Innovation & Technology

Security Awareness Training

PRESENTED BY:

Jose J. Peña, Director

Rick Castro, Asst. Director

October 17th, 2018

Alex Velazquez, Systems & Security Manager

Jason Fernandez, Systems & Security Analyst

Agenda

- What is Cybersecurity?
- Security Threats
- Techniques
- Tips
- Resources
- Videos
- Questions

Pharr

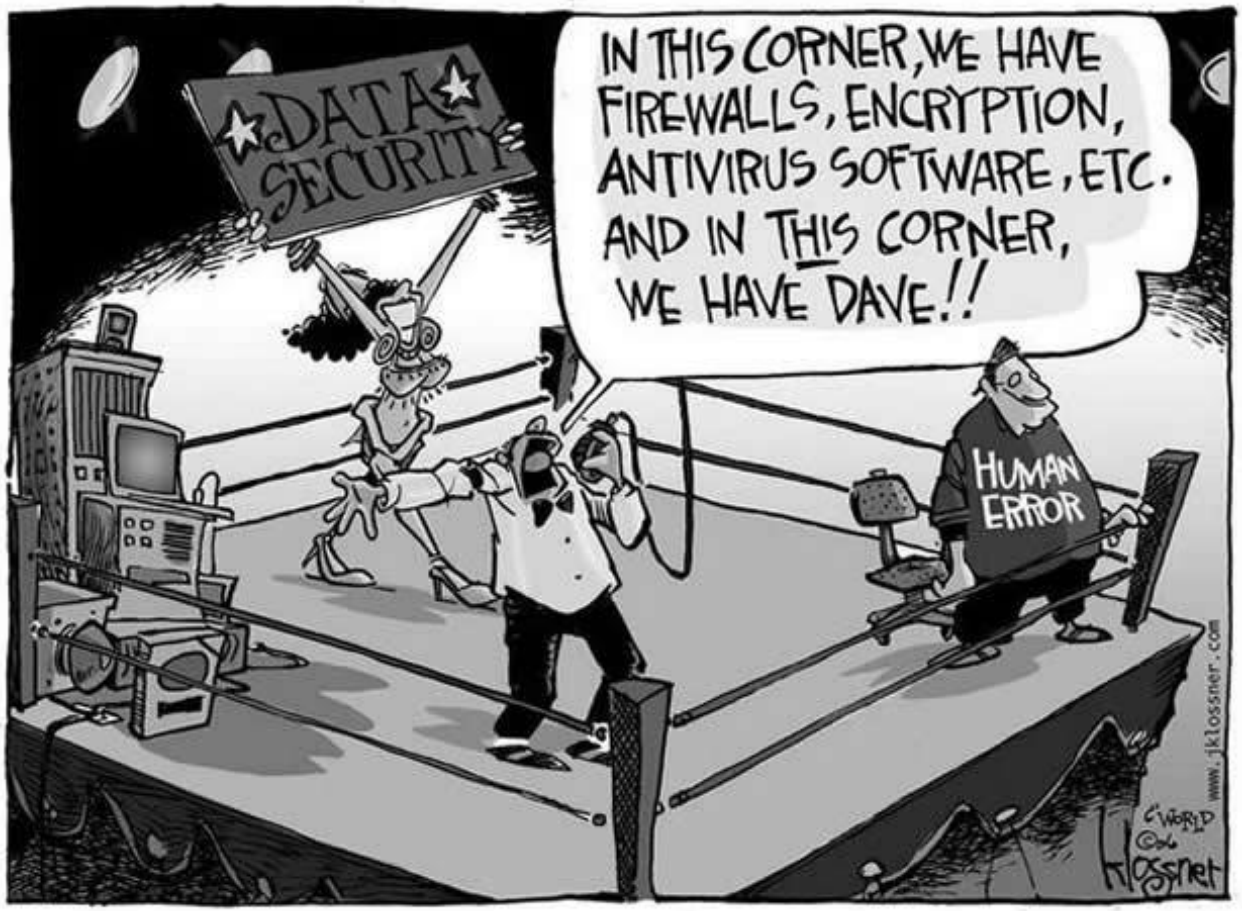
pharr-tx.gov

What is Cybersecurity?

- Cybersecurity refers to a set of techniques used to protect networks, computers, and data from attack, damage, or unauthorized access

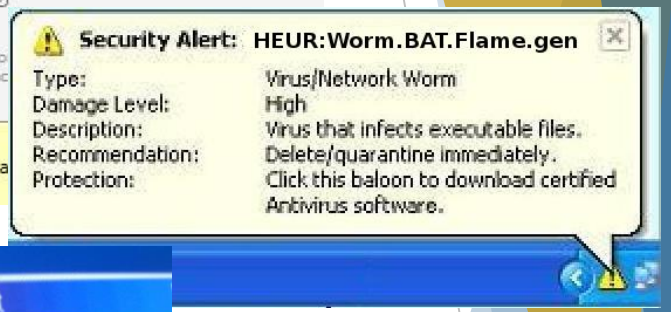
What is the biggest vulnerability in Cybersecurity?

Security?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
WORLD
Klossner

Security Threats

- Malware includes:
  - Viruses
  - Trojan horses
  - Worms
  - Spyware
  - Adware
  - Ransomware
  - *Cryptomining*!

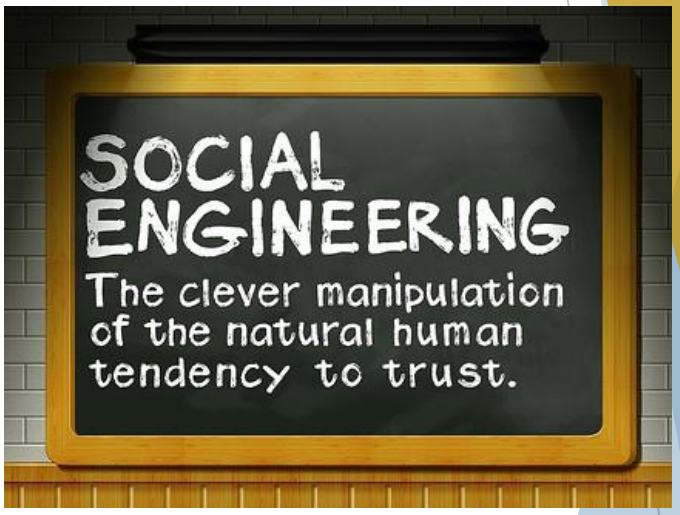


Pharr
pharr-tx.gov

Techniques

- **Social Engineering :**

- *Manipulating people to give up confidential information*
  - CEO Fraud
  - Email Phishing/SpearPhishing
  - USB drive phishing
  - Vishing



- GOAL: Get Username and Password!

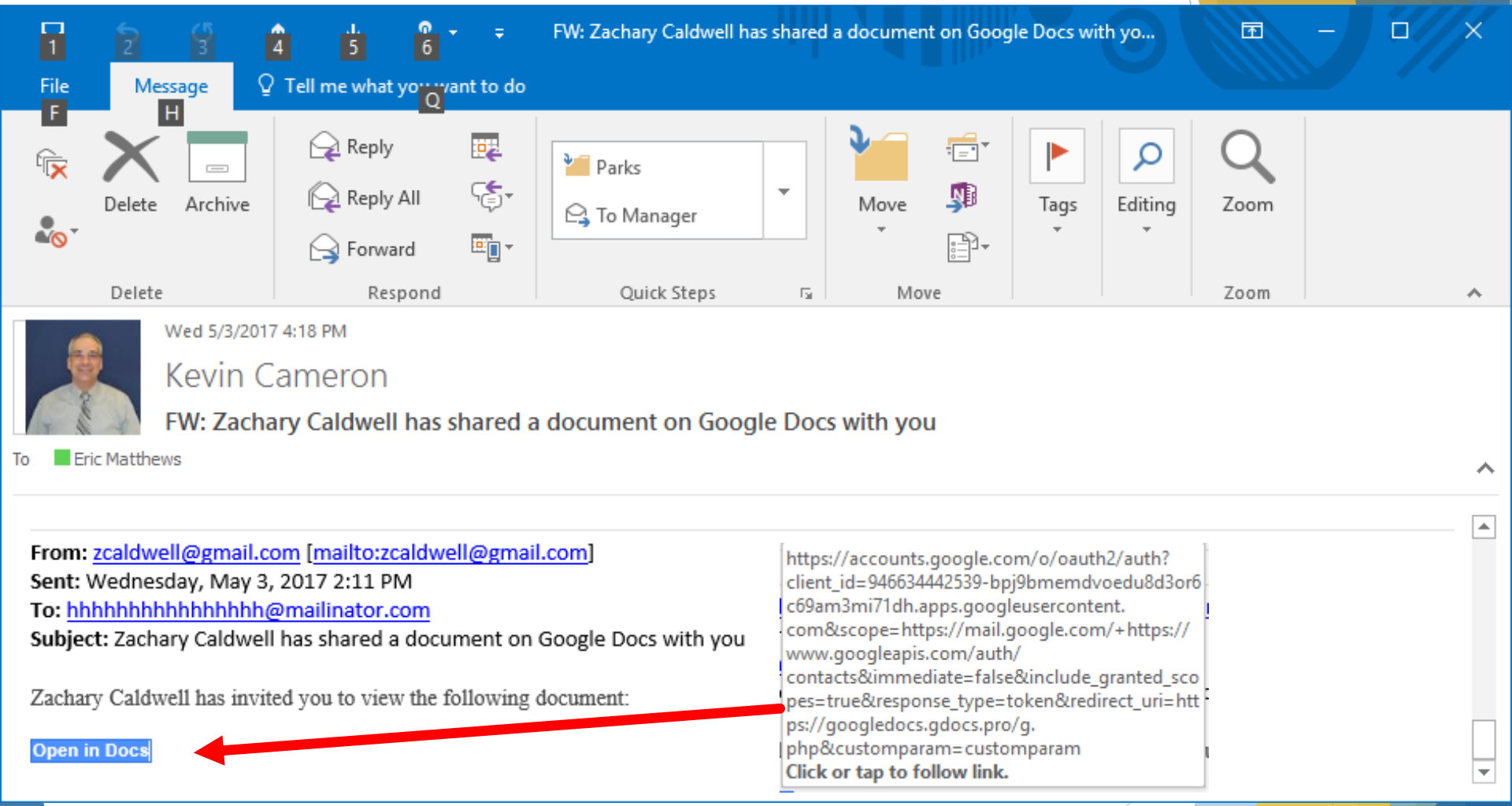
Techniques

- Phishing Emails – *by the numbers*

- **30%** of people open phishing emails
- **12%** of those that open the emails go on to click on their attachments
- The median time from when a batch of phishing emails is sent out and people open them and click on the links they contain is ***1 minute, 40 seconds***
- **#1 delivery vehicle for malware is email attachments**

Gone Phishing….

Some common signs of a possible phishing attempt:



Pharr

pharr-tx.gov

Tips - *Phishing*

- Social Engineering/Phishing :
  - **Protect** your user ID and password, especially from vendors
  - If a message uses high pressure tactics or threats, **be skeptical**
  - **Beware** of attachments
  - Remember to "**hover**" over links

Tips – *Social Media*

Think Before

- Posting a message
- Uploading photos
- Downloading games or software
- Buying something online
- Replying to message

Remember

- Once you post something online, you can't take it back

Tips - *Privacy*

- Use privacy settings on phones and apps
- Share your location only with people you know personally
- Don’t reply to messages that ask for your personal information
- Don’t stay permanently signed in to accounts

- *<u>Keep Confidential</u>*
  - Social Security Number
  - Driver's License Number
  - Mother's Maiden Name
  - Credit / Debit Card Number
  - Bank Account Number

Tips – *Mobile Devices*

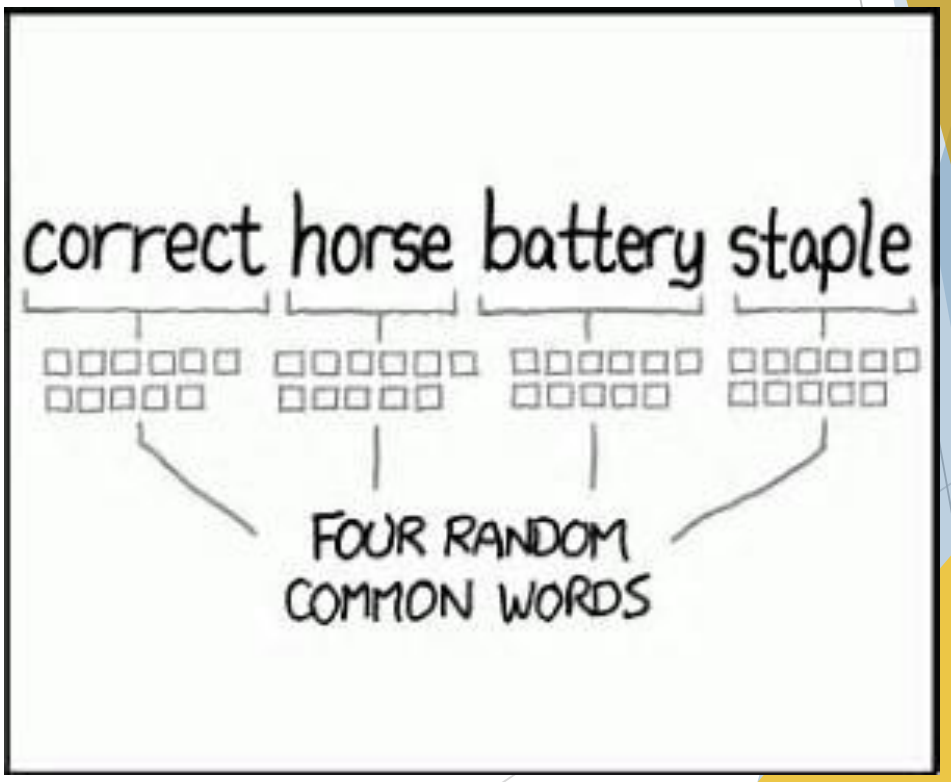
- Turn off the wireless when is not in used
- Turn off the Wi-Fi auto-connect feature
  - Always choose which wireless network to use and when
- Set a password for your device
- Set a screen lock time for your device
  - Time restriction can be 3 minutes
- Backup your files to an external drive or cloud
- Remember: Weather it's your phone, laptop, or tablet, don't leave it in public

Tips - *Passwords*

- **Passwords**
  - DO NOT share your password with anyone
  - NEVER DISCLOSE YOUR PASSWORD IN AN EMAIL OR OVER THE PHONE

Tips - *Passphrases*

- Passphrases or random words are great.
- Make it work for you!



GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

2 Uppercase | 2 Lowercase | 2 Digits | 2 Symbols | 8 Characters

E$4dEt6&

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	8 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	6,704,780,954,517,120
Search Space Size (as a power of 10):	6.70×10^{15}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	2.13 thousand centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	18.62 hours
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.12 minutes

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

(The Haystack Calculator has been viewed 2,413,423 times since its publication.)

Pharr

pharr-tx.gov

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

No Uppercase | 25 Lowercase | No Digits | No Symbols | 25 Characters

thisisareallylongpassword

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26
Search Space Length (Characters):	25 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	246,244,783,208,286,292, 431,866,971,536,008,150
Search Space Size (as a power of 10):	2.46×10^{35}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	78.30 billion trillion [illegible]
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	7.83 hundred trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	7.83 hundred billion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

(The Haystack Calculator has been viewed 2,413,423 times since its publication.)

Pharr

pharr-tx.gov

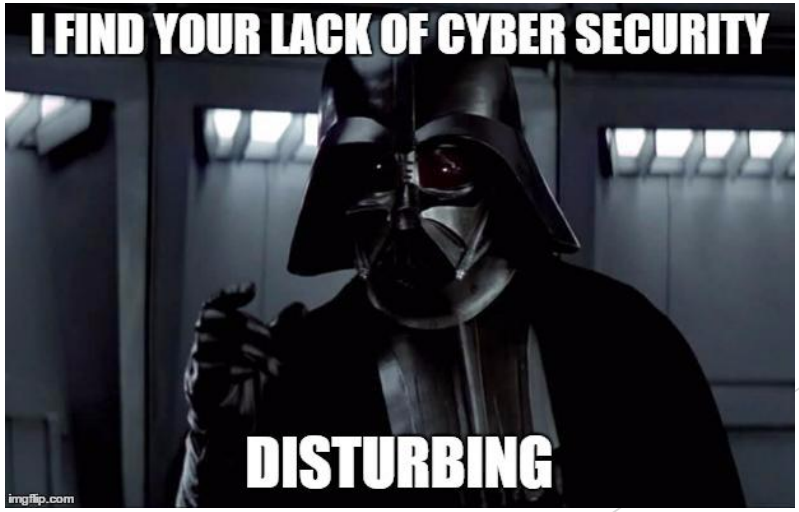
Tips – *for Home*

- Beware phone number **spoofing** – screen your incoming calls
- **Backup** your files – hard drive or online ("the cloud")
- Install ***Malwarebytes*** and scan regularly
- Use **Antivirus** and set it to auto-update. *Free* is better than none!

Pharr
pharr-tx.gov

Cell Phones, Tablets and Phablets…Oh My

- Mobile devices count!
- Keep devices updated with the latest security updates
- Remember, USB drives can be compromised, too
- Beware of “SMiShing”



Pharr
pharr-tx.gov

Stop. Think. Connect. Campaign

STOP. THINK. CONNECT.™ is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. There are a variety of free online safety resources, including tip sheets, videos, posters and memes, that you can download and share.

STOP: make sure security measures are in place. **THINK**: about the consequences of your online actions. **CONNECT**: and enjoy the Internet. There are more than 100 STOP. THINK. CONNECT.™ resources, including videos, tip sheets, infographics and memes, that are available for free to download and share at home, at work and in the community.

Pharr

pharr-tx.gov

Innovation & Technology Online Resources

- http://pharr.it

- Security Awareness Resources
- Videos
- Publications

Pharr
pharr-tx.gov

Training Videos

- General computer security
- Using public Wi-Fi networks
- Protecting your computer from Malware
- Protecting children online
- Online banking security
- Securing your home networks

Questions?

Innovation & Technology

Security Awareness Training

PRESENTED BY:

Jose J. Peña, Director

Rick Castro, Asst. Director

October 17th, 2018

Alex Velazquez, Systems & Security Manager

Jason Fernandez, Systems & Security Analyst