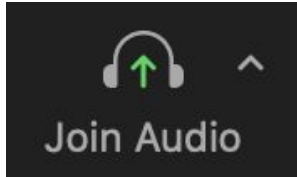




# Welcome to Tech Talks

Mobile Device Security (Apple/Android)

Join Audio / Unmute to Talk



Start Video (optional)

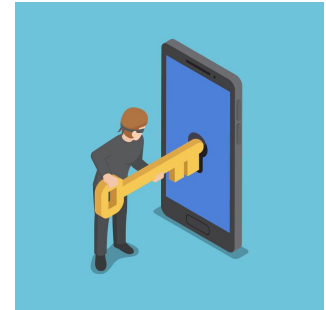
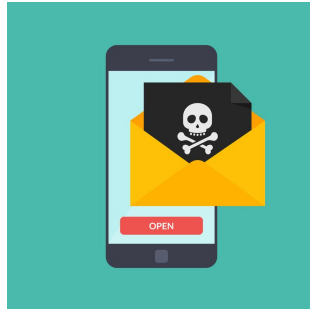
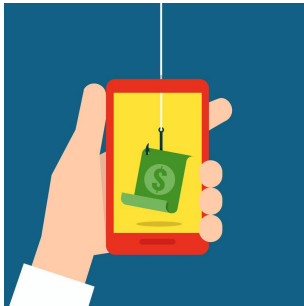


Please find these **buttons** on your Zoom control panel

# Game plan

*Keep your accounts and device secure*

1. Phishing
2. Malware
3. Passwords
4. Precautions

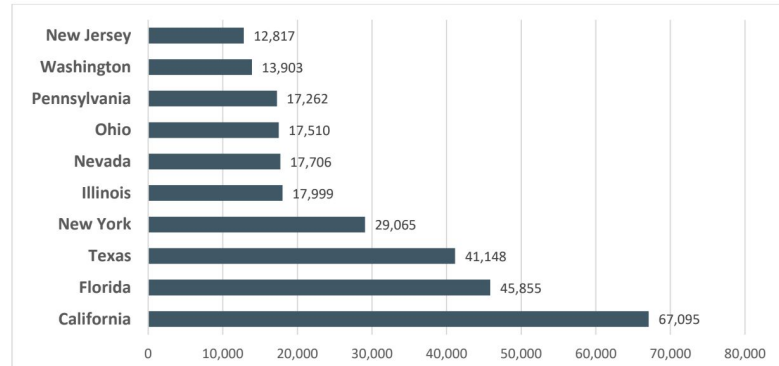


# Internet Crimes (FBI)

2021 INTERNET CRIME REPORT

21

## 2021 - Top 10 States by Number of Victims<sup>19</sup>



## 2021 CRIME TYPES

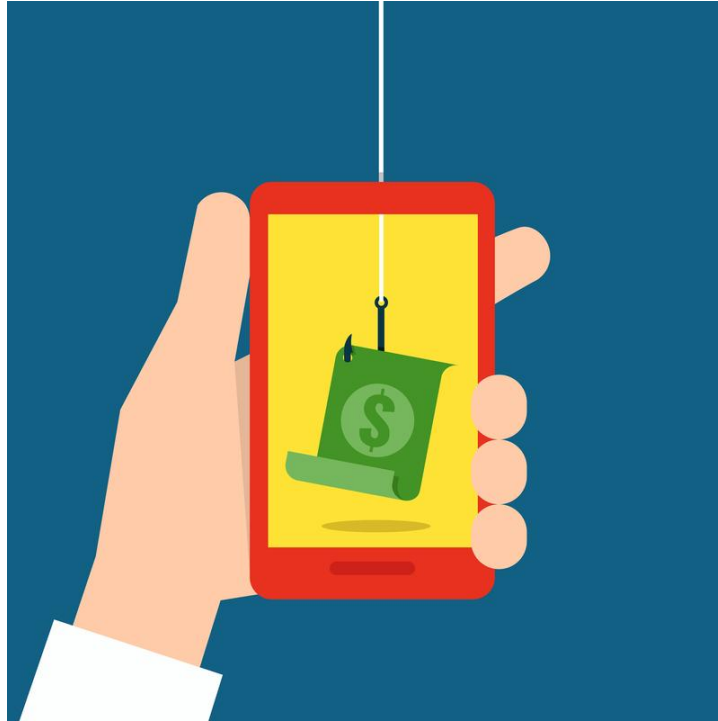
### By Victim Count

Crime Type	Victims
Phishing	323,972
Non-Payment/Non-Delivery	82,478
Personal Data Breach	51,829
Identity Theft	51,629
Extortion	39,360
Confidence Fraud/Romance	24,299
Tech Support	23,903
Investment	20,561
BEC/EAC	19,954
Spoofing	18,522
Credit Card Fraud	16,750

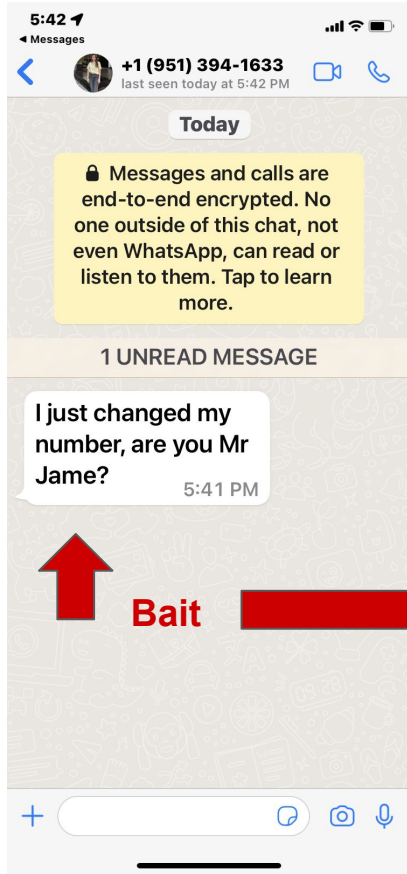
[https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)



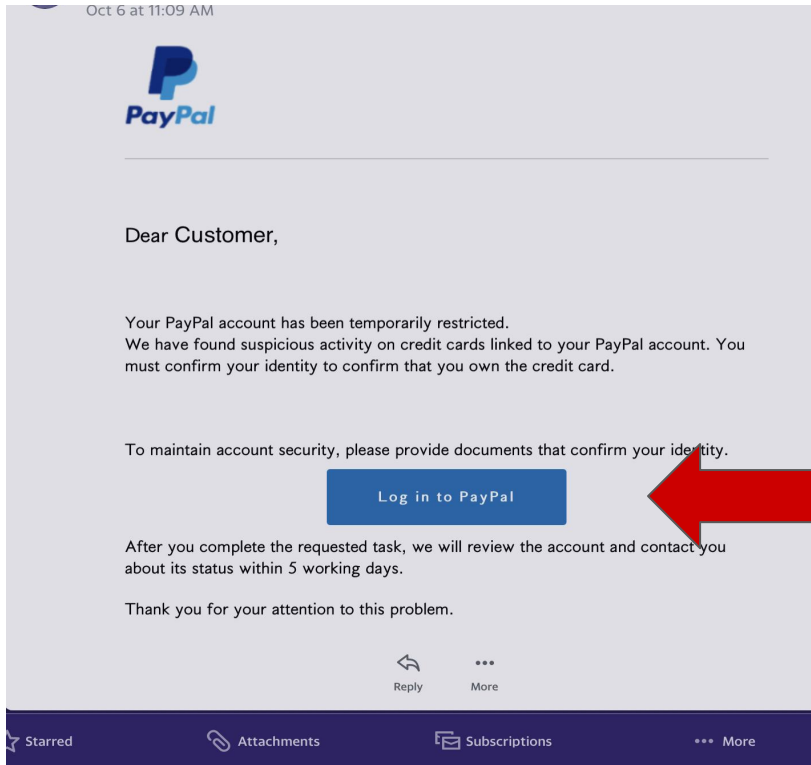
# Phishing



# Phishing: Messaging



# Phishing: Account problem

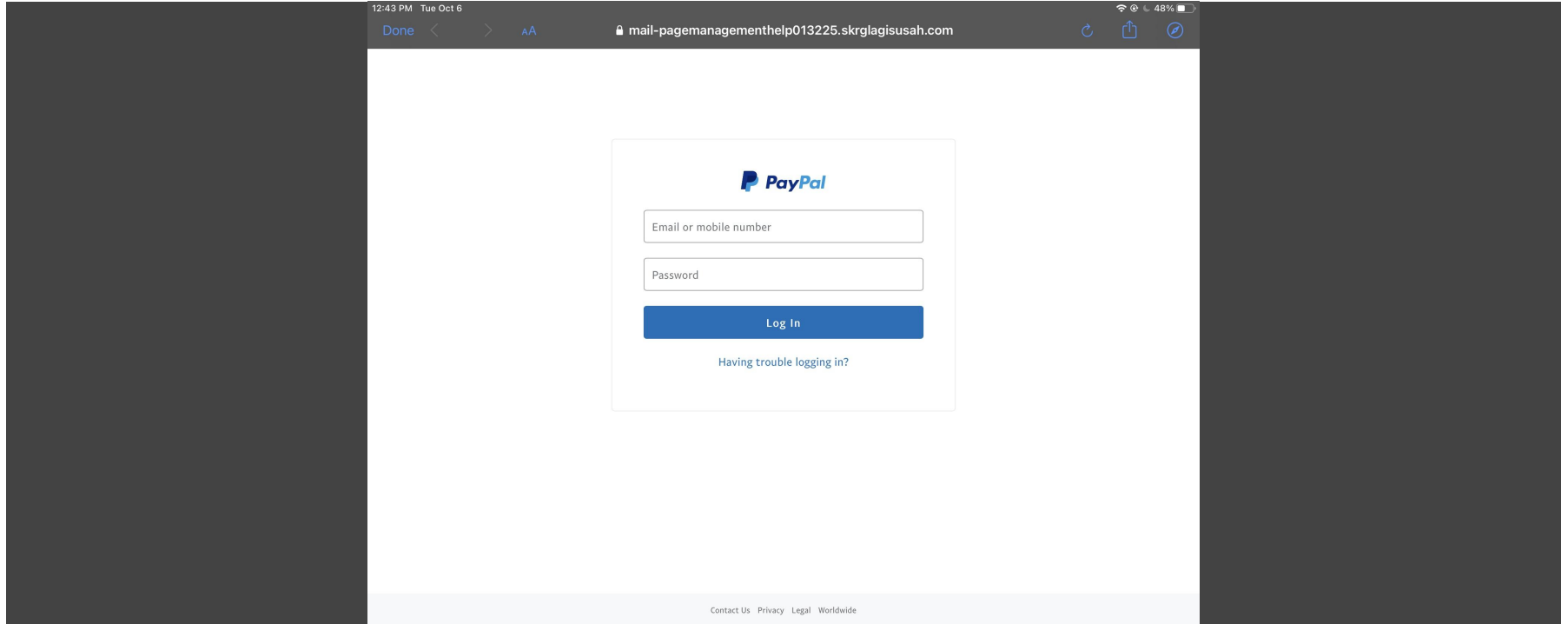


**Don't click this!**  
**go directly to PayPal.com**

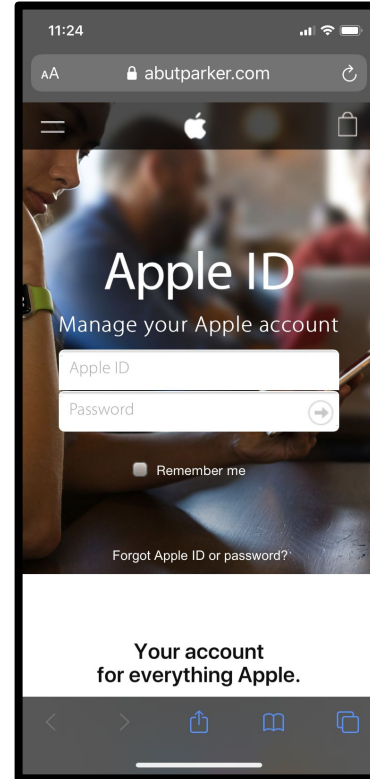
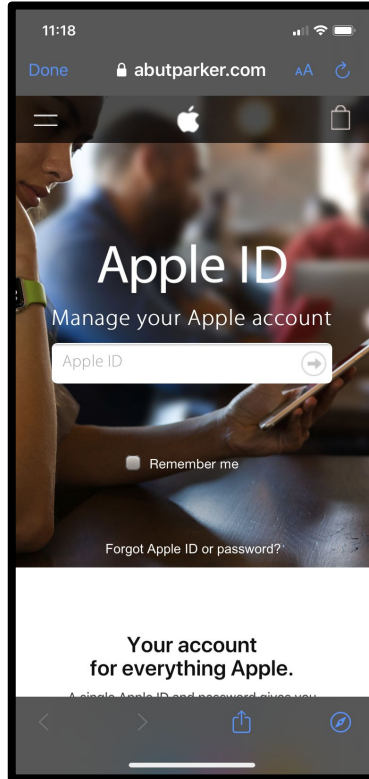
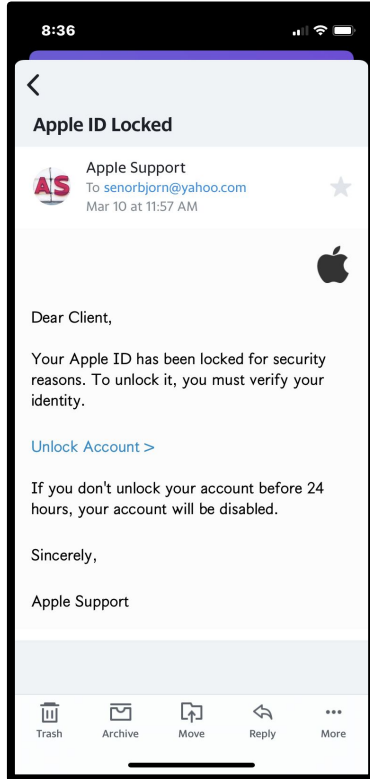


Not PayPal.com web address

Continued (if you clicked)...



# Phishing: Account problem

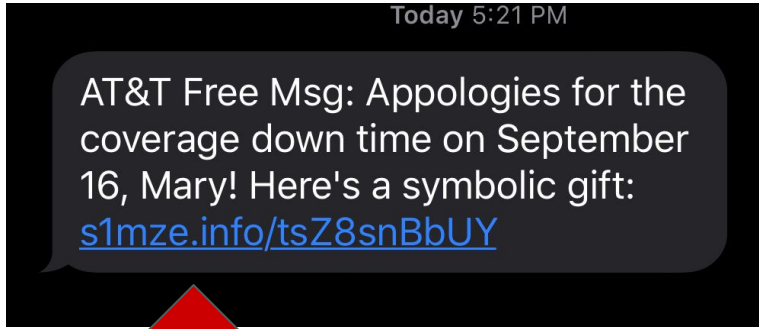


← Not Apple's Web Address

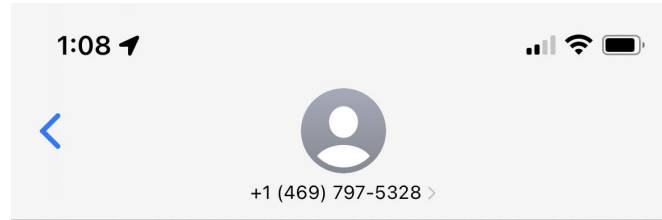




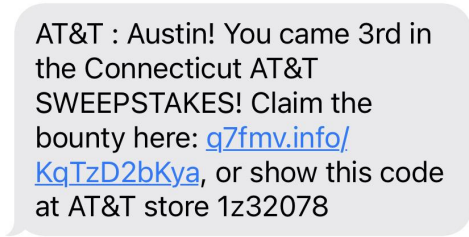
# Phishing: Suspicious links/files



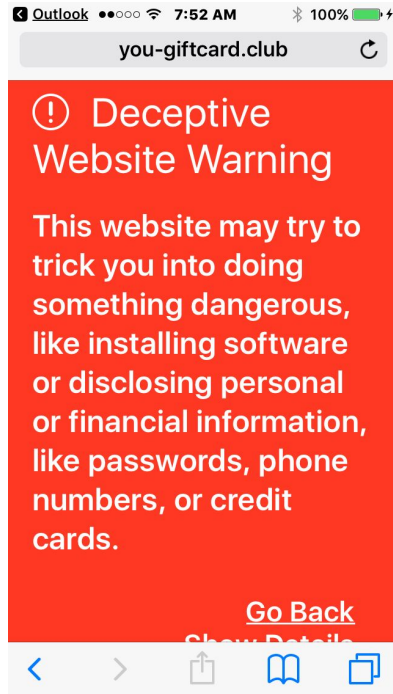
Strange Link Address



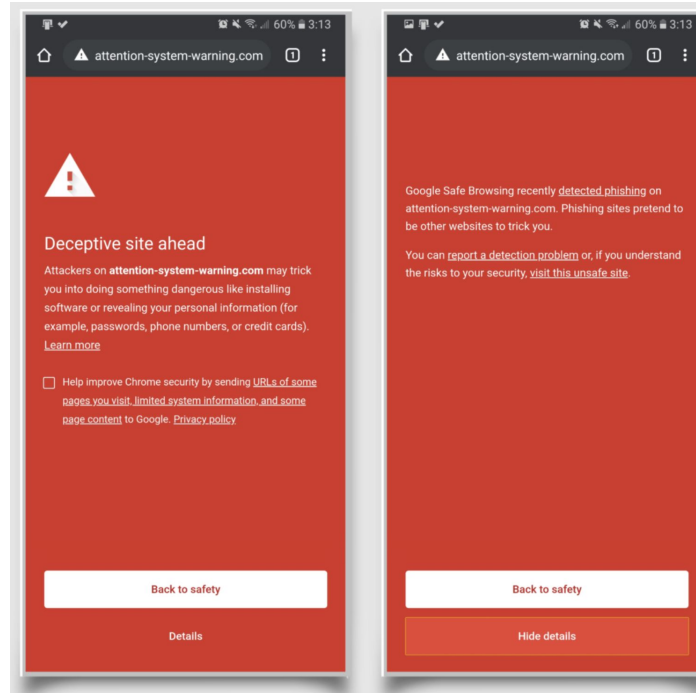
Text Message  
Thu, Feb 4, 5:21 PM



# Phishing: Watch for browser warnings



Safari example



Chrome example



# Phishing: Red Flags



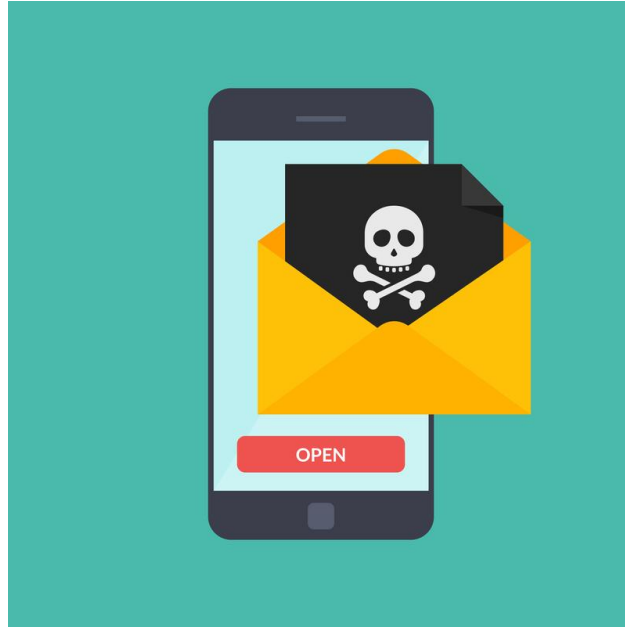
Ignore and delete if...

1. Sounds too good to be true
2. Pushy or threatening
3. Vague salutations (e.g. Hi, Dear Customer)
4. Check “From” line of sender’s email
5. Check destination website address

**Always call or visit organizations directly!**



# Malware





# Malware: Rare but possible

- Data Theft
- Ransom/Extortion
- Spying (location/camera/microphone)



# Malware: Prevention

- Avoid suspicious links/downloads
- Keep Software up-to-date
- Only download reputable apps (from app store / play store)
- Use secure connections (WiFi  and Websites  )



# Passwords



# Passwords: Strategies

- Combination of words, symbols, numbers
- Don't reuse one password for multiple accounts
- Two-factor authentication for important accounts
- Password Managers (e.g. Bitwarden)





# Passwords: Demo

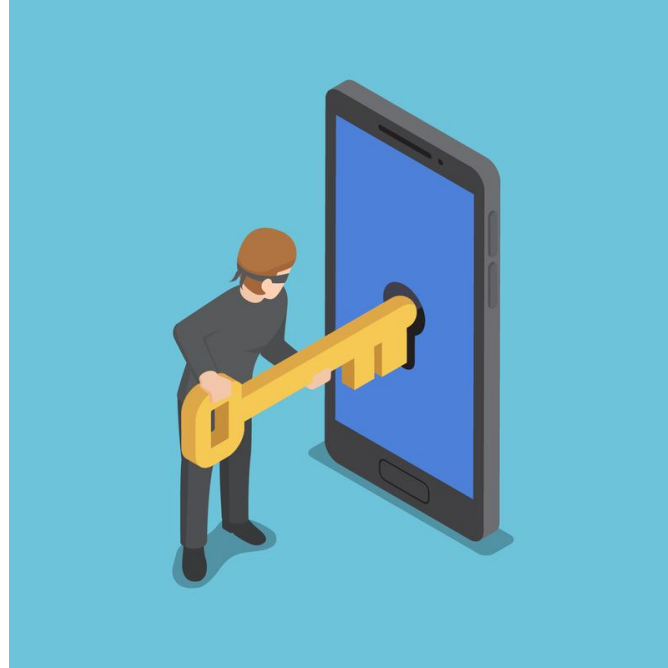
';--have i been pwned?

Check if your email or phone is in a data breach

<https://haveibeenpwned.com>



# Precautions



# Precautions: Suggestions

- Use a screen lock (4 digit passcode minimum)
- Find My (Apple <https://www.icloud.com/find>)
- Find My Device (Android <https://www.google.com/android/find>)



Apple



Android



# Precautions: Demo

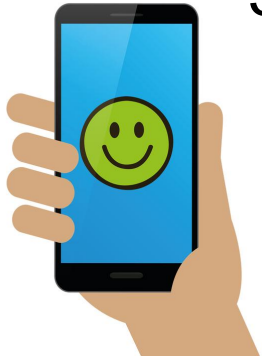


Apple's Find My App



# Summary: Best Practices

1. Be skeptical of links, texts, calls, emails
2. Keep software up-to-date
3. Strong password management
4. Use a screen lock
5. Use “Find my” / “Find my device” app



# Takeaways?

Check out [www.santacruzpl.org/digitalllearning](http://www.santacruzpl.org/digitalllearning)

How'd we do? We'll email you a survey.

