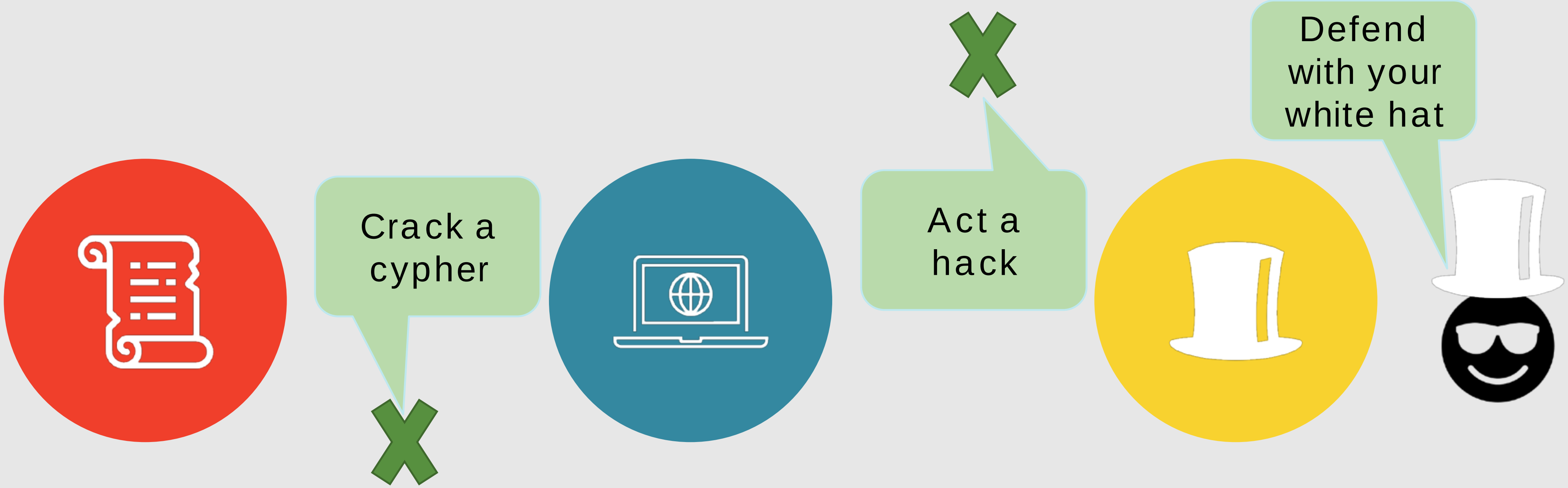
DEFENSE AGAINST THE DARK HATS

How to remain current in an ever-changing landscape by applying the basic strategies of attack and defense in cybersecurity

Mapping our route



Crack a cypher

Act a hack

Defend with your white hat

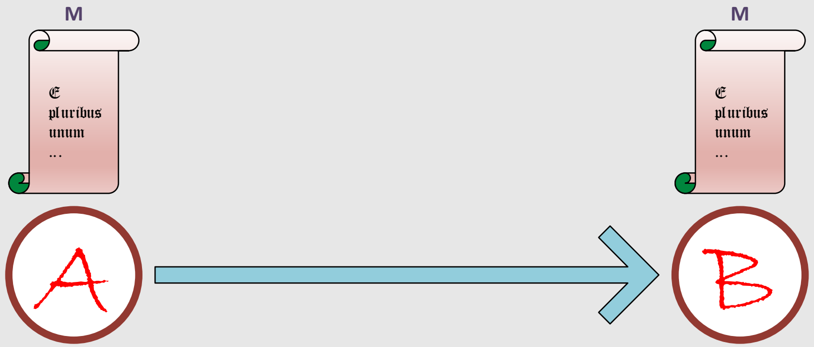
THE HISTORY OF CRYPTOGRAPHY AND OF HACKING

HACKING AROUND THE WORLD

HOW TO BE A WHITE HAT

Cryptography

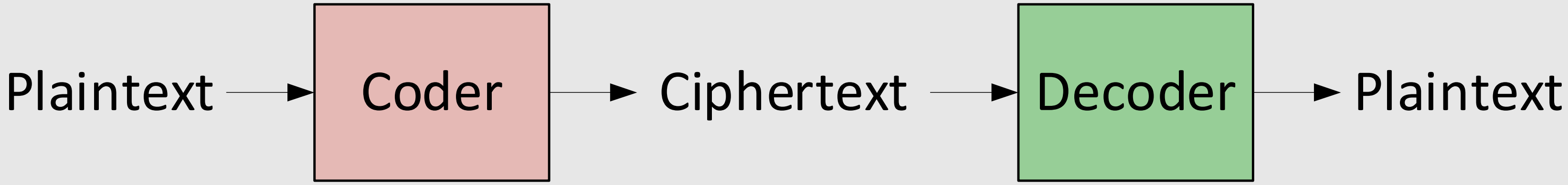
- Cryptography. n. The art of writing or solving codes.
- You want to send a message from point A to point B.
- But the message might be intentionally intercepted, accidentally lost, or peeked at by your messenger.
- You only want **authorized** recipients to be able to understand the message!



So – we use a *cipher*, meaning a <u>secret code</u>

Cryptography Definitions

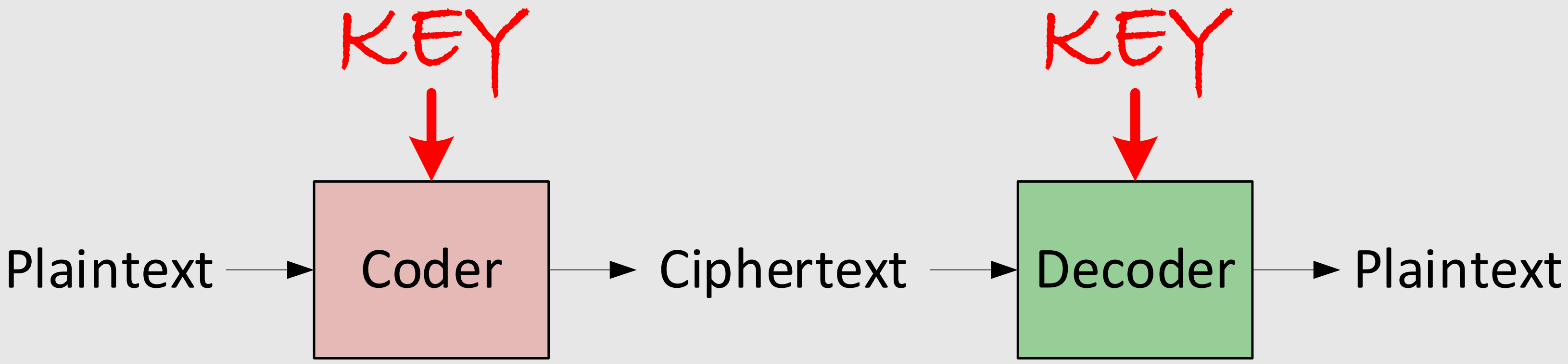
- Plaintext: Unencrypted input data
- Ciphertext: Output of the encryption process

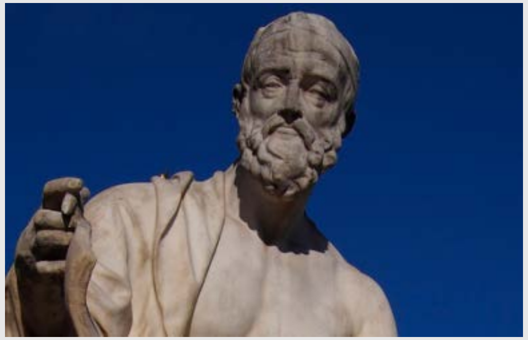


Cryptographic Key

- Many cryptographic systems are constructed as a ***family*** of ciphers.

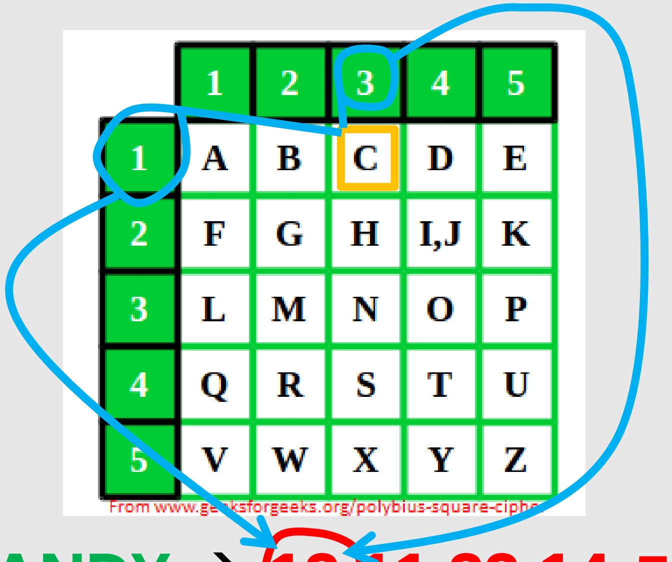
- The family **may** be publicly known – everyone knows how to code and decode messages, but they need to know the KEY *value.*





Cryptography – Ancient History

- The earliest known cryptosystem or cipher is the Polybios square (2150 years ago!)
  - Using a grid of letters, each letter of the message is replaced by the two numbers indicating the row and column for the original letter



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

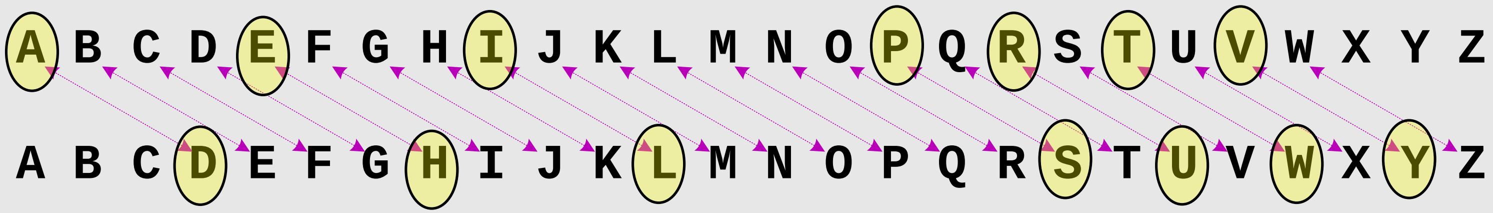
From www.geeksforgeeks.org/polybius-square-ciphe

CANDY → 13 11 33 14 54

- Julius Caesar (2100 years ago) used a cipher to protect messages of military significance
  - **Caesar Cipher**: each letter of the alphabet was coded by substituting using letters in a shifted alphabet

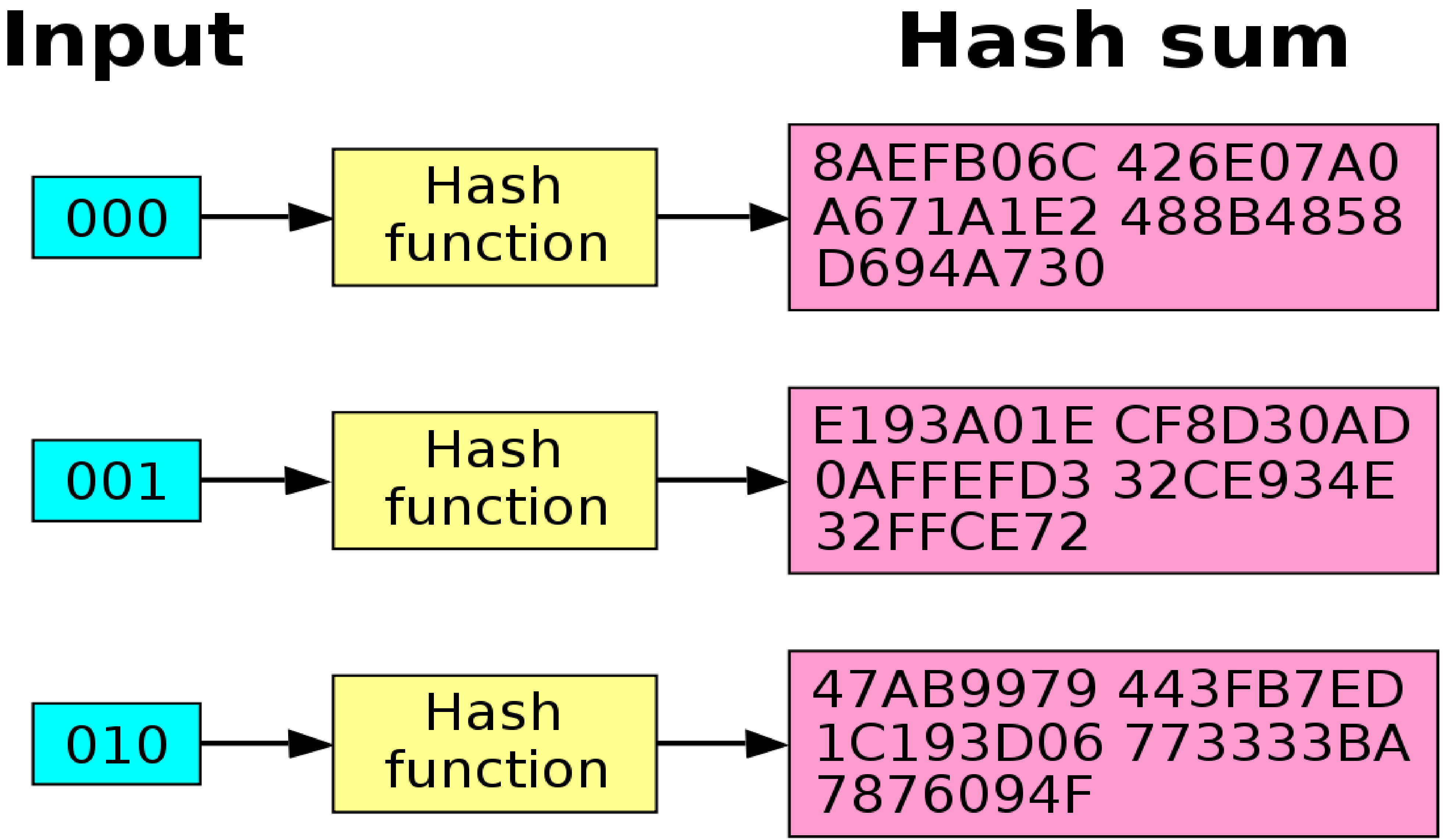
Example:

a→d: PRIVATE → SULYDWH



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



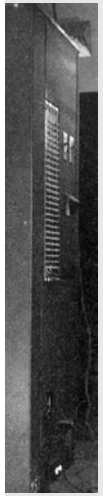
Input

Hash sum

000 → Hash function → 8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730

001 → Hash function → E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72

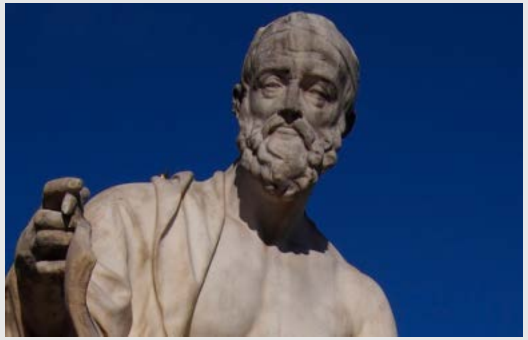
010 → Hash function → 47AB9979 443FB7ED 1C193D06 773333BA 7876094F



Some Simple Ciphers

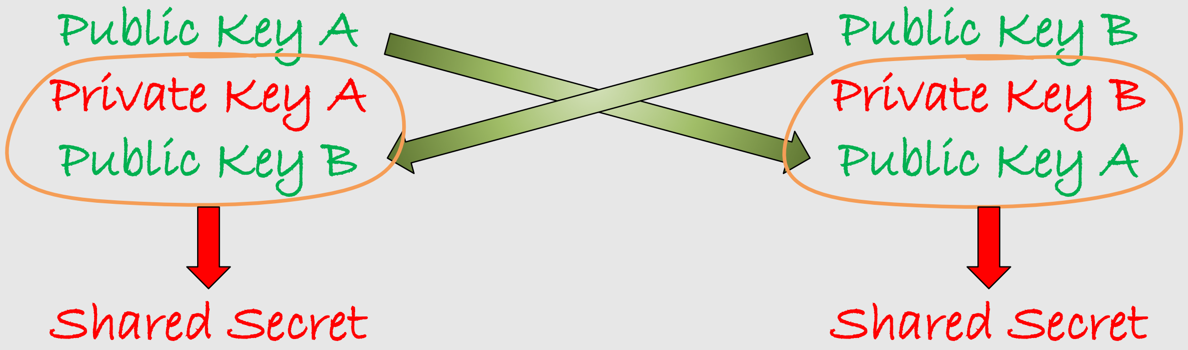
- **ROT13**
  - A Caesar cipher with a fixed alphabet shift. Used in the early days of the Internet to send spoilers and potentially offensive material. Not intended to be secure, but allow voluntary protection from being exposed to information.

- **One-time pad**
  - This is perhaps the only truly uncrackable code.
  - Each element is coded using a separate, randomly selected codebook. The sender and receiver must know the common codebook for each element. For example, one could create a Caesar cipher where the shift for each character is potentially different, and chosen at random (but shared between message sender and recipient). No set of codes is ever reused.



Public Key Cryptography

- The Diffie–Hellman Key Exchange used **Public-Key Cryptography**:
  - Parties at Point A and Point B each have their own Public Key + Private Key pair.
  - They openly exchange Public Key A and Public Key B.
  - They each combine their own Private Key with the other's Public Key to produce the **same shared secret**.



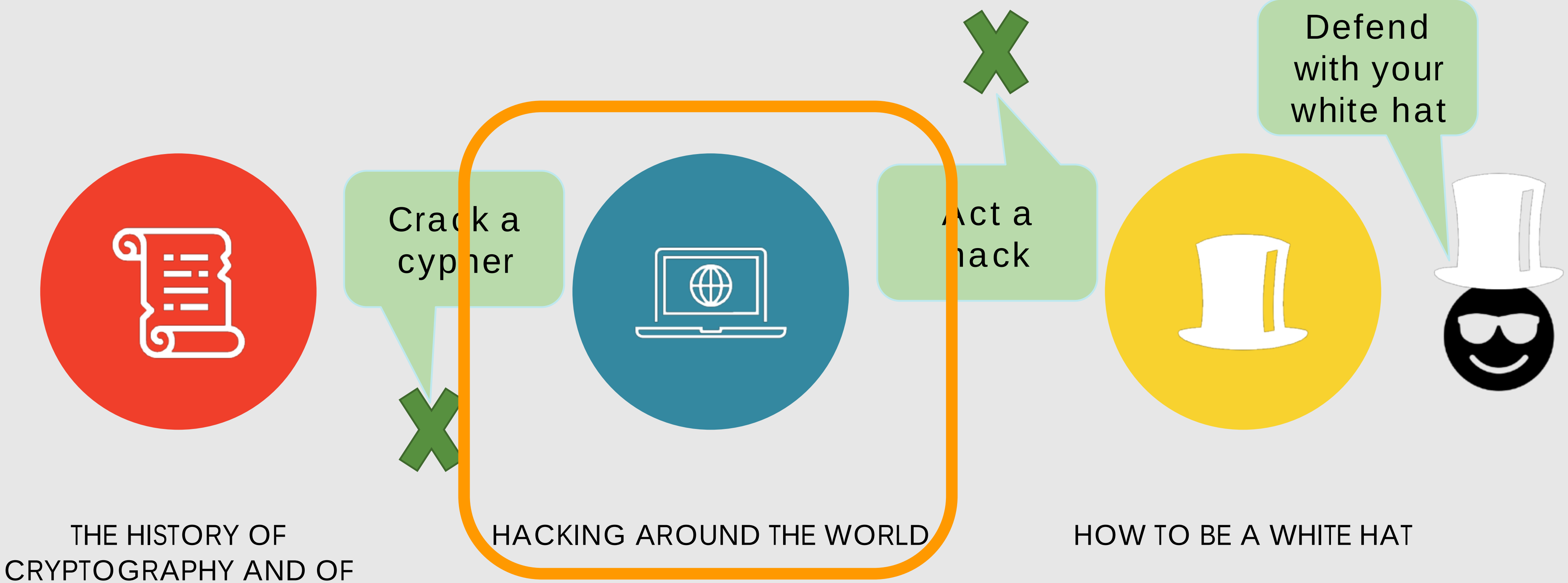
Cryptography Activity

- I will direct you to the website: picoctf.org
- Use the Username: DATDH (for Defense Against the Dark Hats)
- Guess the password!
- To decode each secret message, try an approach – the correct approach will give you a message that looks like English words (without spaces between them).

Cryptography Activities

- The Numbers Cipher, entry format:
  - PICOCTF{ALLCAPSNOSPACES}
  - A pretty simple cipher, but not one that we talked about before.
- Caesar Cipher, entry format:
  - picoCTF{lowercasenospaces}
  - The answer may not entirely look legit.
- Easy1 Cipher (one-time pad), entry format:
  - picoCTF{ALLCAPSNOSPACES}
  - Actually not that easy! HINT: the first coded message letter, U, along with the first KEY letter, S, can be decoded to the letter 'C'.
- 13 Cipher , entry format:
  - picoCTF{lower_case_with_underscores}

Mapping our route



Crack a cypher

Act a hack

Defend with your white hat

THE HISTORY OF CRYPTOGRAPHY AND OF HACKING

HACKING AROUND THE WORLD

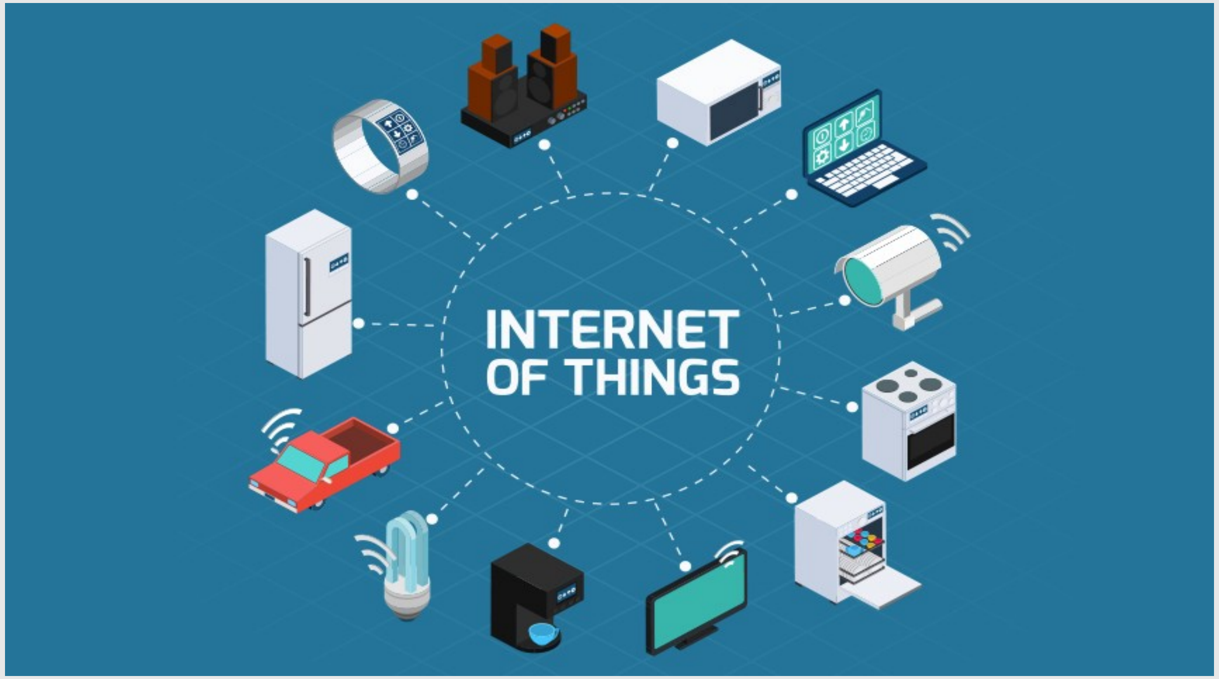
HOW TO BE A WHITE HAT

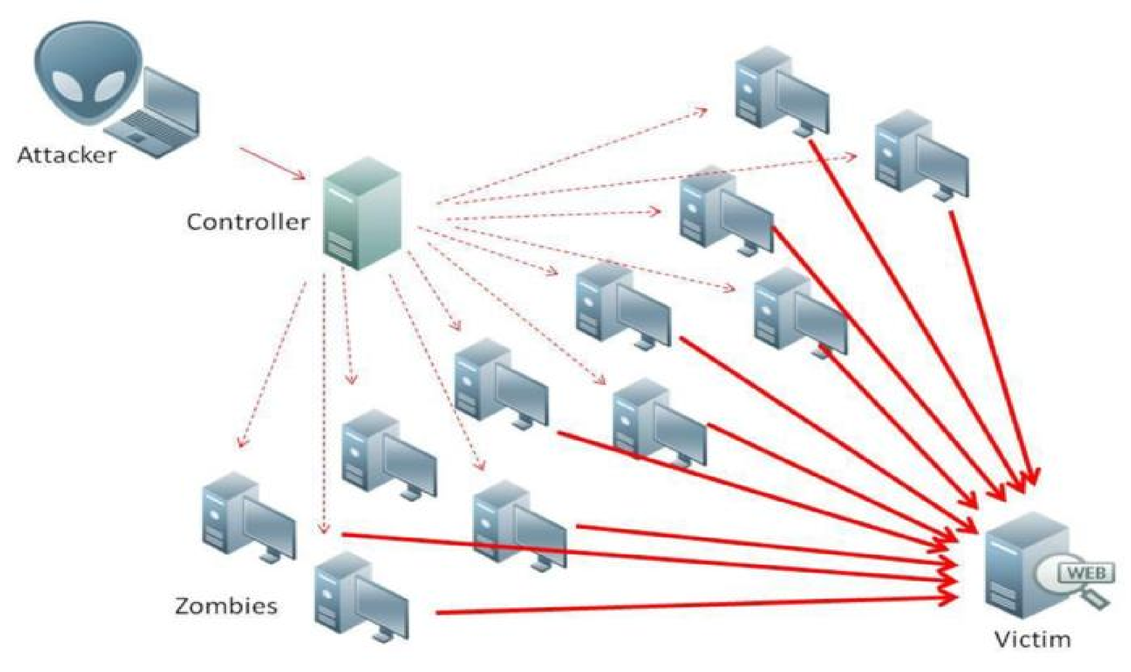
The Cybersecurity Arms Race

- Nov 2, 1988 The first global cybersecurity attack the Morris Worm infected using buffer-overflow exploit in email protocols
  - About 10% of all computers on the internet were rendered useless
- Two new defense strategies emerged from the Morris Worm
  - Try to detect infected files (this led to anti-virus software)
  - Block all packets except the ones delivered in a controlled way (this led to firewalls)
- Response to firewalls - hackers started utilizing exploits on the servers with legitimate websites to attack normal users
- Response to anti-virus software - hackers changed how their malware would be identified (i.e. their signature) without changing its functionality

The Cybersecurity Arms Race

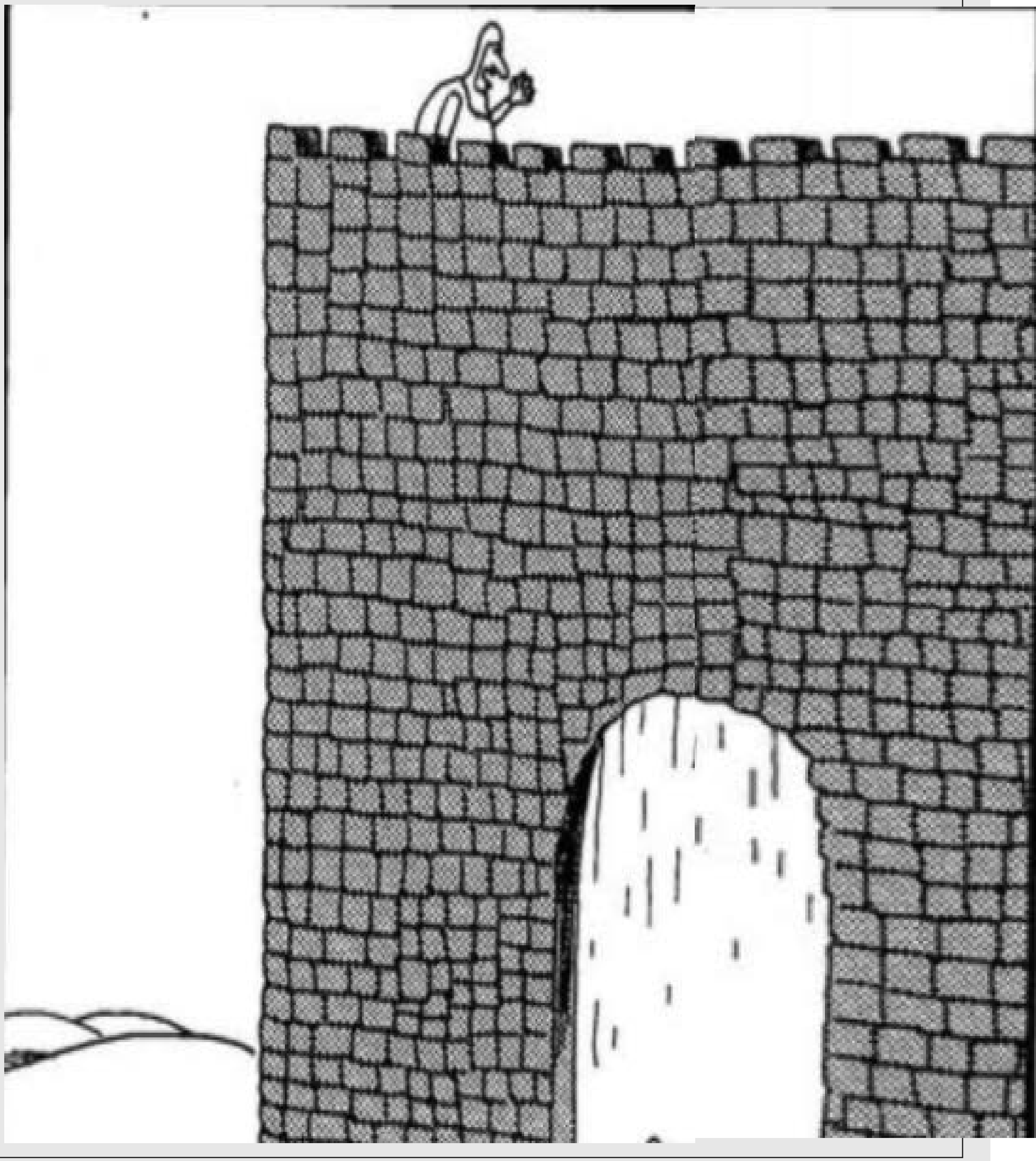
- Internet of Things (IoT) devices (e.g. smart toaster, fridge, watch, car, etc.) are simple, making them ideal targets for an exploit
- September 2016, the Mirai virus targeted IoT devices and used them in a spree of massive distributed denial-of-service (DDoS) attack





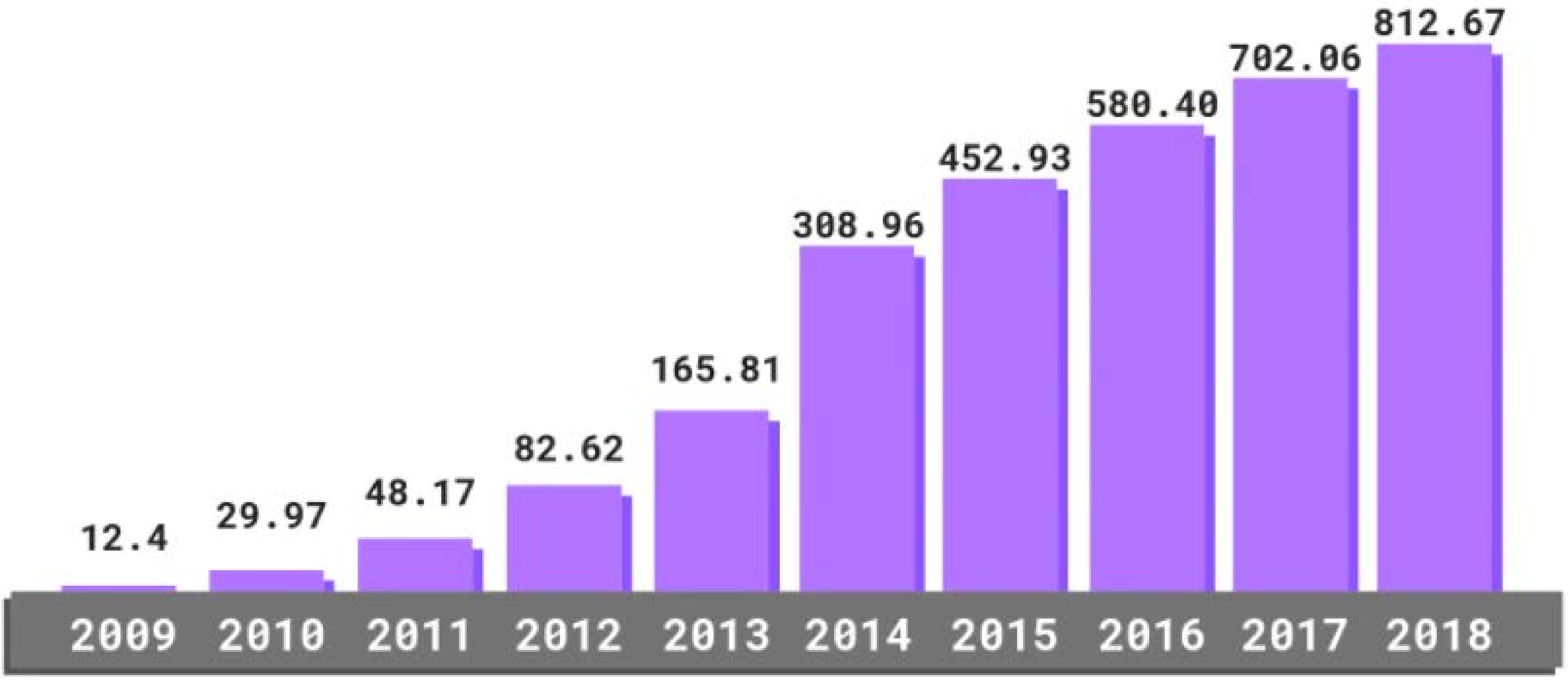
Social Engineering

- **Phishing** (e.g. email with a fake link)
- **Pretexting** (e.g. fake security representative asks for your password to secure your account he claims has been breached)
- **Reverse Social Engineering** (e.g. fake tech support company uses search engine optimization to position their phone number at the top of a Google search of a malware they are secretly responsible for and then asks you to give access to your computer to solve it when you call)
- **Tailgating** (e.g. following a real employee through the secure door and dropping a flash drive with malware)
- **Whaling and Spear Phishing** (e.g. deep research into Yahoo Engineer to fool him and get access to everyone’s email)
- Social engineering has been around long as there has been coveted information
- 2013, over 110 million customers had personal and credit card info stolen, because of Social engineering on an HVAC company with remote access to Target’s network, which was then hacked
- 15 year old Kane Gamble obtained secure emails of the director of the CIA, by convincing Verizon to provide personal details, which allowed Kane to impersonate him and change his credentials



Major Updates in Cyber Security

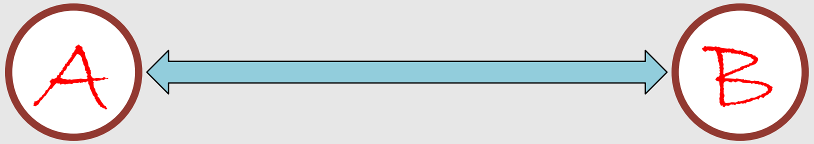
- The problem has exploded in severity!
  - In 1988 there was virtually no cost to cybersecurity
  - The average cost of a security breach affecting small businesses rose from $229k in 2018 to $369k in 2019
  - According to Cybersecurity Ventures, cybercrime will cost the global economy $6.1 trillion annually in 2021
- The complexity; AI and machine learning have made attacks and pre-attack research more effective and sophisticated
- The risk; in 2018 the FBI told The Wall Street Journal that every American citizen’s data may be stolen and on the dark web
- The reward - the average cybersecurity salary is rising to just shy of $100,000 dollars per year



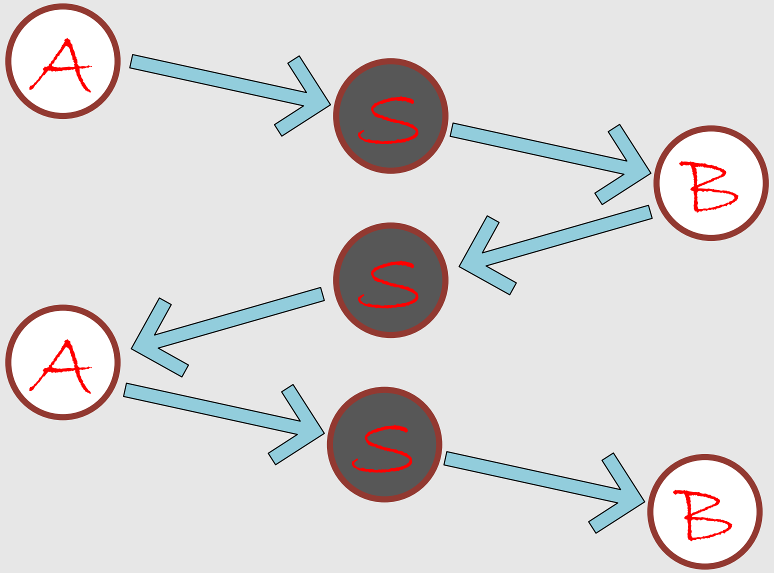
Total Malware Infection Growth Rate (In Millions)

“Man-In-The-Middle” Attack

- Points A and B think that they’re just talking to each other, in private



- In reality, there is a **SPY, S**, in the middle, intercepting and forwarding messages.



“Man-In-The-Middle” Attack

- You think that you click on a link (perhaps in an email, or online ad) to your favorite website, maybe “Instagram.com”
- It actually takes you to 1nstagram.com, or instogram.com
- This MITM (man-in-the-middle) actually goes to the real website, and pretends to be you. On your behalf it requests web pages, and returns them to you.
  - Almost everything looks normal to you!
  - The MITM can capture your usernames, passwords, and any other information that you exchange!
- How to spot a problem:
  1. The URL shown in your browser doesn’t look right – either misspelled, or funny characters
  2. The URL starts with http:// rather than https://
- How to avoid getting tricked:
  - Do not click on links in any suspicious emails. The safest way is to copy the link and examine it before going to the site, or manually type the correct link into your browser.

Exploit Activity

- Write a script, and act out an example of a “Man in the Middle” attack.
- Could be cyber-ish scenario or real-world scenario.

Act Out a Man-in-the-Middle Scenario

Cast: **Joe Browser** (wants to browse their favorite web site)

Bette Midler (intercepts the website request, forwards the request, but intercepts keystrokes)

Ender Wiggin (legitimate web site, does not know that anything is wrong)

Example dialogue:

Joe: Hi Ender, how are you doing today?

Bette (intercepting the greeting, to Ender): Hi Ender, how are you doing today?

Ender (thinking they are communicating with Joe, but are actually communicating with Bette): Hi Joe, I've got many things to show you, but first I'd like you to log in, just like you always do.

Bette (to Joe): Hi Joe, I've got many things to show you, but first I'd like you to log in, just like you always do.

NOTE: Have the narrator tell us what the person in the middle is doing. For example, writing down usernames and passwords.

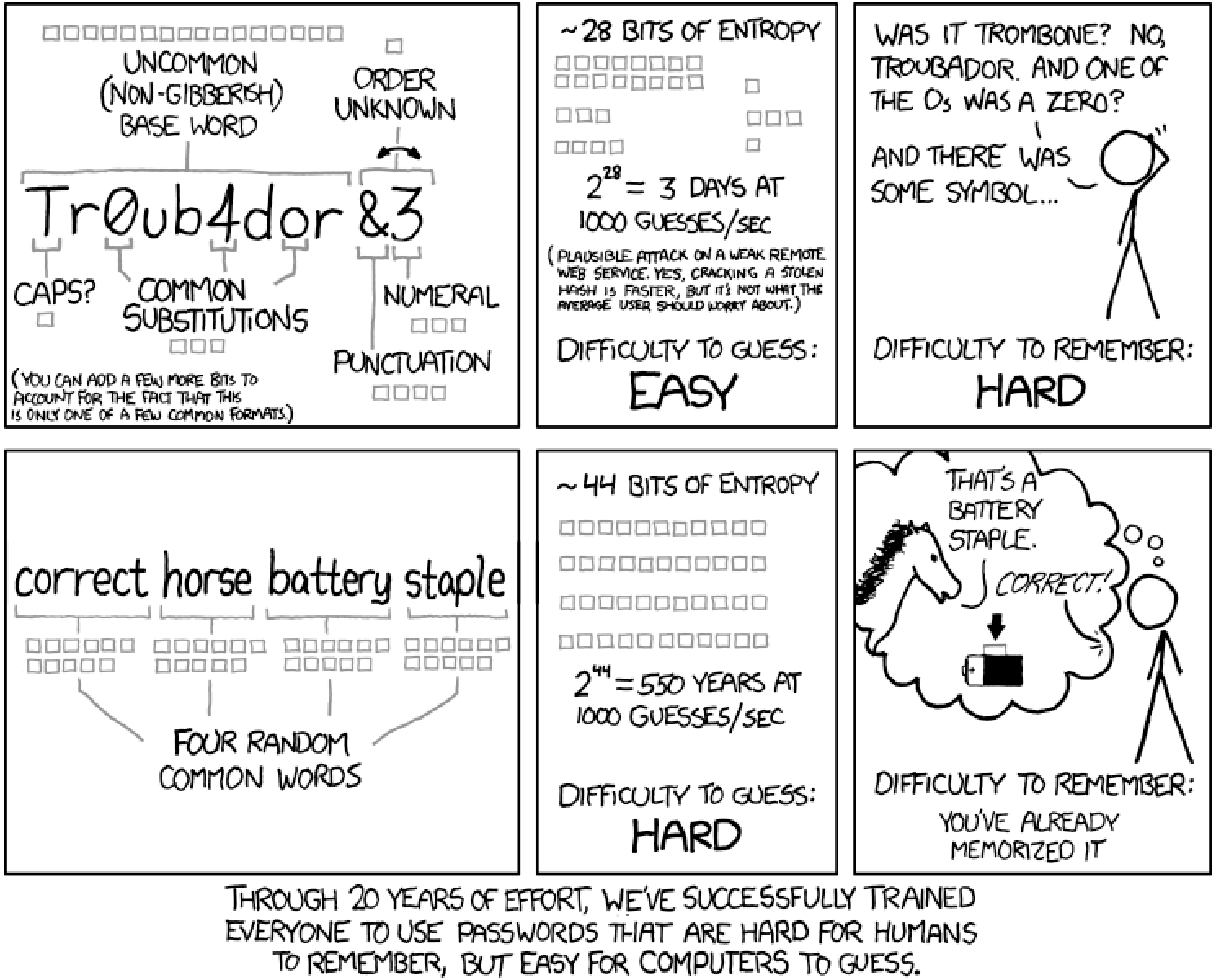
Change the names, to protect the innocent. Do not ever use your real passwords in any examples. ☺

Cracking Passwords

- Passwords are used as keys to access things that you consider valuable:
  - Your GMail, Instagram, Snapchat, Twitter and Facebook accounts
  - Your Amazon and other shopping accounts
  - Your Fortnite, Warcraft, Minecraft, League of Legends, etc.
- Passwords are often stored using encryption
  - But - when a service is cracked, hackers can often guess your password by trying every possible combination of dictionary words and other common decorations.
  - When they produce ciphertext that matches your password’s ciphertext, they’ve got a crack, and you’re toast!

Password Strength

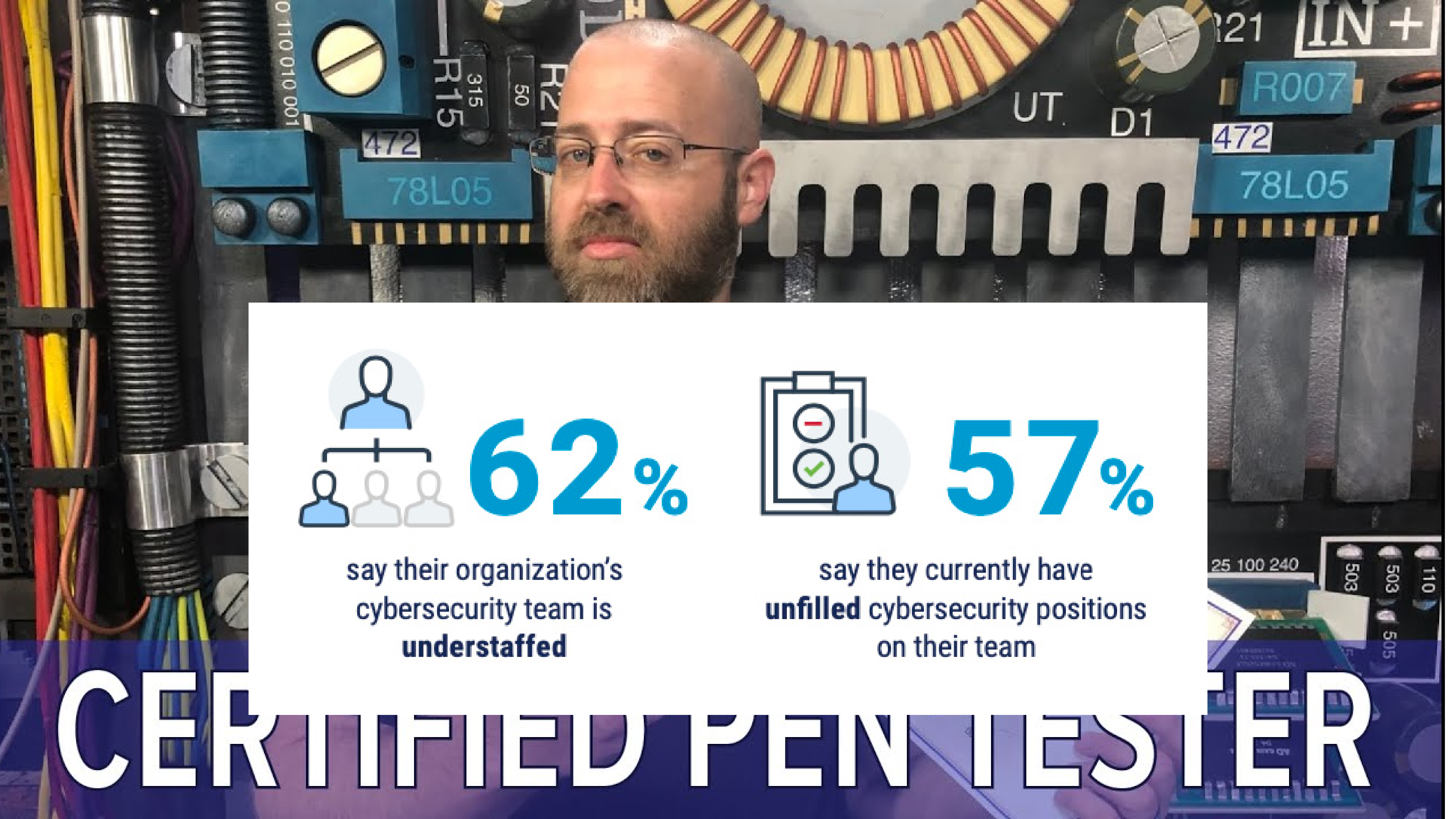
From https://xkcd.com/936/



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.

Password Recommendations

- Use 12-character minimum
- Use passphrases, and mix in symbols and numbers
- Avoid combining fewer than 4 dictionary words or names
- Don’t reuse passwords, if you can avoid it
- Use a different password for each service
- Don’t use too many repeated characters
- A good password looks like random letters, but is easy for you to remember:
  - Otywsse!1778SSE



62%

say their organization's cybersecurity team is **understaffed**

57%

say they currently have **unfilled** cybersecurity positions on their team

CERTIFIED PEN TESTER

YOU MADE IT!

Let’s play a game to celebrate

Works Cited

- *The History of Cryptography*, cs.stanford.edu/people/eroberts/courses/soco/projects/public-key-cryptography/history.html.
- Borowski, Susan. “Code-Breaking Instrumental in Ending World War II.” *American Association for the Advancement of Science*, 2012, www.aaas.org/code-breaking-instrumental-ending-world-war-ii.
- Limon, Rifat. “BANGLADESH BANK SCAM.” *Academia.edu*, 8 Oct. 2018, www.academia.edu/37558490/BANGLADESH_BANK_SCAM.
- Author, No. “Cyberthieves Exploit Banks' Faith in SWIFT Transfer Network.” *The Japan Times*, 22 May 2016, www.japantimes.co.jp/news/2016/05/22/world/crime-legal-world/cyberthieves-exploit-banks-faith-in-swift-transfer-network/.
- Author, No. “Cyberthieves Exploit Banks' Faith in SWIFT Transfer Network.” *The Japan Times*, 22 May 2016, www.japantimes.co.jp/news/2016/05/22/world/crime-legal-world/cyberthieves-exploit-banks-faith-in-swift-transfer-network/.
- “How a Spelling Mistake Stopped Hackers Stealing $1bn in a Bank Heist.” *The Independent*, Independent Digital News and Media, 11 Mar. 2016, www.independent.co.uk/news/world/asia/spelling-mistake-stops-hackers-stealing-1-billion-bangladesh-bank-heist-a6924971.html.
- “SWIFT Announces Updates to the Customer Security Controls Framework for Attestation in 2019: SWIFT - The Global Provider of Secure Financial Messaging Services.” *SWIFT*, 13 Aug. 2018, www.swift.com/news-events/news/swift-announces-updates-customer-security-controls-framework-attestation-2019.
- Authors: James Waldo Katherine Mansted | February 2018, et al. “Ending the Cybersecurity Arms Race.” *Belfer Center for Science and International Affairs*, Feb. 2018, www.belfercenter.org/publication/ending-cybersecurity-arms-race.
- Papazov, Yavor. “Social Engineering.” *S&T Organization*.
- CISM, Raef Meeuwisse. “Is Effective Cybersecurity Expensive?” *Infosecurity Magazine*, 10 Apr. 2019, www.infosecurity-magazine.com/blogs/effective-cybersecurity-expensive.
- DFLabs. “The Cost of Cybersecurity Solutions vs. The Cost of Cyber Attacks.” *DFLabs*, 4 Jan. 2021, www.dflabs.com/resources/blog/the-cost-of-cybersecurity-solutions-vs-the-cost-of-cyber-attacks/#:~:text=According%20to%20the%20findings%20from,highest%20cost%20per%20record%20data.
- Freeze, Di. “Cybercrime To Cost The World $10.5 Trillion Annually By 2025.” *Cybercrime Magazine*, 22 Jan. 2021, cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
- “Cybersecurity Salaries and Job Outlook.” *Berkeley School of Information*, 25 Apr. 2019, ischoolonline.berkeley.edu/blog/cybersecurity-salary/.
- 2, February, et al. “Cybersecurity Budgeting and Spending Trends 2020: How Does Yours Compare?” *Infosec Resources*, 16 Oct. 2020, resources.infosecinstitute.com/topic/cybersecurity-budgeting-and-spending-trends/.
- “Penetration Tester Annual Salary ($116,323 Avg: Jan 2021).” *ZipRecruiter*, www.ziprecruiter.com/Salaries/Penetration-Tester-Salary.
- Kehrli, Jerome. “Technological Thoughts by Jerome Kehrli.” *Niceideas.ch: Deciphering the Bangladesh Bank Heist*, 15 Nov. 2017, www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist.
- The true cost of a data breach & cyber attack. (2020). Retrieved February 07, 2021, from https://www.mcpc.com/Insights/Blog/May-2017/True-Cost-Data-Breach
- Lin, M. (2017, September 07). Cybersecurity: What Every CEO and Cfo should know. Retrieved February 07, 2021, from https://www.toptal.com/finance/finance-directors/cyber-security
- Help Net Security February 25. (2020, February 24). Cybersecurity hiring challenges and retention issues demand new talent pipelines. Retrieved February 07, 2021, from https://www.helpnetsecurity.com/2020/02/25/cybersecurity-hiring-retention/