Larry Moore, CISSP CISA C-CISO

President - Information System Security Association, Capitol of Texas Chapter

July 26, 2017

GOOD PASSWORD HYGIENE

# PROTECTING YOUR PERSONAL INFORMATION

# EXECUTIVE SUMMARY, 2017

## Who's behind the breaches?

**75%** perpetrated by outsiders.

**25%** involved internal actors.

**18%** conducted by state-affiliated actors.

**3%** featured multiple parties.

**2%** involved partners.

**51%** involved organized criminal groups.

## What tactics do they use?

**62%** of breaches featured hacking.

**51%** over half of breaches included malware.

**81%** of hacking-related breaches leveraged either stolen and/or weak passwords.

**43%** were social attacks.

**14%** Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

**8%** Physical actions were present in 8% of breaches.

## Who are the victims?

**24%** of breaches affected financial organizations.

**15%** of breaches involved healthcare organizations.

**12%** Public sector entities were the third most prevalent breach victim at 12%.

**15%** Retail and Accommodation combined to account for 15% of breaches.

## What else is common?

**66%** of malware was installed via malicious email attachments.

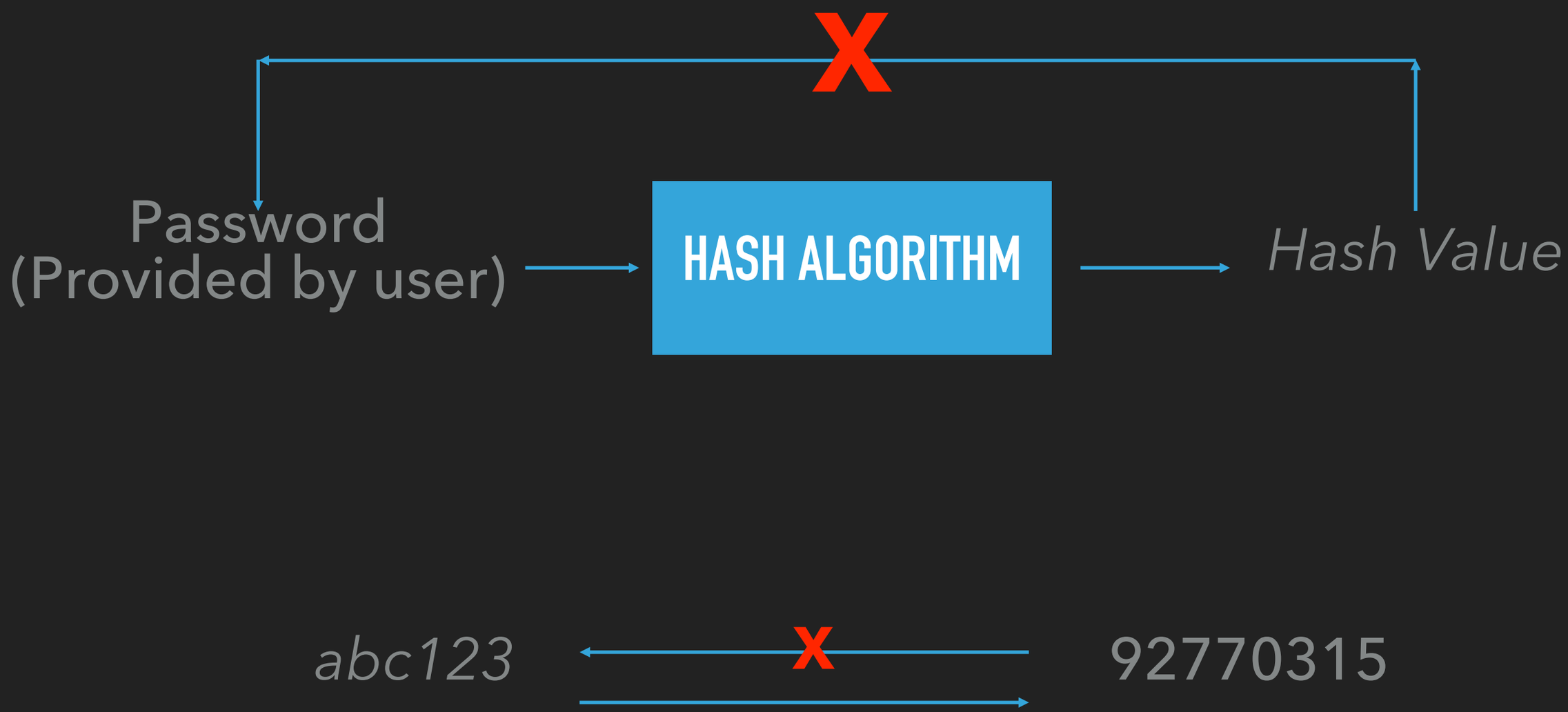
**73%** of breaches were financially motivated.

**21%** of breaches were related to espionage.

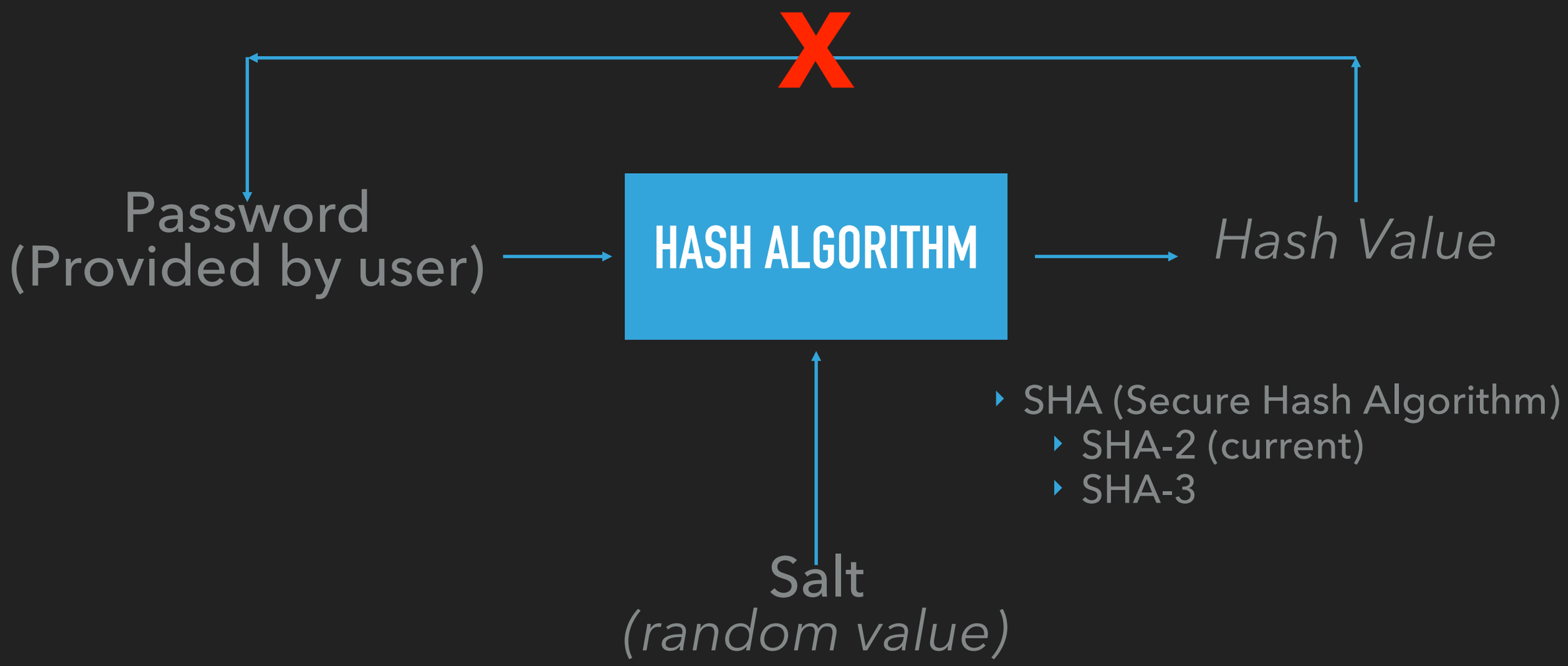
**27%** of breaches were discovered by third parties.

# PASSWORDS - SECURITY

# PASSWORDS - SECURITY



# PASSWORDS - SECURITY




Password + salt = Hash Value

- **Rainbow Table:** Contains hash values used to crack passwords.
- **Dictionary Attack**: Contains known words or groups of words.
- Social media (Facebook, Twitter, LinkedIn, etc.)
- Social engineering
- Phishing email
- Keylogger

## RECOMMENDED READING

- Matt Honan
- *Kill the Password: A String of Characters Won't Protect You*
  - *Wired,* November 15, 2012
  - https://www.wired.com/2012/11/ff-mat-honan-password-hacker/
- **Attackers access Matt's multiple accounts and through aggregation, deduced his password.**
  - Despite using strong passwords, his Apple, Twitter and Gmail passwords were linked.
- **Matt lost valuable photos of his baby daughter.**

## PASSWORD CRACKERS

- The attack is rarely performed from “aaaaa…” to “zzzzz…” but, instead, tries the most common vulnerabilities first.
  - Most common passwords. **Google “worst passwords.”**
  - Many passwords begin with capital letters.
  - They can mix numbers and letters. (L = 1, O = 0, etc.)
  - Common numerical values (e.g. “12345” “123456”, etc.)
  - Common keyboard combinations (“qwerty”.)
  - **The more guessable it is, the more likely it will be cracked.**

## STARTING OFF

- Identify and prioritize the criticality of the account.
  - Ask: “What would happen if this account is compromised?”
  - Does it contain sensitive data such as Driver’s License, SSN, etc.?
- **Create unique passwords, one for each account.**

- Attack Vectors
  - Financial motivator
    - Theft
    - Command-and-Control
  - Your personal brand; pretending to be you.
  - Other people’s data.

- Top accounts at risk:
  - Debit cards (NOT protected)
  - Medical records
  - Credit/finance records

# PASSWORDS - HIGH LEVEL VIEW

Randomness
Length
More characters
Multiple sources

Multi-Factor Authentication, One-time passwords

Long passwords with all printable characters, completely random

Long passwords with multiple words plus numbers and symbols

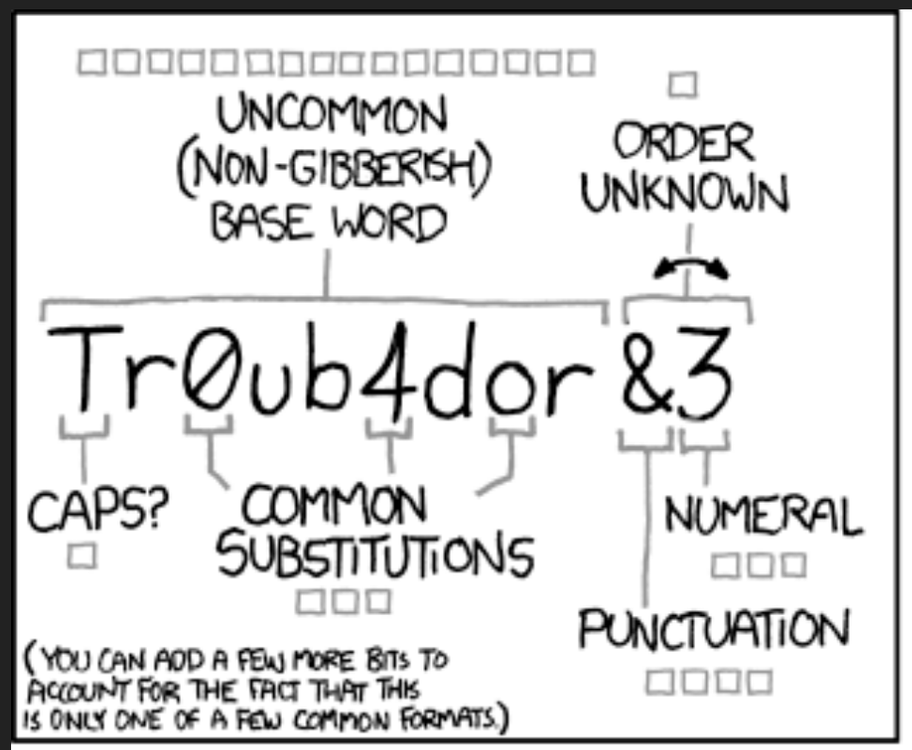
? Biometrics ?

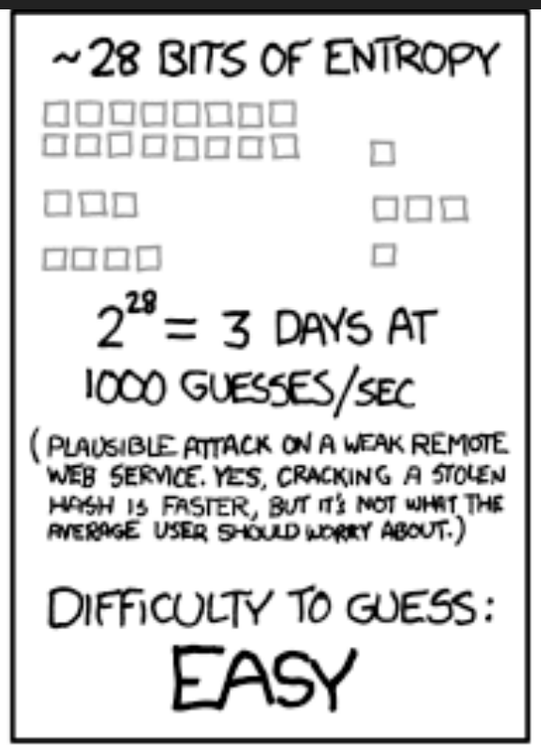
Timeouts and lockouts

Long passwords with multiple words

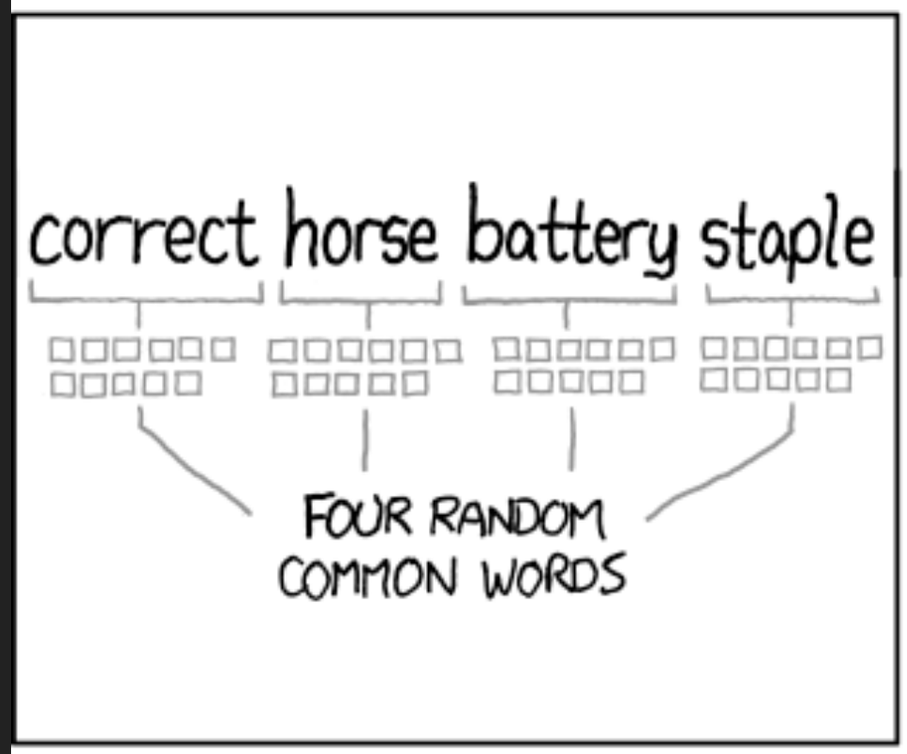
Short passwords

Passcodes (4 digit numeric value)

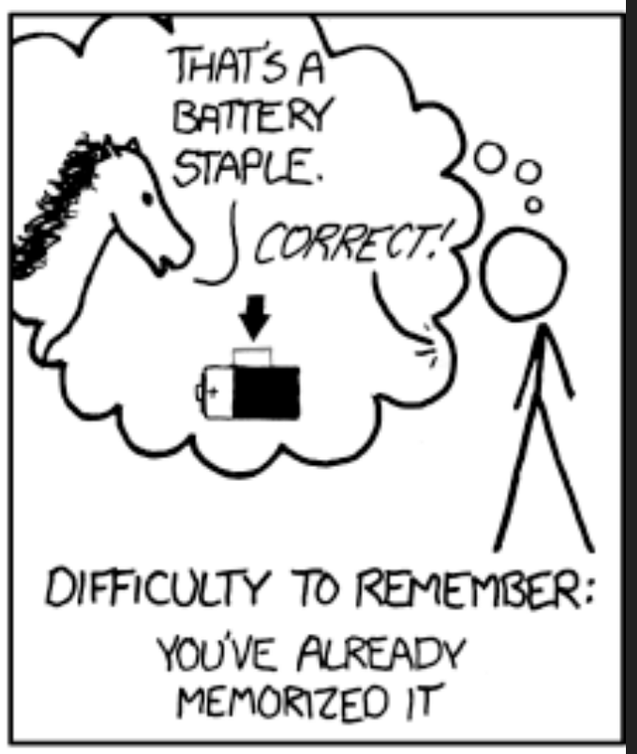











THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com/936/

## LENGTH VS. COMPLEXITY

- **“correct horse battery staple”**
  - Dictionary words - Pattern exists
  - Easier to remember a few patterns.  Harder to remember multiple patterns.
- **)6.-wA7s%2:-jn3#**
  - Not dictionary
  - Random
  - Appears gibberish from a human perspective
  - Harder to remember

## MEMORIZING PASSWORDS

- **Unique passwords are the best!** If one account is compromised the others remain relatively safe.
  - People generally use the same password for all accounts.
  - Increase in processing power + using familiar password words = reduced likelihood of security.
- How many passwords are you able to memorize for **all** of your accounts?
  - Sharing your password across multiple accounts = compromise of one account means others are threatened.
- People tend to words that are familiar to them (e.g. family, hobbies, sports teams, etc.)
- HOWEVER: It is useful for accessing accounts “on the fly” that do not contain critical data.

## PASSWORD ENTROPY

- **Entropy**: Lack of order or predictability.
- US Keyboard
  - 26 uppercase letters (A-Z)
  - 26 lowercase letters (a-z)
  - 10 single digits (0-9)
  - 34 special characters (%^)-~, etc.)
- **96 characters, total**

$x^y$

*x* = number of possibilities
y = number of password characters

*xqbepgvw*

$26^8 = 208,827,064,576$

*xqbepagvwq*

$26^{10} = 141,167,095, 653,376$

*m*5-(1J~0f*

$96^{10} = 6.6483 * 10^{27}$

# PATTERNS ENABLE ATTACKERS TO ACCESS ACCOUNTS

- Vowels follow consonants (and visa versa)
- Proper names begin with capital letters
  - Multiple words or multi-syllable words put together; each begins with a capital letter (e.g. “MyDogIsRex“)
- Replace ‘0,’ ‘O’ or ‘o’ and ‘1,’ ‘l’ or ‘I’
- Words beginning with ‘x’ or ‘z’ are rare
- People use proper words a lot (e.g. towns, sports teams, children, etc.)
- Mixing words with numbers (‘2’ and “two“) are common
- Words requiring the use of the left side and right side of the keyboard (e.g. “D-g-s-R-e-x” uses left hand, “M-y-o-I” uses right hand)

## CALCULATING PASSWORD ENTROPY

$\log_2(x) * y$

$x$ = number of password characters

y = number of characters

*password*

$\log_2(26) * 8 = \sim 4.7 * 8 = 37.6$ bits of entropy

*xpasswordy*

$\log_2(26) * 10 = \sim 4.7 * 10 = 47$ bits of entropy

*m*5-(1J~0f*

$\log_2(94) * 10 = \sim 6.6 * 10 = 66$ bits of entropy

## ENTROPY BIT LENGTH

- < 28 bits = very weak
- 28 - 35 bits = weak, good for “low value” accounts
- 36 - 59 bits = reasonable
- 60 - 127 bits = strong
- 128 > bits = very strong

37.6, 47 and 66

(from previous page)

## OTHER FACTORS TO CONSIDER

- Web site will inform the user of permitted password characters.
  - May not be able to employ full pool list.
- Web sites may send forgotten passwords or hints to the user's email address.
  - If password is sent as plain text = **FIND SOMEONE ELSE!**
- **Security questions such as "Mother's maiden name" increase risk.**

## SECURITY QUESTIONS

- There is no rule that requires the answers to be correct.
  - Ex:
    - *Where were you born?* **Answer:** *"The Sewer"*
    - *What is your mother's maiden name? "8 + 10"*
- Are there any words that you remember from your childhood?
- Don't lose the answers.
- Try for unique answers for each account, if possible.
  - Answers are **not** protected from a breach; they are not hashed.

## PASSWORD HAYSTACKING

- The attacker must guess **100%** of the correct password.
  - This means that the attacker must use *every* character. One missing character will mean failure.
- In a sense, it's adding needles to your password haystack.
  - Not perfect but an improvement.

- Ex:
  - *To be or not to be*
  - *(To be or not to be)* **or** */(To be or not to be)/*
  - *http://www.exampleabcd.com*: ***e****To be or not to be****d***

## PASSWORD STRENGTH

- Learn how to enter accents on your phone.
  - How will you enter it on your desktop?
  - Not all sites support these characters.

## PASSWORD MANAGERS

- The Good
  - Promotes strong passwords.
  - Great for multiple devices.
  - Some managers allow you to share your passwords with others securely.
- The Bad
  - Single point of failure.
  - Passwords may not be accessible if there is no Internet connection.

# LASTPASS

- Free for desktops, $12/year for mobile devices.
- Stores your passwords in the cloud encrypted.
  - Encryption key generated locally.
    - Lastpass cannot access your passwords.
- Supports Multi-Factor authentication.
- Notes for each account are also encrypted.  Perfect location for storing security questions.

# KEEPASS

- Free
- Stores passwords locally encrypted (offline).
- But…
  - Storing locally means you cannot share passwords with multiple devices dynamically.
  - If you lose your encrypted file then you lost everything.

# IRONKEY

- Secure, hardware encrypted flash drive.
- Option for secure web browser.
- Flash drive is permanently destroyed if too many incorrect passwords are entered.
- Secure, local backups are available.
- But…
  - Device is small and can get lost.

# VERACRYPT

- Formerly known as *TrueCrypt*.
- Container encryption.  Creates an encrypted file that serves as a virtual drive.
- Possible to create “hidden” containers.
- Supports some Multi-Factor authentication.

# HANDWRITTEN NOTEBOOKS

- Not a good idea in all cases.
- Offline and free.
- Extremely secure against remote attacks.
- BUT:  write carefully and store it in a safe place.

# Password Card

| | |
|---|---|
| !97Kb#32qn | IunV91ayDD |
| 88bVp;+]lp | F&@19-6asb |
| ~O@-k4n;ss | I1OOol$aZ; |
| qxi@2AKW_} | -_[+=\|dfQZ |
| O}#skv49Sn | +==lE81Mcc |

# Password Card

| | |
|---|---|
| !97Kb#32qn | IunV91ayDD |
| 88bVp;+]lp | F&@19-6asb |
| l1O0ol | I1O0ol |
| qxi@2AKW_} | -_[+=\|dfQZ |
| O}#skv49Sn | +==lE81Mcc |

Helvetica

Courier

# MULTI-FACTOR AUTHENTICATION

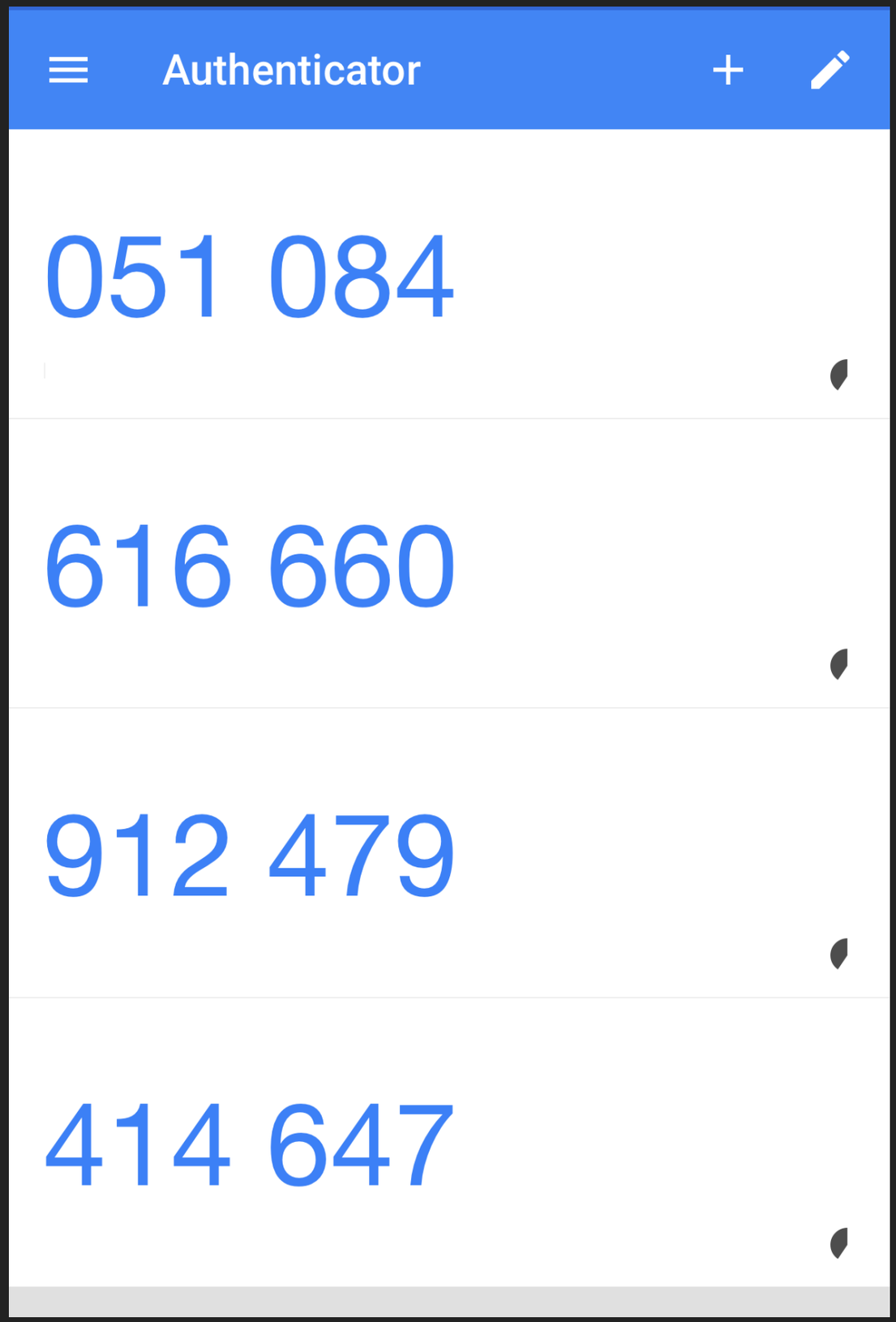
- Two or more, at least one from each category:
  - Something you know
    - passwords
  - Something you have
    - tokens
  - Something you are
    - biometrics

Starfleet Single-factor Voice Print Identification

Apparently, 24th century security experts have yet to learn about the 20th century technology known as digital sampling.

# MULTI-FACTOR: GOOGLE AUTHENTICATOR

- Must be supported by application.
- One-time passwords.  Values change every 30 seconds.
- Create one authenticator per account.
- Print QR Code on paper as backup.  Otherwise, must reinstall.



# MULTI-FACTOR: YUBIKEY

- Token
- USB connection.
- Press the “y” to authenticate.
- https://yubico.com

# MULTI-FACTOR: GENERIC FLASH DRIVE

- Create text file containing VERY large number of random values.
  - Save that file as read-only (e.g. PDF) to prevent accidental modification.

# SMS MESSAGES

- In general, not a good idea but better than nothing.
- Attackers have successfully accessed SMS messages.
- Sent in-the-clear.
- You cannot spoof your phone.
  - **SUDO**:  App that creates phone numbers and email addresses on demand.
    - Free, up to 9 accounts.

## PASSWORD ALTERNATIVES

- Fingerprint scanners
  - Fingerprints are stored as a hashed value.
  - Cold or wet hands tend to cause rejections.
  - Doesn’t work with gloves.
  - Biometric authentication can be bypassed; BUT requires skill, tools and resources.
- Face recognition
  - Camera scans and identifies face.
  - Sunglasses, hat, shadows or other objects may cause rejection.
  - Camera use drains battery.
- Tokens

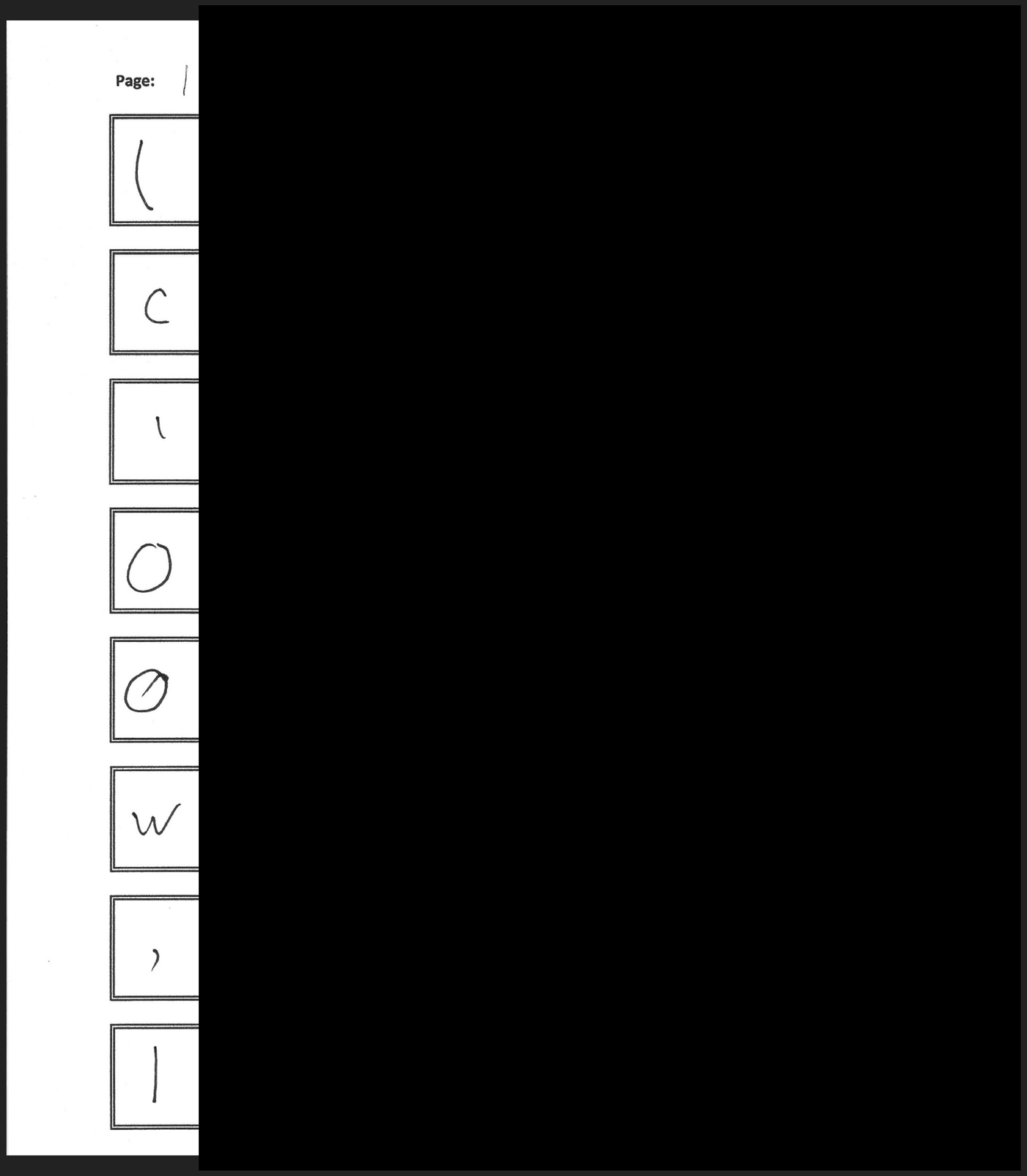
# WI-FI PASSWORD MANAGEMENT

attwifi

attwifi

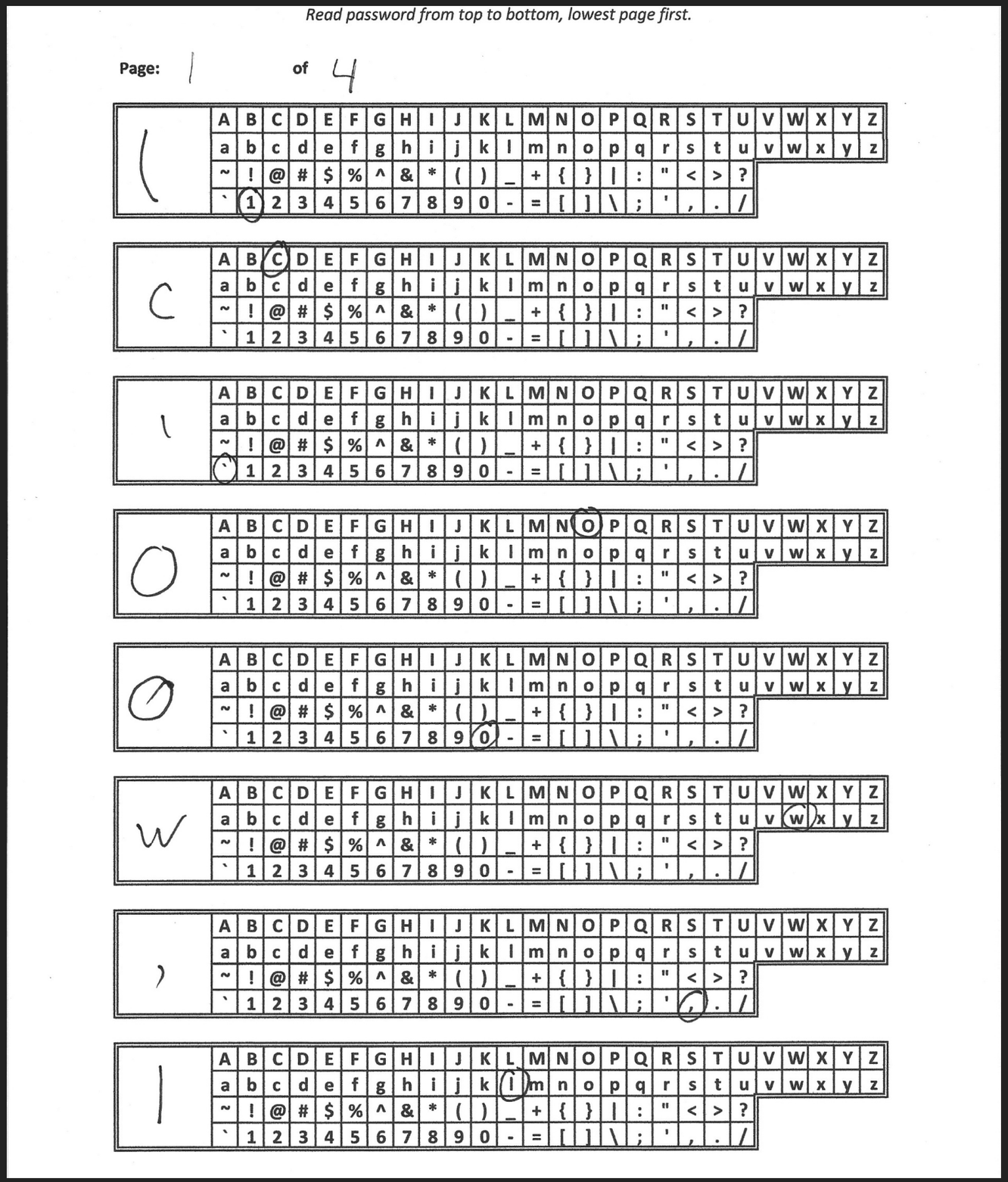
- Attackers steal passwords by way of spoofing valid public WI-FI accounts.
- The SSID (Service Set Identifier) is the **only** means of identifying a WI-FI access point.
- Be **very** careful when logging in to a public WI-FI if you are asked for your password.
- Change your password if you entered it for a wi-fi account.

Guess this password:



# SECURING PASSWORDS IN BUSINESS

- A grid, like the one on the right, minimizes password guessing when the password is needed the most.
- Created from an Excel spreadsheet.
- Can contain any number of passwords.



*Read password from top to bottom, lowest page first.*

**Page:** 1 **of** 4

| | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| l | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| W | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

| | 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 |
| | ~ | ! | @ | # | $ | % | ^ | & | * | ( | ) | _ | + | { | } | \| | : | " | < | > | ? | | | | | |
| | ` | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | = | [ | ] | \ | ; | ' | , | . | / | | | | | |

## WRAP UP

- **Create unique passwords for *each* account.**
  - Understand password requirements for each account.
  - Take advantage of all supported characters to increase entropy.
- Prioritize your accounts and set passwords according to each account.
- Encrypt your laptop hard drive.
- Note security questions.  Avoid anything that can be referenced.
- Experiment with the “Lost Password?” option.
- Avoid using email addresses for user names, if possible.

## WRAP UP

- When in public places…
  - REMEMBER:  EVERYONE has access to the same public WI-FI.
  - Make sure to use *https://…*
  - Don’t display your passwords for others to read.
- Learning Multi-Factor Authentication:
  - Create a “dummy” account and experiment.
  - Learn how to use it properly.
- Trace examples on how to recover your lost password (remember Matt Honan).
  - Create non-public accounts.

## WRAP UP

- For new accounts…
  - Use general password for account creation then *immediately* change to unique, strong password.
  - Avoid using your email, if possible.  Create unique user name.
- Note your URL.  Look for *https://…*, padlock or other identifier and CHECK IT!  Bookmark it.
- **AVOID clicking links on email.**

- Implement lockouts and timeouts, if possible.
  - Know how to recover.
- Keep the number of your cell carrier handy.
- Implement data erasures, if possible.
  - Don't forget backups.
- Consider alternative authentication methods.
- NIST 800-63 Suite: *Digital Identity Guidelines*
- REMEMBER: **You** decide what is a good password.

# LARRY MOORE

LARRY.MOORE.CISSP@GMAIL.COM
LINKEDIN.COM/IN/LAWRENCEMOORE

HTTPS://WWW.AUSTINISSA.ORG
(CHECK OUT OUR CALENDAR)