

CS50 for MBAs

Privacy, Security

secure



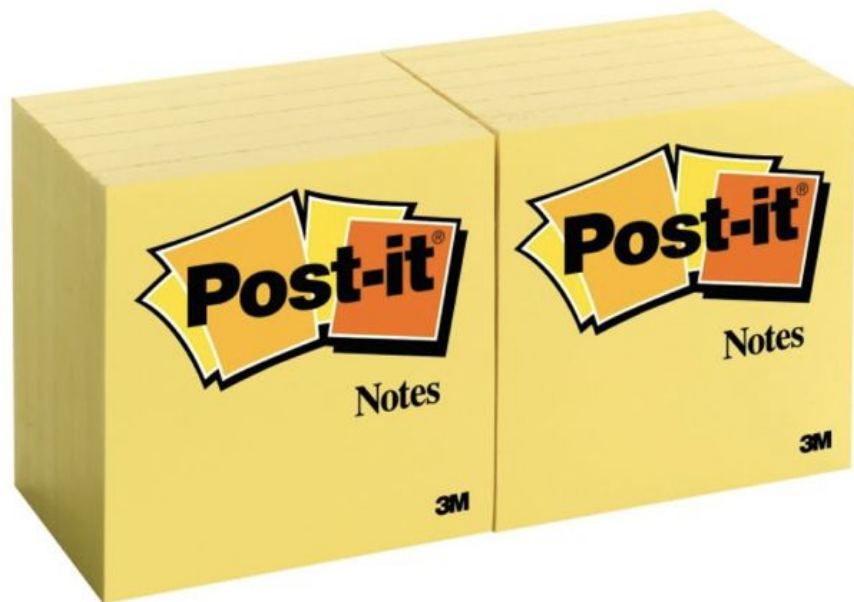
Meeting ID: 918 7212 9083

Meeting ID: 918 7212 9083

Passcode: 022056

<https://cs50.zoom.us/j/91872129083?pwd=MHhIRm1PMGwyeUxYSFIBOHpqRVFzZz09>

passwords



1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567

brute-force attacks



4-digit passcode

$$10 \times 10 \times 10 \times 10$$

10,000

4-letter passcode

$$52 \times 52 \times 52 \times 52$$

7,311,616

4-character passcode

94 × 94 × 94 × 94

78,074,896

8-character passcode

94 × 94 × 94 × 94 ×
94 × 94 × 94 × 94

6,095,689,385,410,816



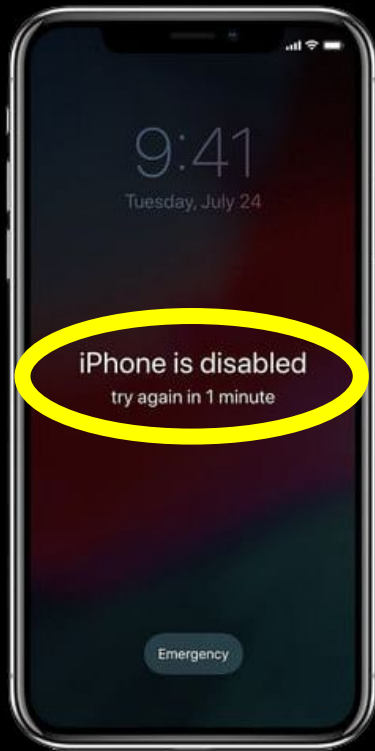
9:41

Tuesday, July 24

iPhone is disabled

try again in 1 minute

Emergency



9:41
Tuesday, July 24

iPhone is disabled
try again in 1 minute

Emergency

9:41

Tuesday, July 24

iPhone is disabled

try again in 1 minute

Emergency

Google Fi

📶 🔒 📶 🔒 60%



11:27

Thu, May 28 ☁️ 24°C

Too many attempts. Try again later.

Google Fi

📶 🔒 📶 🔒 60%



11:27

Thu, May 28 ☁️ 24°C

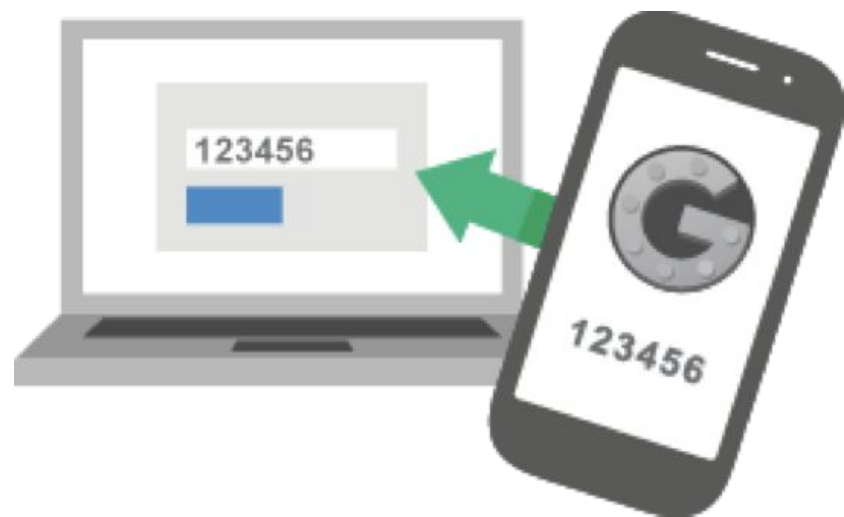
Too many attempts. Try again later.



Too many attempts. Try again later.

two-factor authentication





password managers

1password.com

lastpass.com

...

SSO

hashes

haveibeenpwned.com

encryption

secret-key encryption



Memo:
Confidential

Re:
Fiscal Review

This quarter's
earnings have
just come in
and...

plaintext



encryption

BEGIN PGP

gANQR1DBw
U+dB/b95Xx
QQzrGYXD9
VSoOTF6gk
IXTBPce8+M
mdf&UWLdDe5

END PGP

ciphertext



decryption

Memo:
Confidential

Re:
Fiscal Review

This quarter's
earnings have
just come in
and...

plaintext

Or fher gb qevax lbhe Binygvar.

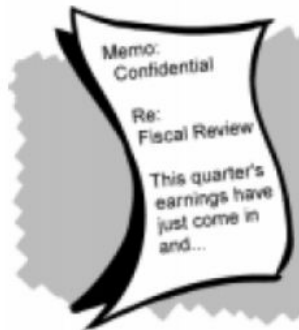
Be sure to drink your Ovaltine.

public-key encryption

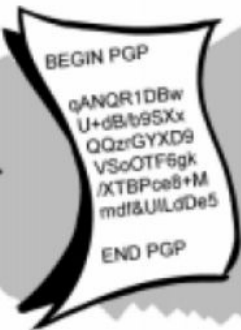
public key



private key



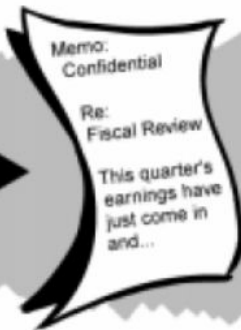
encryption



ciphertext



decryption




plaintext


HTTPS

Only authenticated users can join: Sign in to Zoom

Encrypt

Encryption key stored in the cloud.


Enhanced encryption 

End-to-end encryption 

Waiting room
Only users admitted by the host can join the meeting

Only authenticated users can join: Sign in to

Encryption

Enhanced encryption 

End-to-end encryption 

Encryption key stored on your local device. No one else can obtain your encryption key, not even Zoom.

Several features will be automatically disabled when using end-to-end encryption, including cloud recording and phone/SIP/H.323 dial-in.



[Learn more](#)

Assignment 10

Office Hours

CS50 for MBAs

Privacy, Security