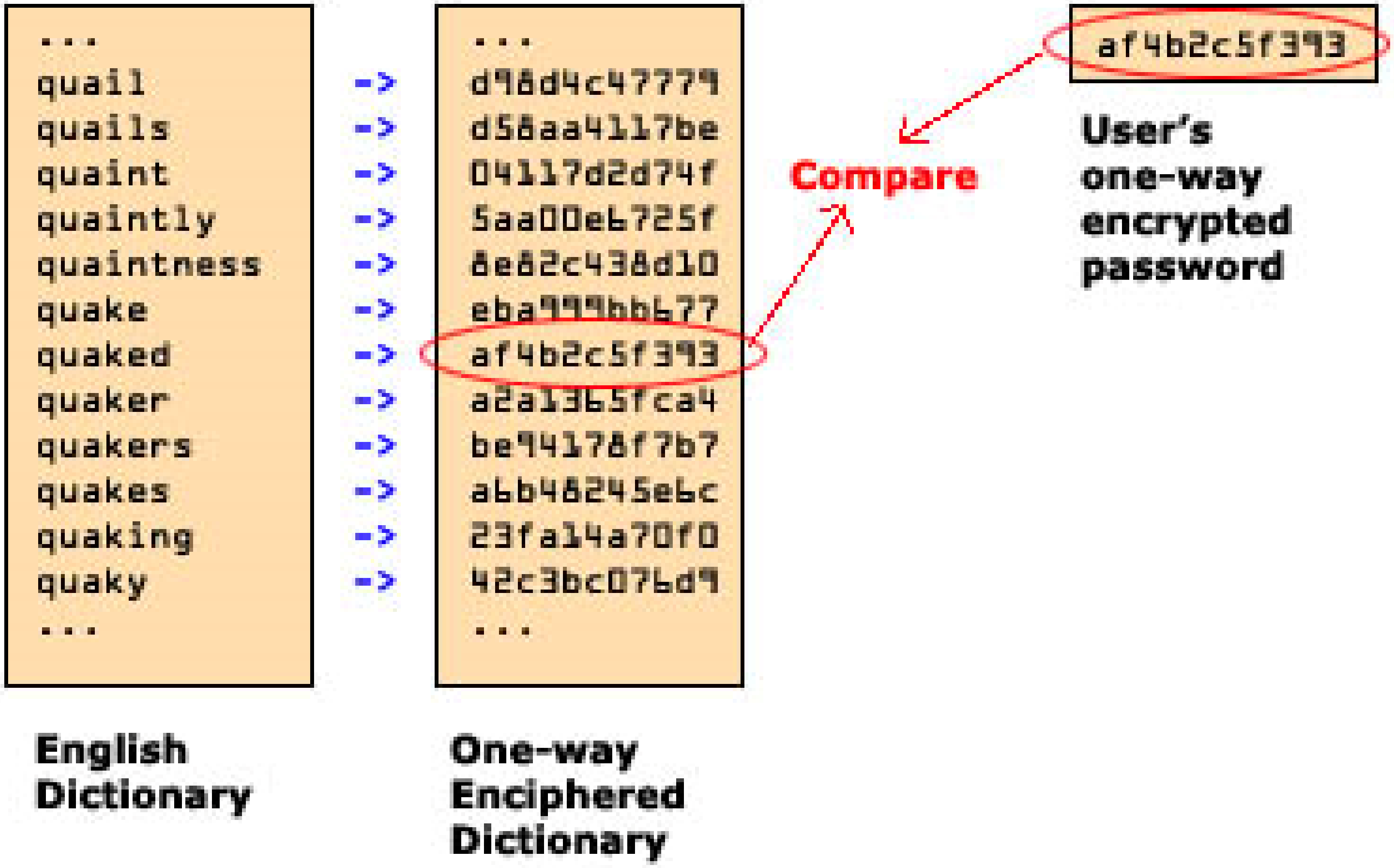
exrygbzyf
kgnosfix
ggjoklbsz
…
…

Password based attacks

- Dictionary attacks – uses a dictionary of words to guess
- Brute forcing – guessing large numbers of password combinations, very slow

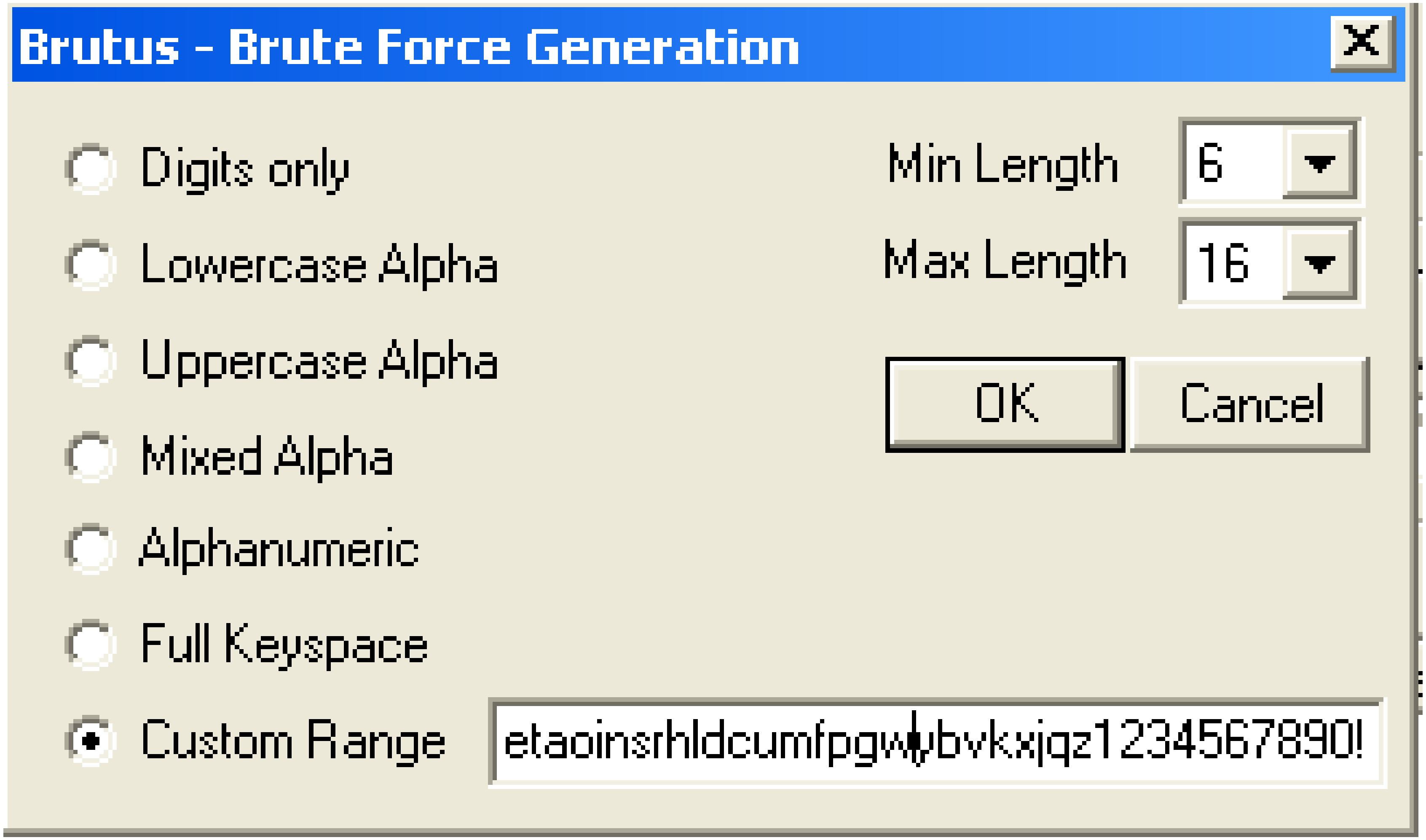
Dictionary Attack

- Typical password dictionary
  - 1,000,000 entries of common passwords
    - people's names, common pet names, and ordinary words.
  - Suppose you generate and analyze 10 guesses per second
    - This may be reasonable for a web site; offline is *much* faster
  - Dictionary attack in at most 100,000 seconds = 28 hours, or 14 hours on average
- If passwords were random
  - Assume six-character password
    - Upper- and lowercase letters, digits, 32 punctuation characters
    - 689,869,781,056 password combinations.
    - Exhaustive search requires 1,093 years on average



Brute Force Attack

- Brute Force Searches:
  - Simply try every possible key
  - Effort required is proportionate to the key size
  - You must recognize the plaintext once you see it!
  - Typically uses no knowledge about the cipher, the cipher text, or the plaintext, so it is very easy to do.



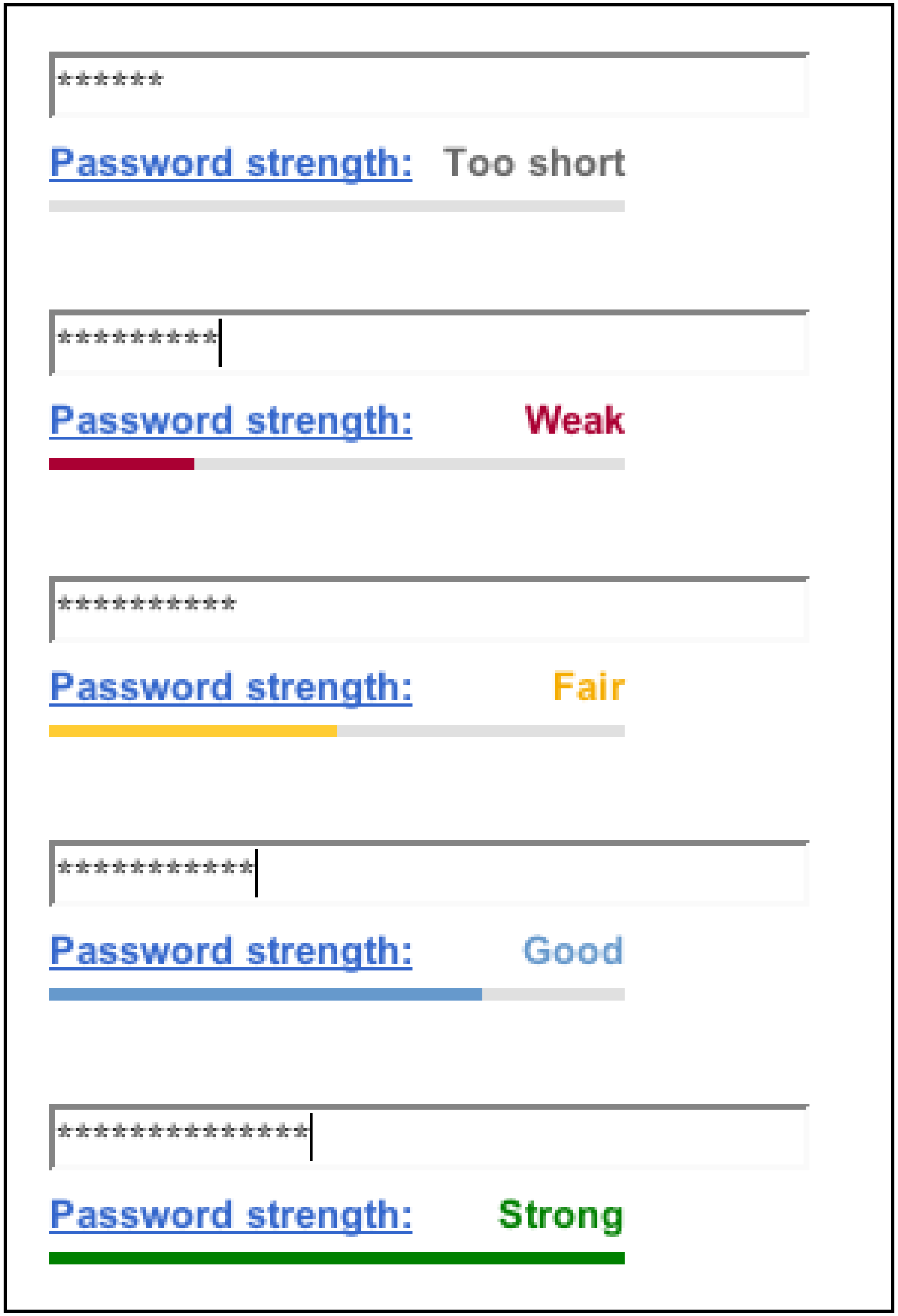
○ Digits only
○ Lowercase Alpha
○ Uppercase Alpha
○ Mixed Alpha
○ Alphanumeric
○ Full Keyspace
● Custom Range etaoinsrhldcumfpgwybvkxjqz1234567890!

Min Length 6

Max Length 16

Strong vs. Weak Passwords

- Long, randomly generated passwords containing varying capitalization, numbers, and symbols if permitted
- Should be changed frequently
- Technique involves making a “pass-phrase”



******

Password strength: Too short

****

Password strength: Weak

****

Password strength: Fair

****

Password strength: Good

****

Password strength: Strong

Remembering Passwords

- Human brain is conditioned to work well with repetitive “chunks” – random sequences are difficult to remember
- 2000 study: most users with a randomly generated password kept it written down

Keeping Track of Passwords

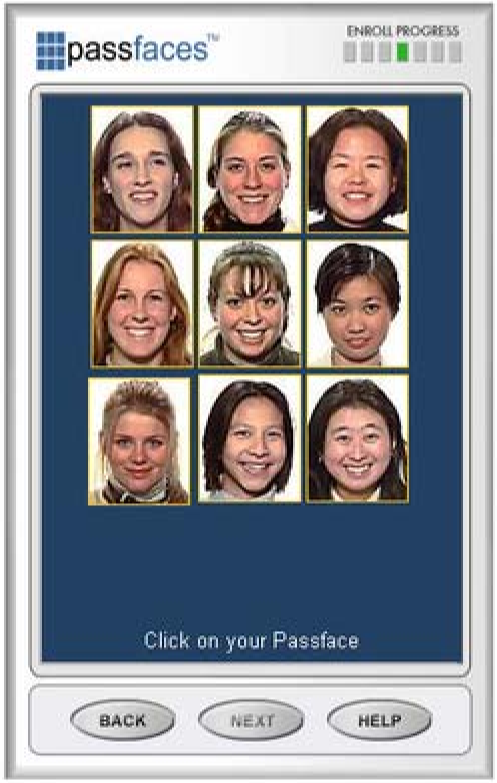
- “Remember password” function on browsers is dangerous
- Keeping written records is also unsecure

Keeping Track of Passwords

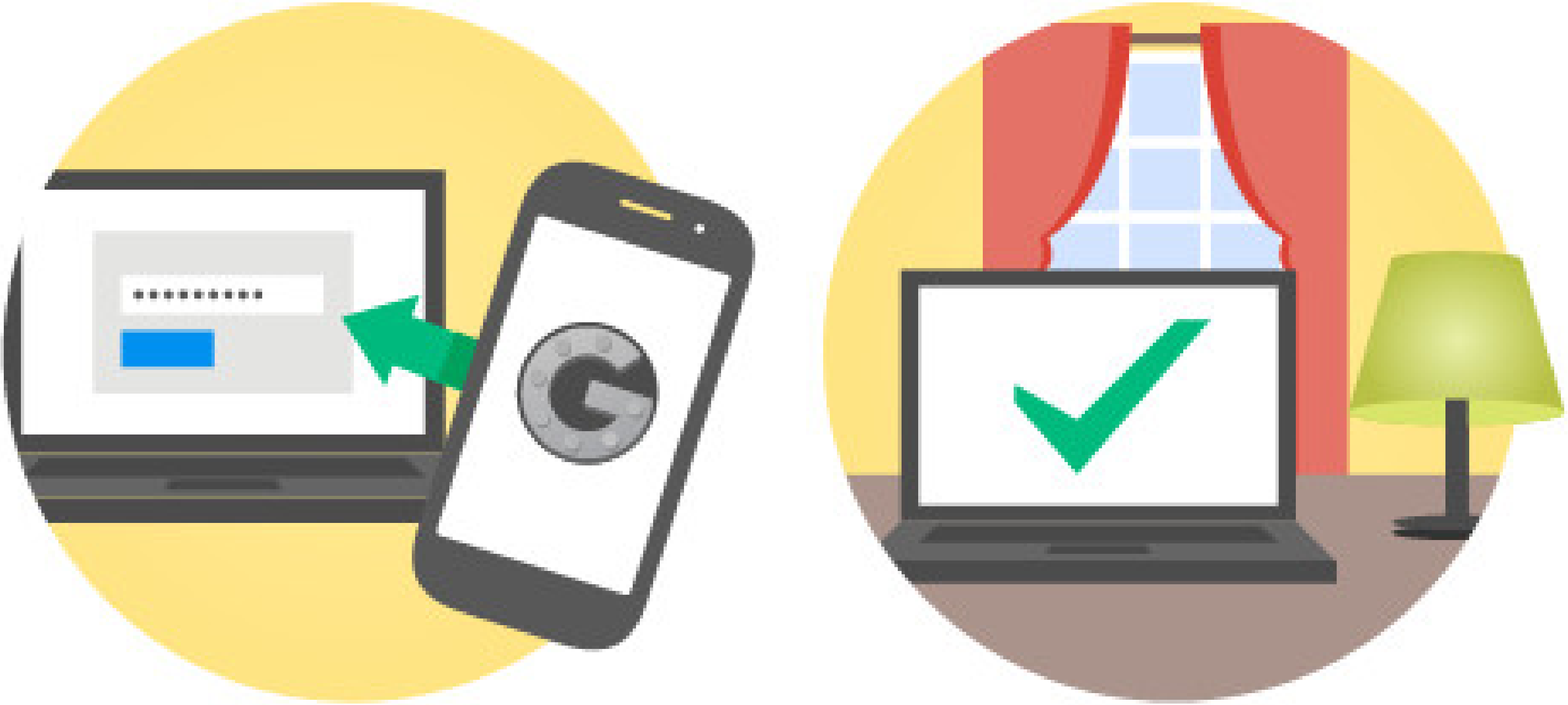
- KeePass: free, open source, stores passwords in a database locked with a master key. Encrypted (AES).
- Robopass
- Lastpass
- SplashID
- 1Password

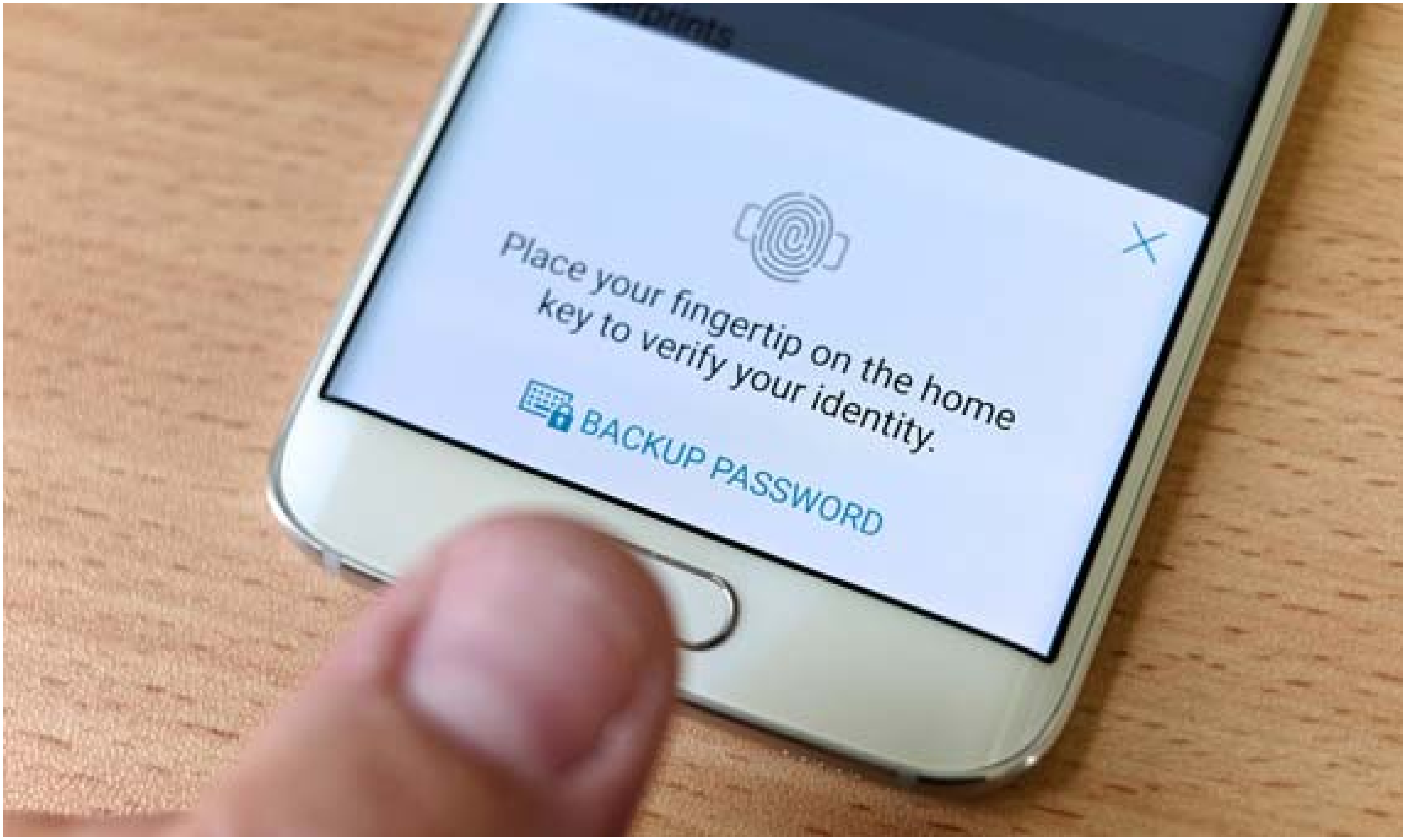
Alternatives to the current system

- PassFaces



Signing in with 2-step verification





Place your fingertip on the home key to verify your identity.

eToken™
PRO Anywhere

Alternatives to the current system

- These alternatives render dictionary attacks and brute force attacks useless

The End