Protecting your Dolphin Data (and yourself!) from Hackers and other Threats

Steve McEvoy

March 1st, 2018

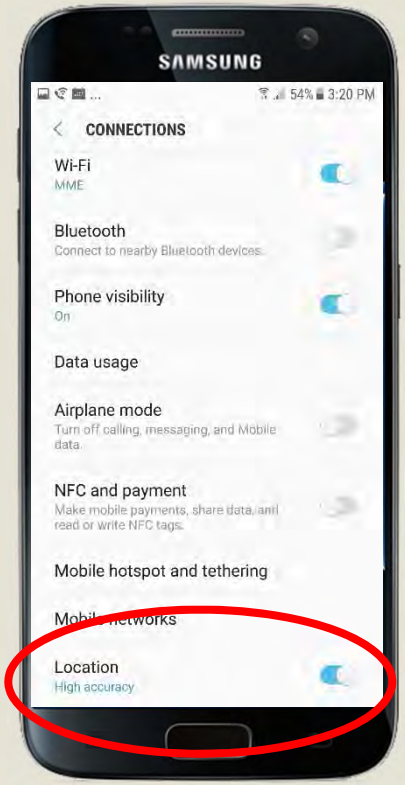
Las Vegas, NV

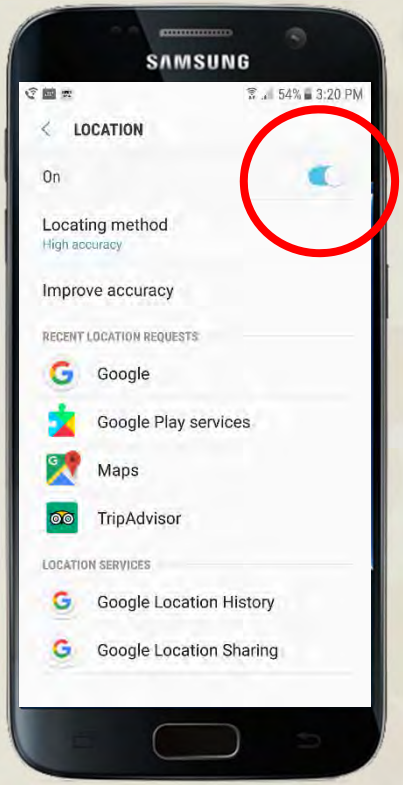
What do you think Google knows about You?

- www.google.com/history

Location Services

- Feature that your SmartPhone prompted you about when you got it.
- Used to provide information back to apps to better serve you
  - Yelp, Trip Advisor, etc.
- Can be turned off
  - Android OS
  - Apple OS
  - Google Account





Tracking Tips

- Keep your Gmail Password Private
- Make your Gmail Password Hard
- Do you Care?
  - Not really? Then enjoy the features!
  - Yes? Consider turning off Location Services on your phone or adjusting Google settings.

They still track you down…

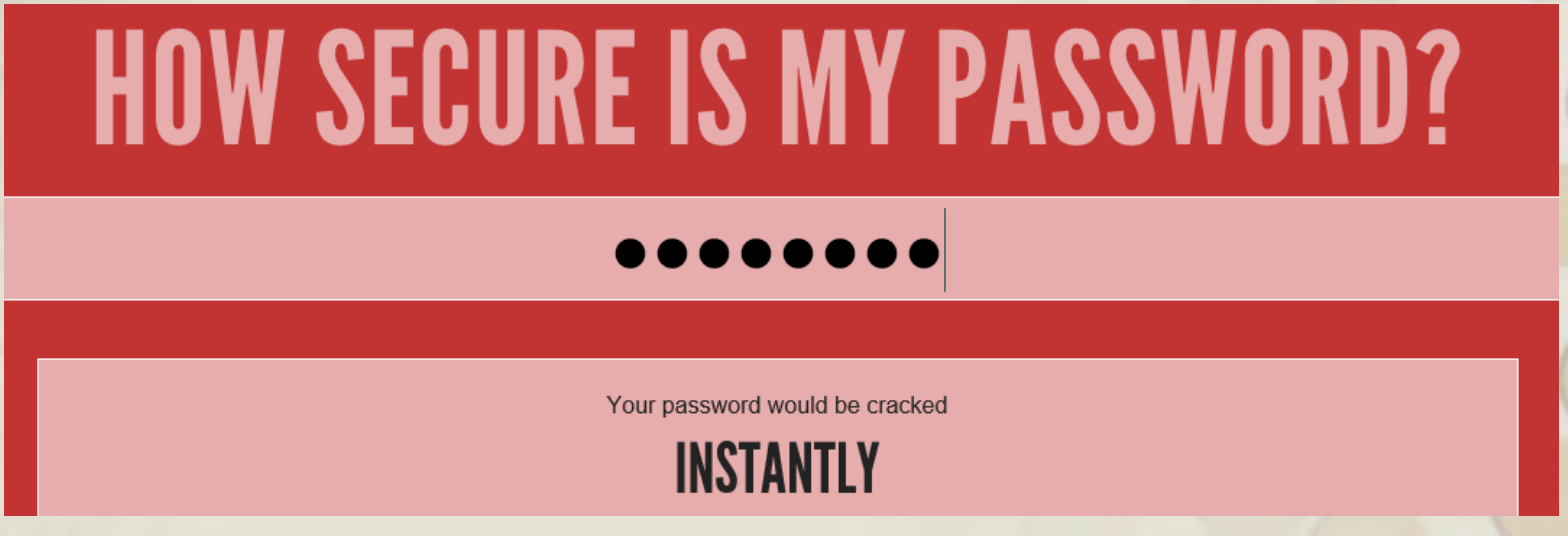
- Turning off Location Services just stops the easy way to know where you are

- They can still track you by various means
  - Device ID (MAC address or IMEI number)
  - WiFi zone location
  - DNS queries you make
  - Search Terms
  - And more….


YAHOO!
Dropbox
Experian™
Adobe
COMCAST
LinkedIn
Bell
MME CONSULTING
© mme consulting inc

How do you know if your passwords have been leaked into the wild?

www.howsecureismypassword.net



Caution!

- You don’t really know who is behind the website
- Perhaps they are recording the passwords you try
- Don’t put in your current or future passwords unless you know the risk

Username too!

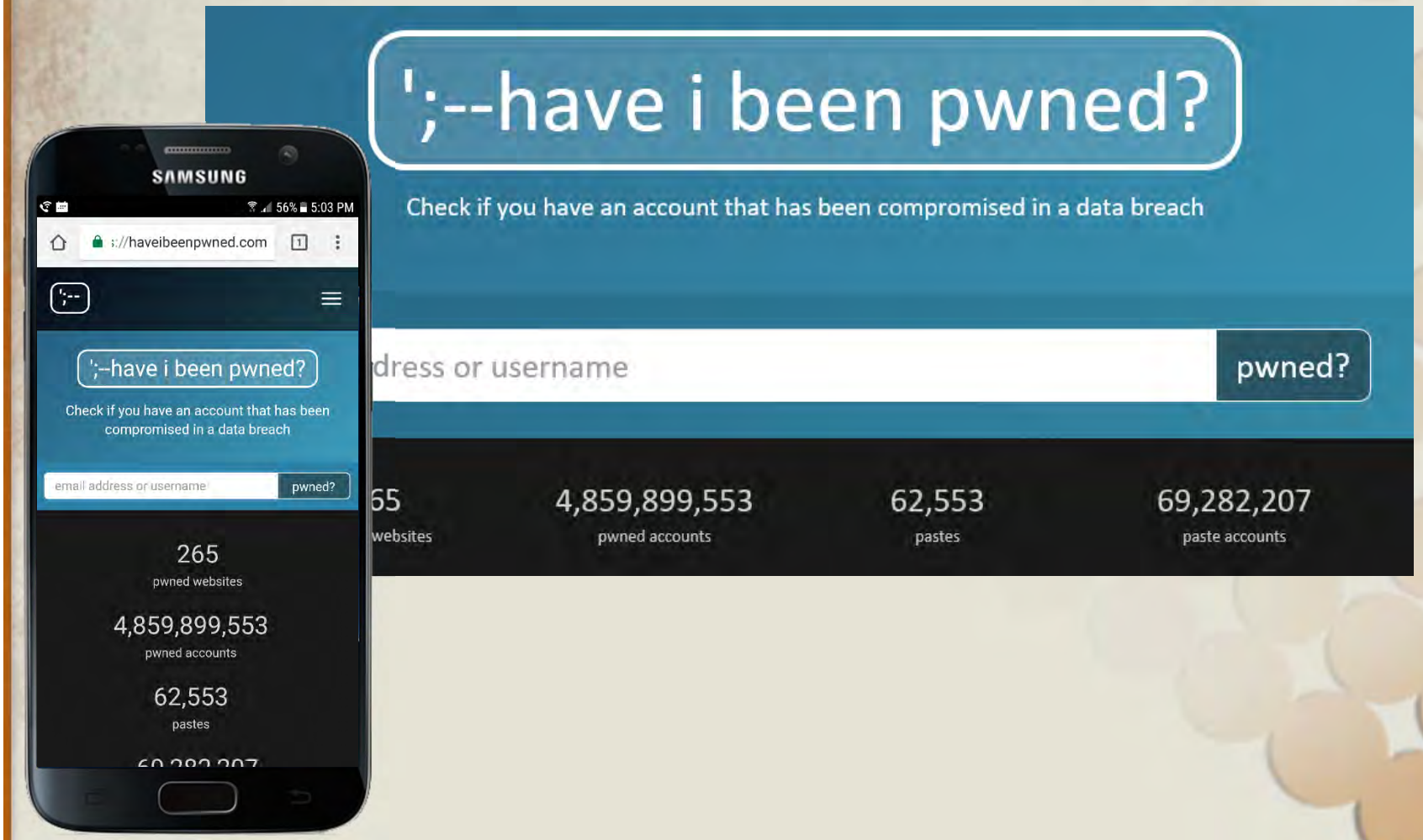
- Not only your password was stolen, but your Username was too.
- If you use the same username (likely an email) on multiple sites, AND, you have a bad habit of using the same password, they have a wide open door

Troy Hunt

- Security Expert from Microsoft
- Searched the Dark Web
- Compiled a list of 5 ~Billion hacked accounts

- Created "Have I been pwned?" website
  - 'Pwned' is a slang term
- Securely check if your username and passwords has been stolen

www.HaveIBeenPwned.com



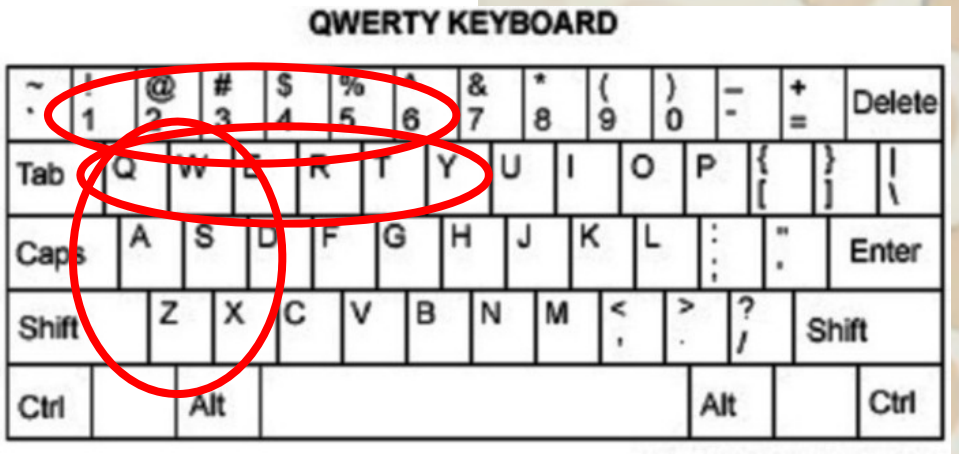
Subtle Difference

- Hacking peoples accounts one at a time is a slow, resource intensive process
- Hacking the websites full of usernames and passwords yields bulk results
- They never targeted you personally, but the result is they have the information
- The difficulty of your personal Password never mattered

What makes a Good Password?

B

1 - **123456** (ranking unchanged since 2016 list)
2 - **password** (ranking unchanged)
3 - **12345678** (up 1)
4 - **qwerty** (up 2)
5 - **12345** (down 2)
6 - **123456789** (new)
7 - **letmein** (new)
8 - **1234567** (Unchanged)
9 - **football** (down 4)
10 - **iloveyou** (new)
11 - **admin** (up 4)
12 - **welcome** (unchanged)
13 - **monkey** (new)
14 - **login** (down 3)
15 - **abc123** (down 1)
16 - **starwars** (new)
17 - **123123** (new)
18 - **dragon** (up 1)
19 - **passw0rd** (down 1)
20 - **master** (up 1)
21 - **hello** (new)
22 - **freedom** (new)
23 - **whatever** (new)
24 - **qazwsx** (new)
25 - **trustno1** (new)



What Makes a Good Password?

- Generation Zero (back in the 80's and 90's)

BLANK

- Then what changed?

What Makes a Good Password?

- Generation 1 (early 2000's)
  - a non-dictionary word with at least 1 case change, a number and at least 7 characters

Cowboy9

- Stopped the obvious 'guesser'
- Then what changed?

What Makes a Good Password?

- Generation 2 (late 2000's through today)
  - Same as Gen 1, but now add Special Characters

Sj7$qq#56

- Stopped the automated attack (?)
- Really hard to remember, so staff rebel
- Now what has changed?

Vast Computing Power

- Complexity doesn't matter to a Computer
  - $ s S (they are all just a character like a b c)
  - It just pounds through all the possibilities

National Institute of Standards and Technology

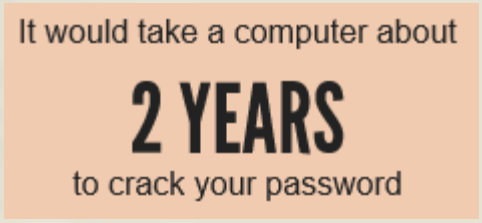
- Recently updated their recommended digital identity standard (SP 800-63)

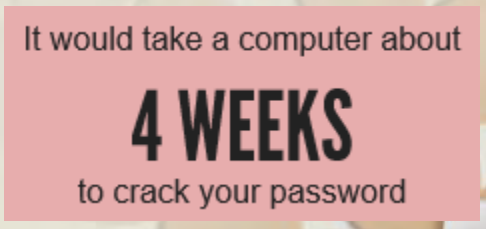
- Troy Hunt canvased NIST and others to derive what the collective wisdom is thinking

Next Gen Boils Down To…

- Length better than complexity
- 3 or 4 small dictionary words is fine
- Unassociated, but memorable
- 12+ characters

- reddogheadcow is better than Sj7$qq#56





Nothing Personal!

- 3 or 4 RANDOM UNASSOCIATED words
- Not:
  - Just 2 longer words
  - Your kids, spouse, pets names
  - Your favorite movies, foods, songs, etc.
  - Years you were married, born, graduated, etc.
  - No personal demographic info
  - Not the Practices Marketing Slogan
- Use some imagination!

Standards Don’t Change Overnight

- They ‘Evolve’
- Websites, banks, etc. will need to learn and adopt these standards
- reddogheadcow wouldn’t meet their current ‘complexity checker’

What Makes a Good Password?

- Generation 3 (2018 and on)
  - Three or Four unassociated dictionary words
  - At LEAST 12 characters in length
  - Capitalize First Letters
  - Add a 2 digit year to the end (reminder)

- RedDogHeadCow18
  - 609 Million Years to Hack
  - Much easier to remember

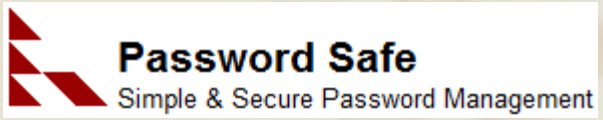
Password Best Practices

- Don’t use the same password everywhere
  - Limits your pain if one is compromised
  - A generic hard password might be OK in some circumstances
- Don’t save them in your web browser
- Don’t leave them written on Post-it notes all over the place

A Safe Place for Passwords

Password Storage Apps

- Password Safe
- KeePass
- … many others
- Benefits
  - Can generate your passwords
  - Stores them
  - Can link you back to the login page
  - Encrypted
  - Some available through the Cloud



Two Factor Authentication

Two Factor Authentication

- Where the website sends you a separate text when you login with a random code you have to enter
- Thwarts the hackers that even have your username and password
- Gmail, LogMeIn, Banking websites

- Turn it on EVERYWHERE you can!

Stop by to Visit

Thank You!

Presentation online at
www.mmeconsulting.com/Presentations

steve@mmeconsulting.com

MME CONSULTING
MMEconsulting.com

Technology Planning and Integration for Dental Specialists