Foundation of Computer Security

DigitalOcean

@masonegger

Mason Egger
Developer Advocate

@masonegger

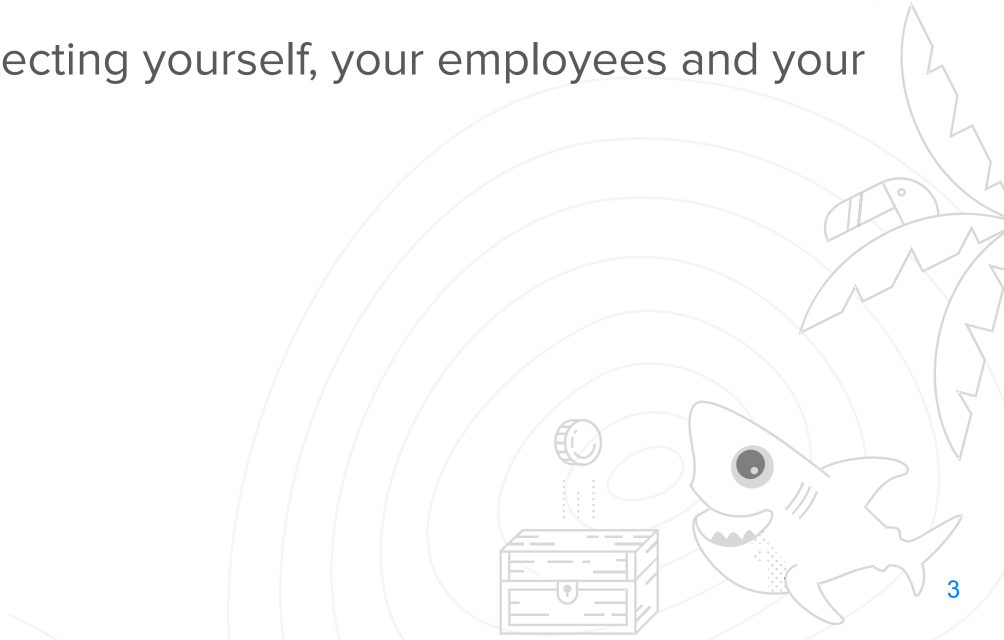
https://mason.dev

https://twitch.tv/codingwithmason

mason@do.co

Webinar Goals

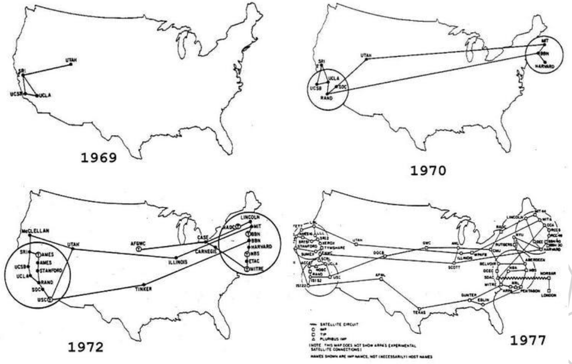
- Learn about the History of Computer Security and why it's necessary
- Discuss common threats that you may encounter
- Suggested Practices for protecting yourself, your employees and your customers



History of the Internet and Computer Security

Birth of the Internet and the Web

- ARPANET (Advance Research Projects Agency Network) - first wide-are packet-switching network with distributed control.
  - 1969 - Initial 4 computers connected
  - 1975 - Declared operational
- 1989 - World Wide Web conceptualized at CERN
- 1990 - First web page served
- 1991 - Adoption began outside of CERN
- 1993 - First web browser released in 1993
- 1996 - Web gets sophisticated. Flash expands capability, brings flaws, bugs, and vulnerabilities
- 2003 - Internet usage skyrockets. More data created in 2003 than entire human history up to that point. Begins altering commerce, business
- And it just keeps growing...



Evolution of Cyber Security

○ 1971 - Creeper Virus is created and infects mainframes.

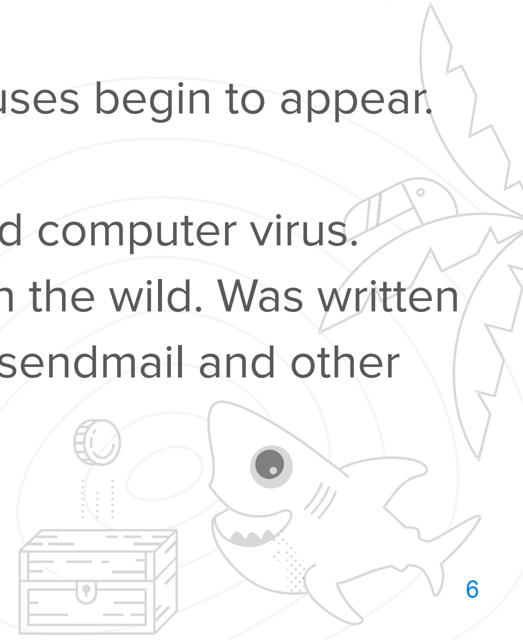
○ 1973 - Robert Metcalfe warns that the network is too easy to access from the outside.

○ 1978 - Computer Scientists attempt to incorporate encryption into TCP/IP. Face many hurdles, one of which is the National Security Agency.

○ 1981 - Elk Cloner virus appears, first since Creeper. More viruses begin to appear. Most were simple to fix, just download a patch.

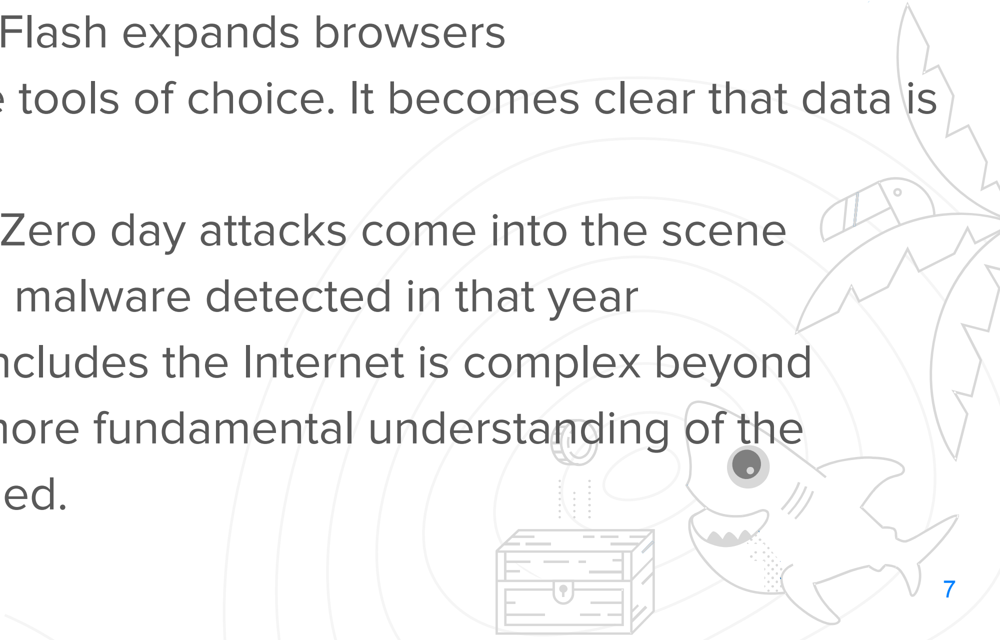
○ 1987 - First documented case of the removal of an in-the-wild computer virus.

○ 1988 - “The Morris Worm”: First virus to spread extensively in the wild. Was written to determine the size of the internet. Used security holes in sendmail and other Unix applications as well as weak passwords.



Evolution of Cyber Security cont.

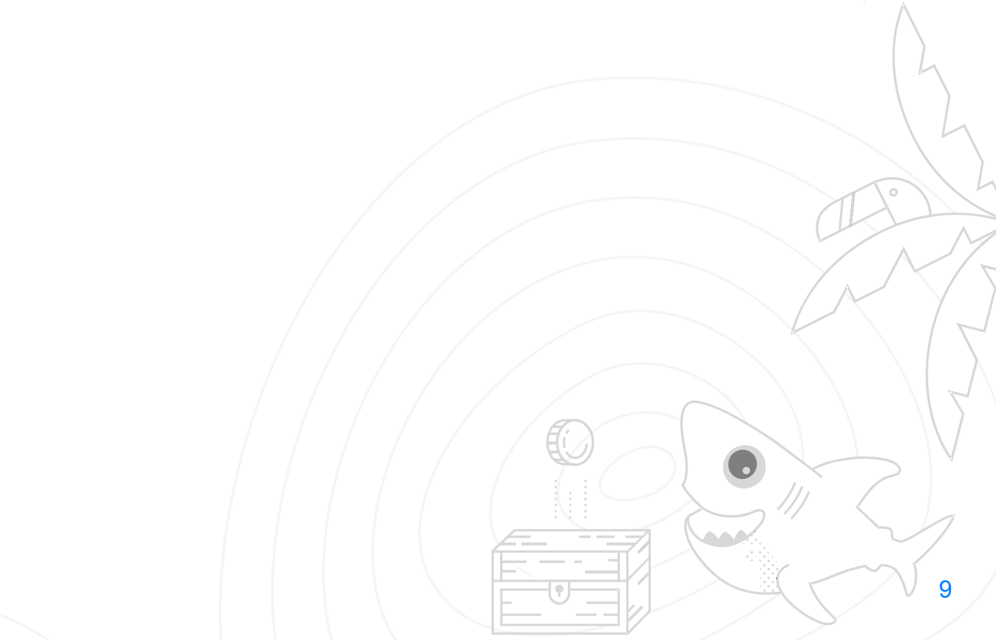
- 1987-1989 - Cyber Security companies and programs such as McAffee, Symantec, Ultimate Virus Killer start to appear
- 1993 - First web browser released. Internet sees large growtn. See the first web robots and DDoS attacks
- 1996 - Phishing becomes a problem. Flash expands browsers
- 2000 - Adware and spyware become tools of choice. It becomes clear that data is worth billions
- 2003 - Internet adoption skyrockets. Zero day attacks come into the scene
- 2007 - Reports of 5.49 million unique malware detected in that year
- 2010 - Pentagon’s JASON project concludes the Internet is complex beyond modern understanding. Suggests a more fundamental understanding of the science behind cybersecurity is needed.



Common Threats

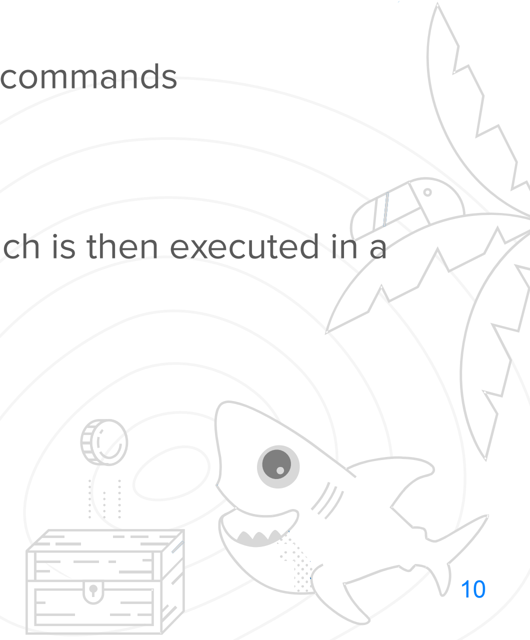
Disclaimer

- This is not a comprehensive list of attacks by any means.
- These are considered some of the more common



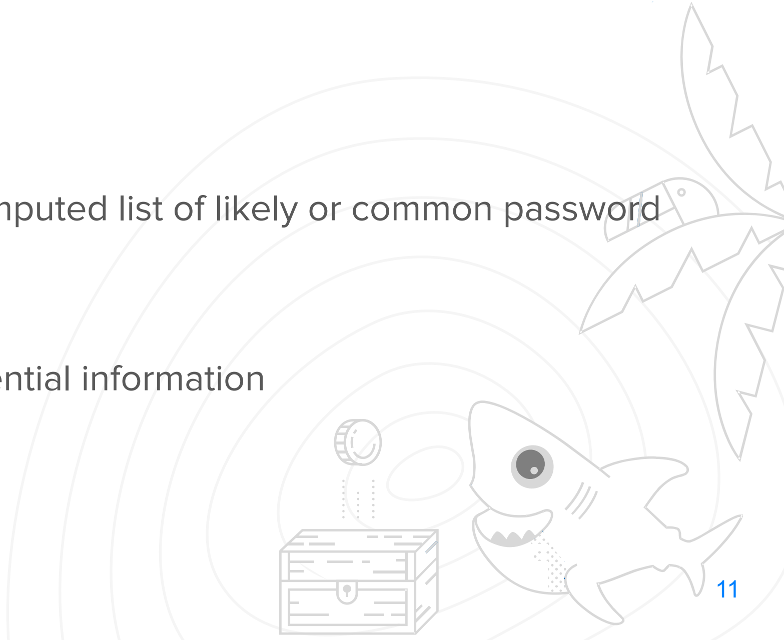
Injection Attacks

- SQL Injection
  - Injects malicious database commands are passed in and executed via an insecure input
- Code Injection
  - Injects malicious code which can execute operating system commands
- XSS
  - Injection of arbitrary JavaScript into a legitimate website which is then executed in a victim's browser



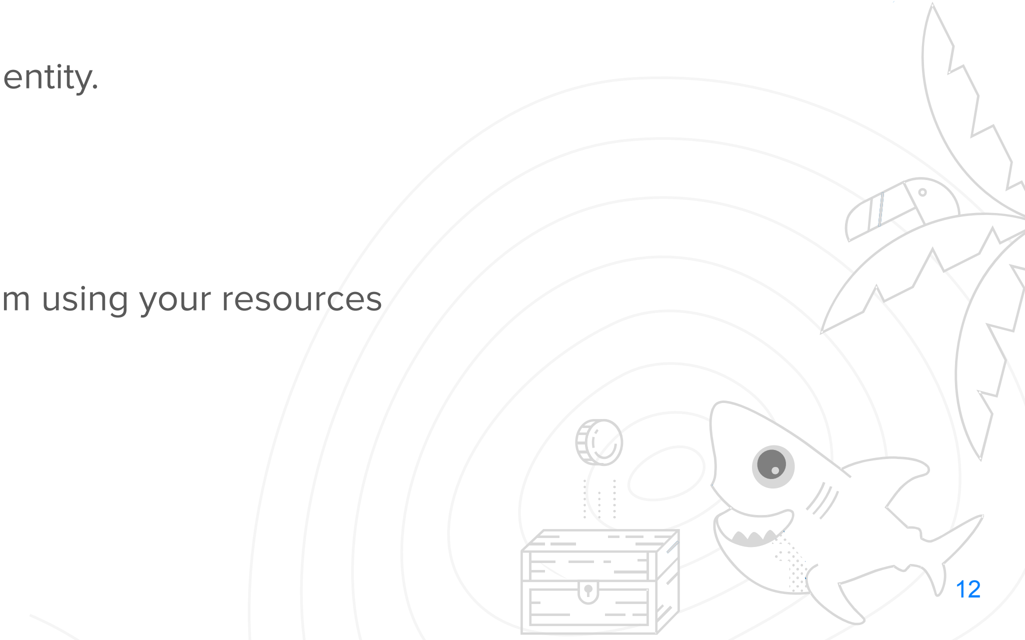
Credential Stealing

- Phishing
  - Pretending to be a legitimate entity and convincing the user to input sensitive data
- Brute Force
  - Attacker randomly guessing passwords
- Dictionary Attack
  - Attempting to gain access by using a precomputed list of likely or common password
- Social Engineering
  - Manipulating people so they give up confidential information



Network Based Attacks

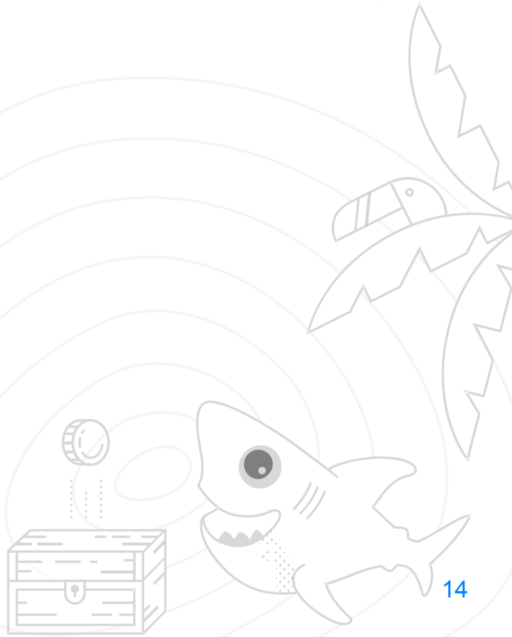
- Sniffing
  - Attacker is analyzing the network data-stream.
- Spoofing
  - Pretending to be a legitimate entity.
- Denial of Service
  - Attacker is preventing you from using your resources



Common Practices

Security in Layers

- There is no “one tool to keep them all away”
- Security works best in layers
  - Firewalls
  - Intrusion detection systems
  - Port monitoring
  - Integrity Checks
  - Etc….
- All are necessary to prevent compromise
- A bad actor may bypass one and get stuck/detected on another



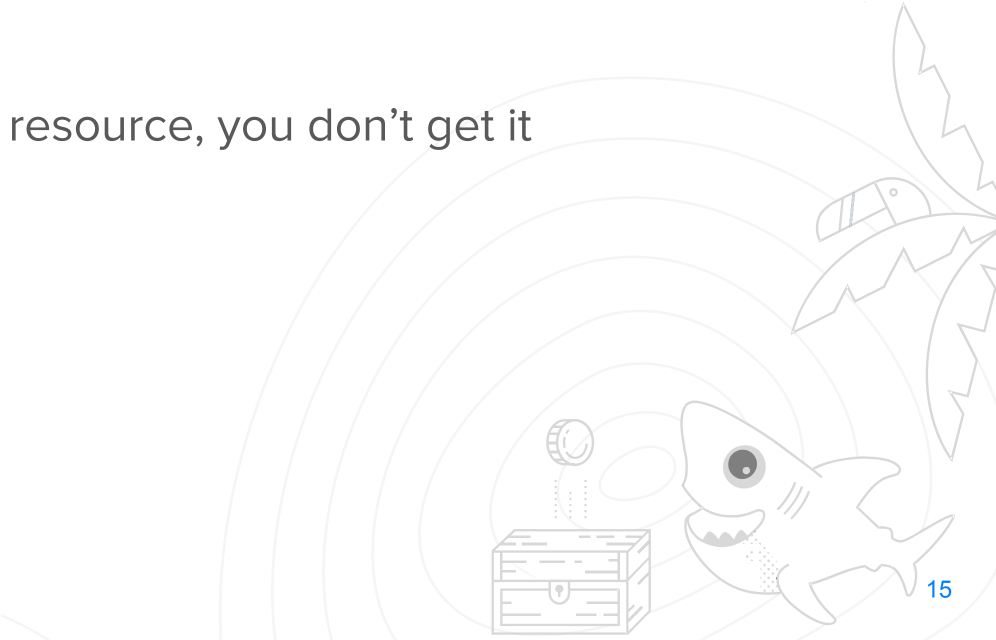
Least Privilege

- Only those who need administrator access should get it

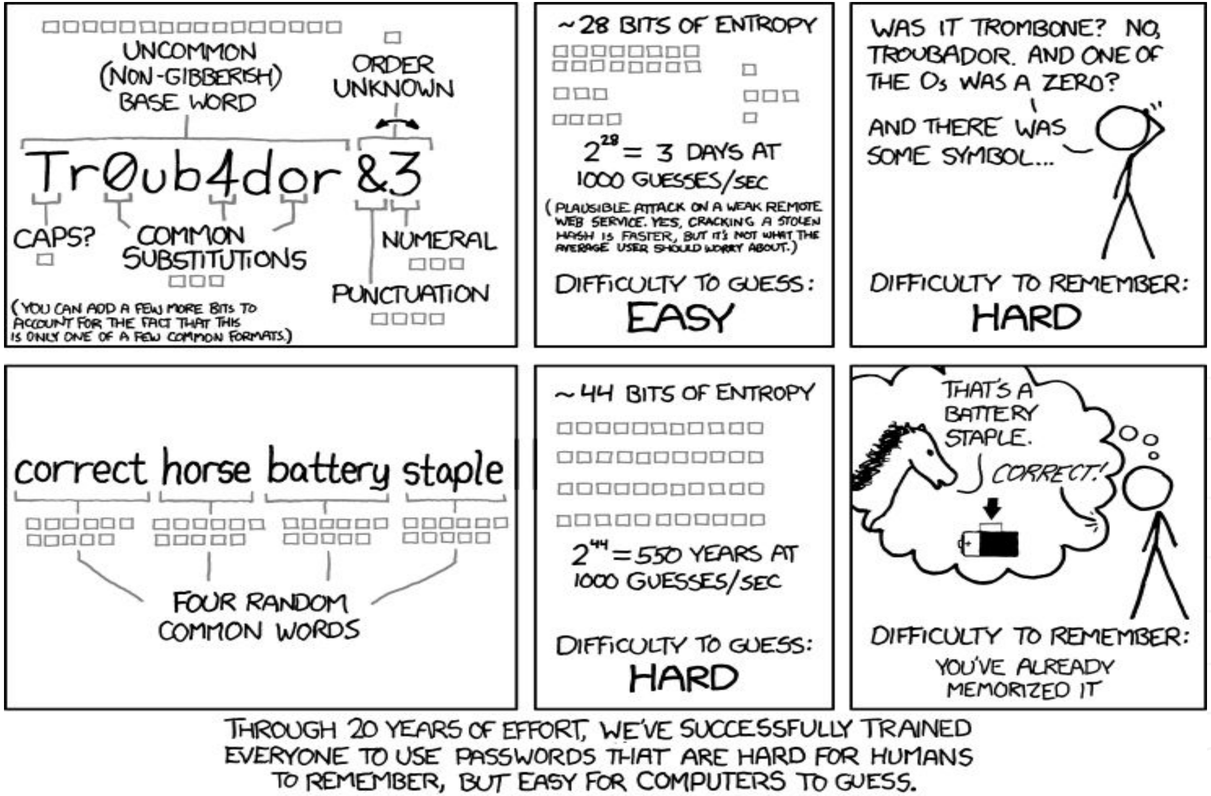
- All resources/tools/data should be behind some form of authentication and authorization

- Unless you need access to a resource, you don’t get it

- **DO NOT SSH AS ROOT!**



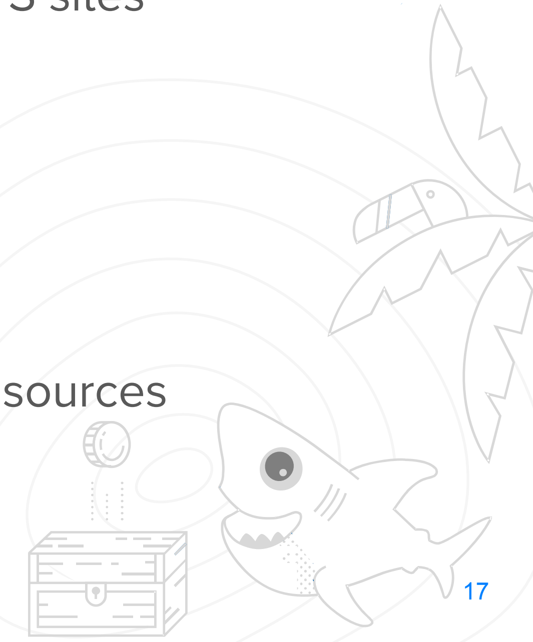
Password Policies


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44}=550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: XKCD Comic

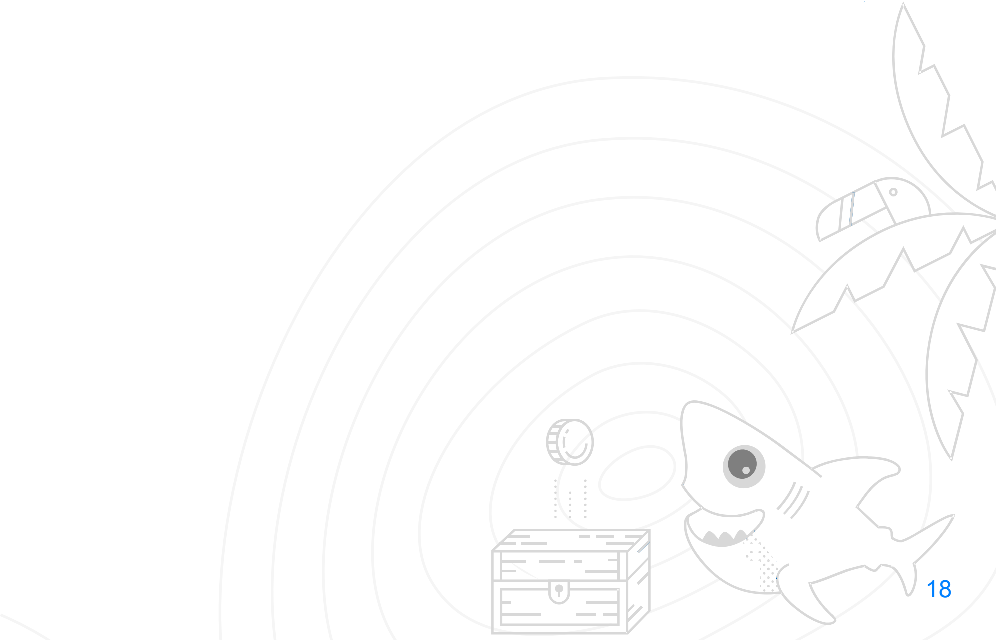
Use HTTPS

- SSL/TLS are used to ensure data sent to and from the web server is encrypted and can’t be read by outside sources (sniffing)
- Google actively warns people away from non-HTTPS sites
- Browsers warn against insecure sites
- Never been easier to secure a website
- Make sure *ALL* of your content comes from secure sources



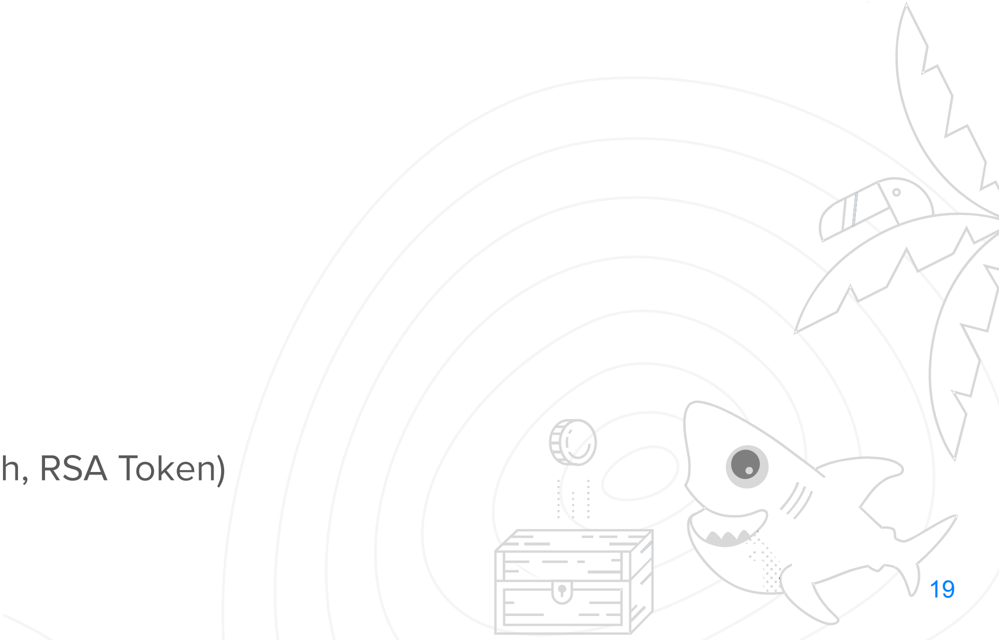
Securing SSH

- ○ Always use key based authentication
- ○ Secure with something like Fail2ban to keep out pesky bots
- ○ Use 2FA using PAM



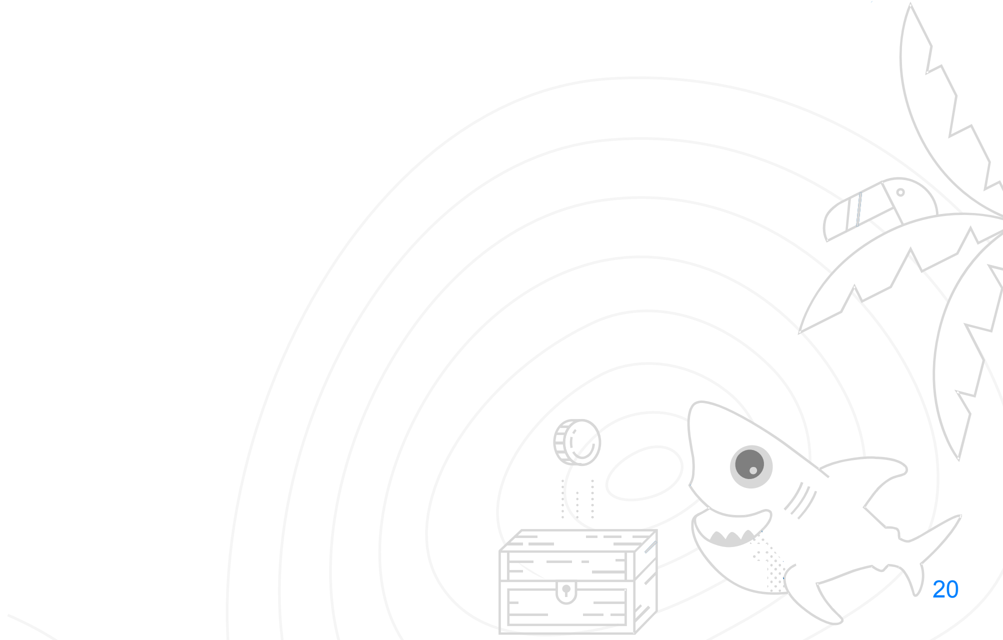
Multi Factor Authentication (MFA)

- Identity can be determined by one or more of the following
  - Something you know
  - Something you are
  - Something you have
- Something you know
  - Password, Passphrase
- Something you are
  - Fingerprint
  - Facial Scan
  - Retina Scan
- Something you have
  - Ubikey
  - Rotating Passcode (Google Auth, RSA Token)



Biometric Authentication

- ***Something you are***
- Getting better, but can be fooled
- Good option, just be weary



That’s all for this time!

○ Be sure to be on the lookout for more DigitalOcean webinars/workshops like this!

○ Tune in every last Thursday of the month to watch more of my webinars

○ My next webinar will be “Securing Your Droplet” on August 28 at 10:00 CST.

○ Try out DigitalOcean with $100 free credit for 60 days with https://do.co/mason

Thanks for attending!

DigitalOcean