Pure IT CUSO
AXFI
CyberSecurity Track
Session 1: Password Palooza

Steve Koinm
VP Professional Services

PURE IT CREDIT UNION SERVICES

Steve Koinm

Vice President – Professional Services

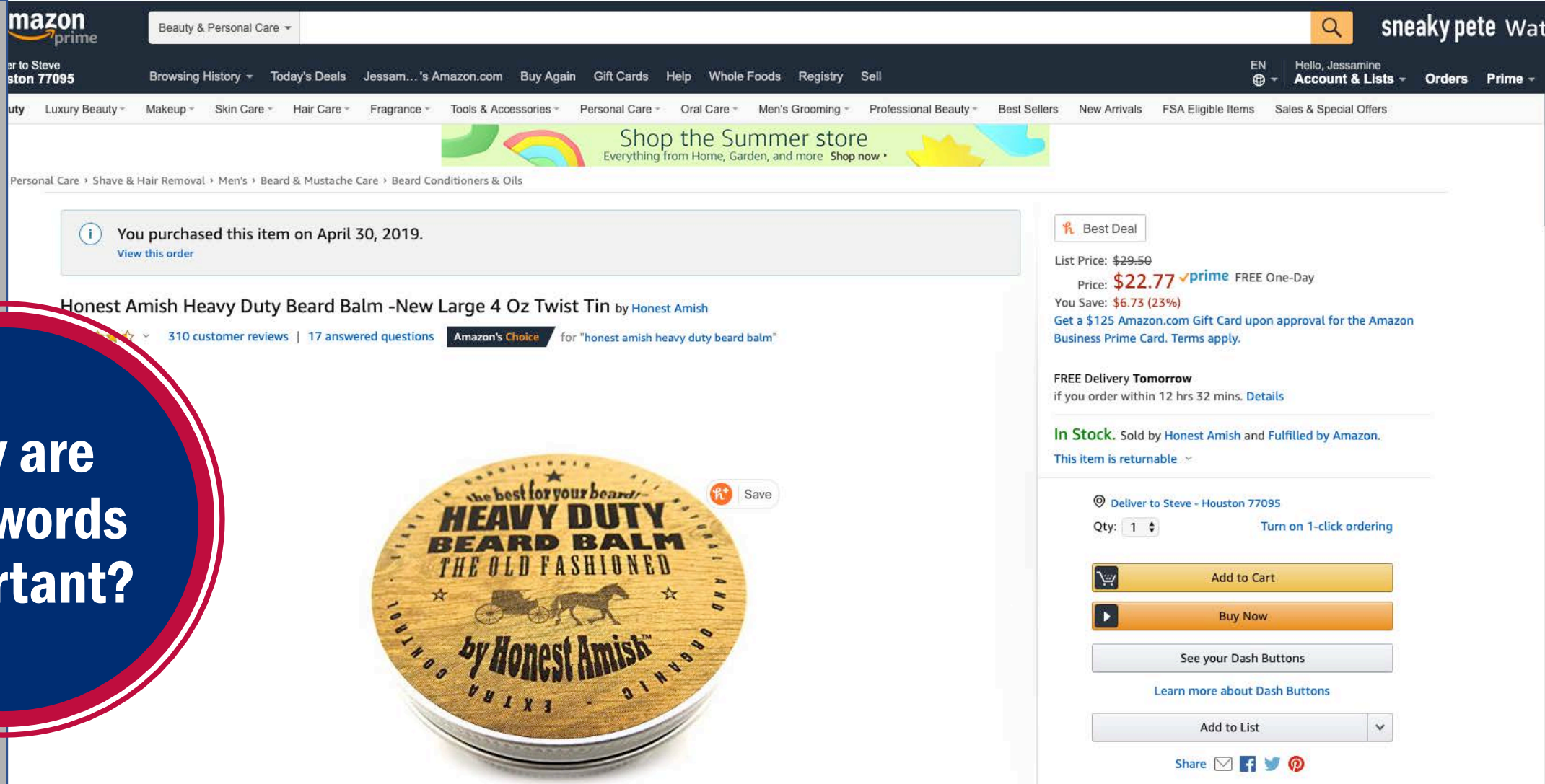
At Pure IT, Steve partners with credit union to assess IT Infrastructure and Operations. He identifies opportunities to improve the efficiency, sustainability, and business focus using technology. He works with all areas of credit unions including, executives, operations, finance, and IT support. Steve also provides analysis and roadmaps for business resilience and business continuity. He engages with credit union management to strategize around financial spend and best practices for the institution. Steve functions as the CIO, CTO, and CISO for several credit unions and CUSOs.

Steve has had a successful career in IT as an Enterprise Architect designing and teaching IT Architecture for large systems in Telecom, Healthcare, and Oil and Gas companies. After some time, he rose to the executive ranks, pitched an idea to VC's, received $20MM in funding and created a successful Managed Services and Hosting company that was sold to VeriCenter which was then purchased by Sungard.

From there, he continued Consulting, Enterprise Architecture, Systems Integration before going to Sungard building out the reference architecture for the business he had created before. He then worked for Oracle where he taught companies how to tap into the potential of Big Data, tracking info, trends, buying habits, etc. He also led business development at Rumscheidt Enterprises, a Digital Strategy firm, where he was an Entrepreneur that consulted with Entrepreneurs about being an Entrepreneur.

PURE IT
CREDIT UNION
SERVICES

Why are Passwords Important?



PURE IT
CREDIT UNION SERVICES

Why are Passwords Important?

- To protect your information
- To protect the company's info
- It is not always about you

PURE IT
CREDIT UNION SERVICES

The Bane of Complex Passwords

- Composition Rules
- Change every XX days
- Cannot use previous # passwords

PURE IT
CREDIT UNION SERVICES

How did we get here?

- NIST SP 800-63
  - First released in June of 2004
  - Update 1.0.2 in Apr 2006
  - Not updated again until 2011
  - Now under active refresh and comments
- Levels of Authentication for Access
- “Empirical and Anecdotal data suggests that users will choose easy to guess passwords when the system allows them to.”
- Provided an example of minimum required entropy in Appendix A.

PURE IT
CREDIT UNION SERVICES

Composition Rules Example

- 8 Characters from alphabet of 94 characters
- 1 upper case, 1 lower case, 1 number, and one symbol
- Dictionary of common passwords to disallow
- Will give an entropy of 30 which met the minimum for Level 2 access (10 bit)
- Change password so that the attacker will have to start guessing again every # days

PURE IT CREDIT UNION SERVICES

Composition Rules Fallout

- We then create rules that are hard for a human to remember
- Causes humans to write the password down
- Standard substitutions:
  - $=s @=a 3=e 0=o 1=i
- Frequent changes cause re-use of passwords
- Non-reuse causes sequencing of passwords
- Typically capitalize just the First letter
- Thought that folks would be sitting and trying to guess and enter in a password. Turns out we steal hashed passwords or credential stuff
- Easy for computers to calculate

PURE IT
CREDIT UNION SERVICES

Easy to Compute

- Passwords are stored in a hashed format
- Lossy mathematical formula
- Cannot be reversed, must be recalculated
- Uses a salt or hashing key
- Transmitted in hashed format
- In most cases today, many combinations to store and search efficiently…today (Rainbow Table)
- How to get the hashes
  - On Network
  - Ntds.dit file
  - Wireless
  - SMB External

PURE IT
CREDIT UNION SERVICES

Effect of Moore's Law

- How fast are computers today?
- Typical home PC with 8 core 2.8Ghz processor can run 588,000 hashes/second on the CPU
- Cryptocurrency's influence on hash calculations
- MacBook Pro's onboard Intel graphics does 8.6 Billion hashes/second
- The nVidia GeForce 1080ti card released in Q1 2017 can do 32 Billion hashes per second. Retail price $600
- The nVidia GeForce 2080ti card released in Sept 2018 can do 64 Billion hashes per second. Retail price $1,400

PURE IT
CREDIT UNION SERVICES

How Long to Crack a Password

PURE IT
CREDIT UNION SERVICES

How Long to Crack a Password

- How many combinations of 7 character passwords?
- 94^7 = 64 trillion combinations
- 64 e^12 / 64 e^9 = 1000 seconds or 16 minutes on the 2080ti
- 64 e^12 / 8.6 e^9 = 124 minutes on Macbook Pro

PURE IT CREDIT UNION SERVICES

How Long to Crack a Password

- How many combinations of 8 character passwords?
- 94^8 = 6 quadrillion combinations
- 6 e^15 / 8.6 e^9 = 193 hours on MacBook Pro
- 6 e^15 / 64 e^9 = 26 hours on one video card
- Server Chassis with 8 2080ti - ~$15,000
- 8 character passwords in 3.3 hours
- How many servers can I afford?

PURE IT CREDIT UNION SERVICES

How Long to Crack a Password

- How many combinations of 9 character passwords?
- 94^9 = 573 quadrillion combinations
- 573 e^15 / 64 e^9 / 8 = 310 days on one Brutalis server
- How many combinations of 10 character passwords?
- 94^10 = 53 quintillion combinations
- 53 e^18 / 64 e^9 / 8 = 80 years on one Brutalis server

PURE IT
CREDIT UNION SERVICES

How Long to Crack a Password

- Every year these numbers get cut in half due to performance improvements
- Quantum computing
- How many servers can someone really needing to crack a password afford?
- How much time does the APT actor have to crack the password?
- They won't have to try every combination, they will usually get the answer in less than half that time
- First path is to try a dictionary of all the known passwords, then run some sequences, then brute force
- We cannot adequately defend against offline attacks

PURE IT
CREDIT UNION SERVICES

What is Today's Guidance?

- If it is not user friendly, users will cheat!
- Be realistic, many more things need MFA
- Put the burden on the verifier
  - Do not ask the user to do things that do not improve security

PURE IT
CREDIT UNION SERVICES

What is Today's Guidance?

- At least 8 characters and accept up to 64
  - Hashed passwords are a fixed length so it does not matter how long they are
  - Encourage pass phrases or pass sentences
  - This is all Steve's #$@% fault!
  - Rely more on MFA
- No Composition Rules!
  - Length matters
  - Use other characters
  - Canonacalize spaces
  - Use all of Unicode – even emoji

PURE IT
CREDIT UNION SERVICES

What is Today's Guidance?

- No routine expiration
- No hints
- No Knowledge Based Authentication
- OOB (Out of Band) authenticator should not be SMS or VoIP phone
  - Physical tokens
  - Token software
  - Biometric

PURE IT
CREDIT UNION SERVICES

Practical Steps for Users

- Use a password manager
- Know 2 passwords
  - Computer
  - Password Manager
- 1Password compares with HaveIBeenPwned.com and PwnedPassword.com and alerts you

PURE IT
CREDIT UNION SERVICES

Questions and Comments