CYBER SECURITY OVERVIEW

DAVID G. CHACON

INFORMATION TECHNOLOGY AUDITOR

APRIL 05, 2019

THE FUNDAMENTALS

- Lock your devices and protect your devices
- Anti-Virus Solutions and Malware Solutions
- Patch your devices (All of Them)
- Patch your home routers or replace
- Avoid Public Wi-Fi
- Choose an Email carrier wisely
- Use a VPN for sensitive transactions
- Backup your devices separately

CURRENT TRENDS

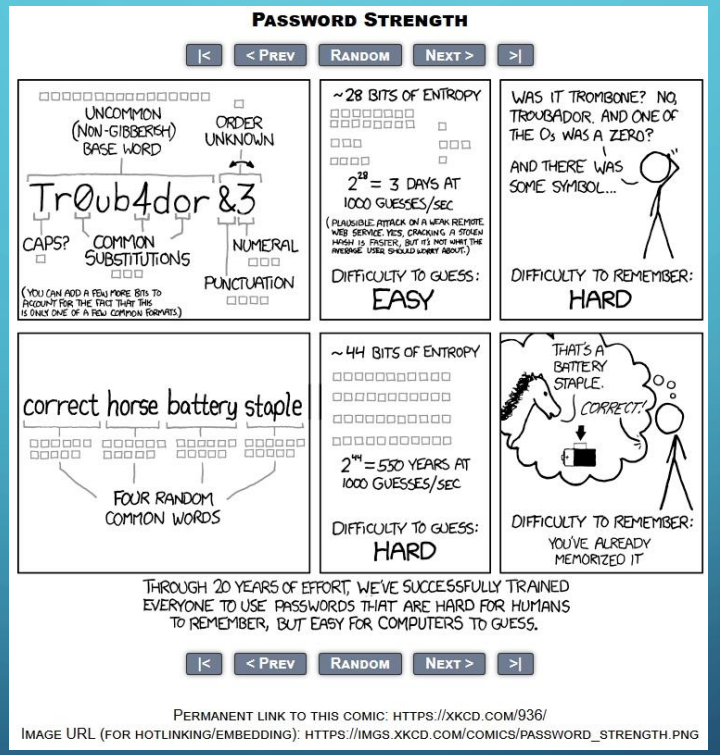
- Business Email Compromise
- Spear Phishing/Vishing
- Whaling
- Social Engineering

CURRENT TRENDS (CONT.)

- Ransomware/Scareware
- Extortion/Sextortion
- Fileless Attacks
- Cloud Computing
- Knowledge Based Authentication

VISHING – VOICE SOLICITATION

PASSWORDS


Password Strength
|< < Prev Random Next > >|
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.
|< < Prev Random Next > >|
PERMANENT LINK TO THIS COMIC: HTTPS://XKCD.COM/936/
IMAGE URL (FOR HOTLINKING/EMBEDDING): HTTPS://IMGS.XKCD.COM/COMICS/PASSWORD_STRENGTH.PNG

PASSWORDS (CONT.)

- Password Length is Key
- Use Password Phrases
- No personal information
- Change passwords regularly or after a breach
- Use a password manager

PASSWORDS (CONT.)

- **1. 123456** (Unchanged)
- **2. password** (Unchanged)
- **3. 123456789** (Up 3)
- **4. 12345678** (Down 1)
- **5. 12345** (Unchanged)
- **6. 111111** (New)
- **7. 1234567** (Up 1)
- **8. sunshine** (New)
- **9. qwerty** (Down 5)
- **10. iloveyou** (Unchanged)

- Spring2019
- MeToo2019
- j8Te9wm!
- Favorite Team
- Current Sport Season
- Spouse, Children, Pets
- Birthdate, Address, Wedding

INSIDER THREATS

- Financial
- Travel
- Foreign Contacts
- Drug or Alcohol abuse
- Recruited – Volunteer - Clueless
- Unauthorized downloads
- Taking assets home
- Elevated privileges
- Hours of work / Vacation
- Enticement for access

OPEN SOURCE INTELLIGENCE

- Search Engines
- Social Media Sites
- Blogs, Forums, Discussion Boards
- People Investigations
- Image Search
- Place of Employment
- Legal/News Reports
- Web Analysis
- Video Sites
- Geospatial Activation
- War Driving

IT CONTROLS

- Access Management
- Integrity of Data
- Secure Configurations
- Application Defenses
- Elevated Privileges
- Failure to Plan for Disruption
- Failure to review audit logs
- Wireless Access Controls

REPUTATIONAL RISKS

- Small Business
- Educational/Healthcare
- Search Results/Data Science
- General Data Protection Regulation
  - GDPR, EU
- Retail Fraud
- Supply Chain
- US Weapon Systems
- Regulation Complexity
- Unmet Board Expectations
- Outdated Business Processes
- Search Engine Optimization (SEO) Poison
  - Blacklisting
  - Redirects
  - Untrusted Sites

THE "SO WHAT"

- Employee Education
- Team Collaboration
- Backup/Restoration
- Cost of Security
- Client Data
- Encryption
- Impact to Business
- Human Factor
- Policies and Procedures
- Risk Mitigation Review
- Insurance

THANK YOU