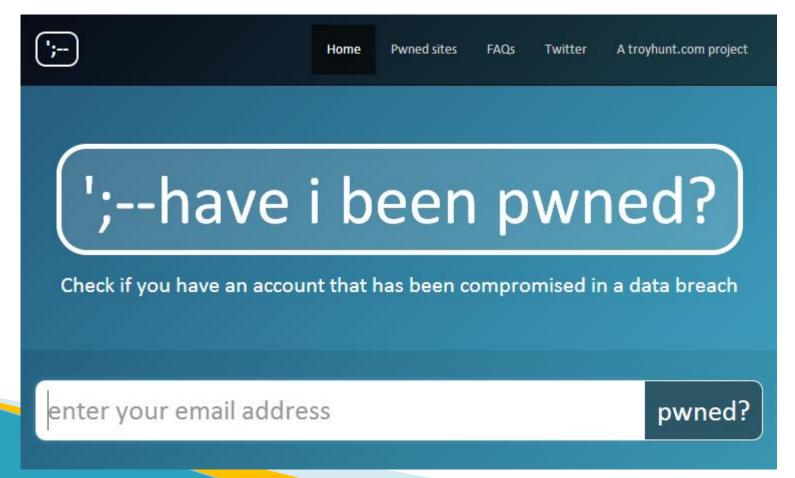
How to be safe in the Age of Big Brother and Big Data

Nilesh Trivedi Virginia Department of Education

Check if you have an email account that has been compromised in a data breach

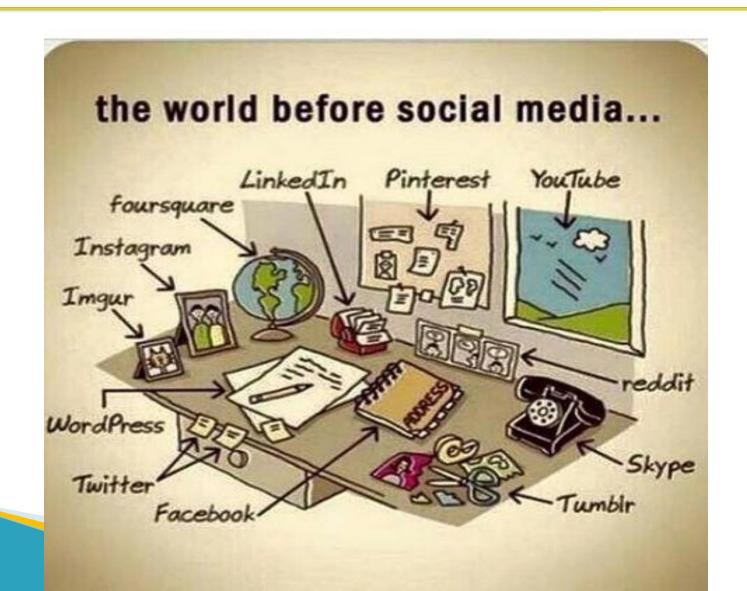
https://haveibeenpwned.com/



Whether your privacy is compromised?

Search your name on Google Such as "Brian Jones Glen Allen VA"

The world before social media



If the Titanic Sank Today



Agenda

- ➤ Your Password can be cracked!
- ➤ Managing your passwords
- ➤ Cellphones and text messages
- ➤ Browsing web anonymously
- ➤ Block annoying ads and confuse online profilers
- ➤ Safe WiFi Behavior
- ➤ Department of Human Resources and Management (DHRM) website URL highjacking demo (*if time permits*)

Password can be cracked...





Setting up answer to security questions or password hints.

Sarah Palin's Yahoo email account required her birth date, zip code and answer to the security question: "Where did you meet your husband?"

- > Your mother's maiden name?
- > What's your favorite color?
- What's your father's hometown ?
- > Where were you born?
- What's your ideal vacation spot ?

Honest Answers to security questions builds your online profile

Setting up answer to security questions

- You may be penalized for setting up answers to security questions honestly. In case of data breach, your security question setup may be compromised.
 - > Your mother's maiden name? Bestname
 - > What's your favorite color? Bestcolor
 - What's your father's hometown? Besthometown
 - > Where were you born ? Bestborn



"Your security question will be 'which programmer deserves a huge raise?' and the answer is my name."

Weak Passwords

- CEO of Sony Entertainment, Michael Lynton used "sonyml3" as his domain account password!
- ➤ In July 2015, Ashley Madison hack compromised 11 million accounts and it was posted online. The most common were "123456", "12345", "password", "DEFAULT", "123456789", "qwerty", "12345678", "abc123"
- > Name and birth year such as alexander75, Charles86
- ➤ Easy to guess such as Al3xand3r@75

Solution to weak password

- Use strong password.
- > Use random characters.
- > Can not be guessed.
- Do not keep the same password for different accounts.
- Check password strength at

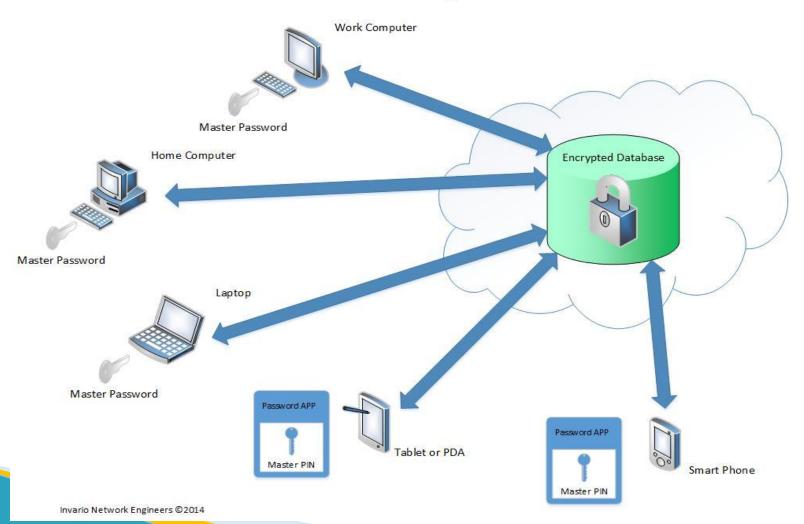
https://howsecureismypassword.net/

How to remember passwords?



Use Password Manager to remember all passwords

How a Password Manager Works



Security Concerns with Password Manager



How does one master password protect all of my accounts?

- Master Password is not stored anywhere in cloud.
- Zero Knowledge Protocol
- > Two factor authentication

Open Source Password Managers





KeePass

Commercial Password Managers

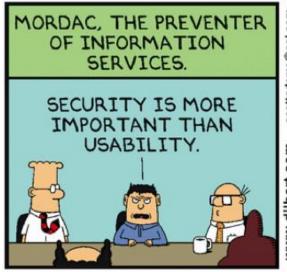
- Keeper
- Blur
- Sticky Password
- Password Boss
- LastPass
- Dashlane
- EnPass
- LogmeOnce
- RoboForm

Two Factor Authentication (2FA)

- ATM : Bank issued card (something you have) and a PIN (something you know)
- Password + Finger Print + Text Message (MFA)
- Password + Text Message
- Password + Google Authenticator
- Turn 2FA wherever possible.



"Now we need to pass the face recognition test, answer the three secret questions, and complete the sing along verification."







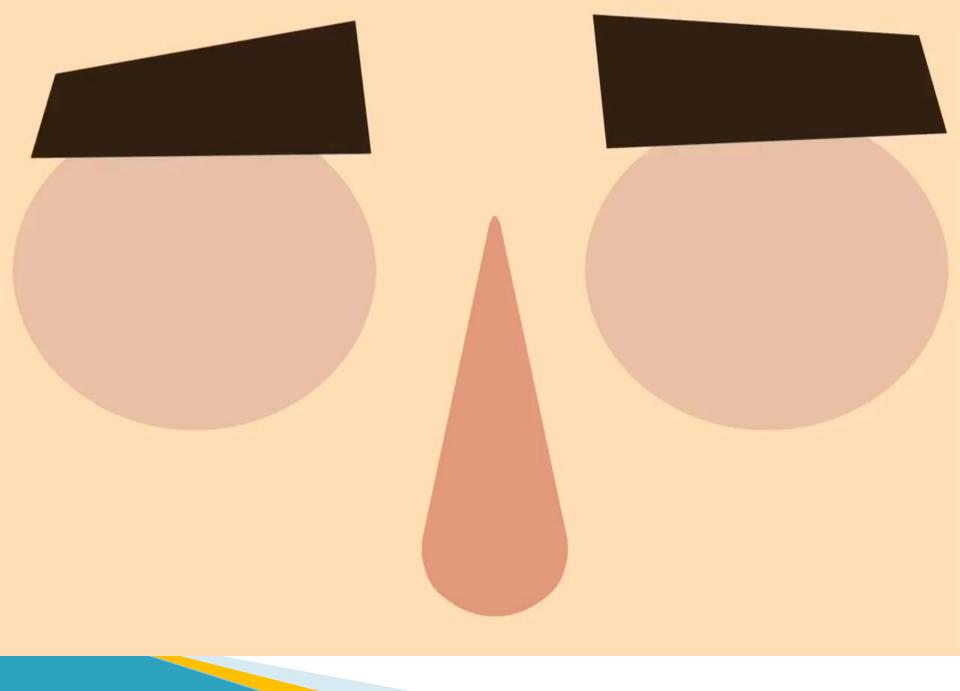
Remove your information from Google Search

Delete Me

https://joindeleteme.com

Email

- Gmail, Yahoo, Microsoft is reading your email and mining the information.
- If you want your message 100% unreadable by mail provider, lock the message with the encryption.
- Use the mailvelope plug in
- Anonymous Remailer



Cellphones

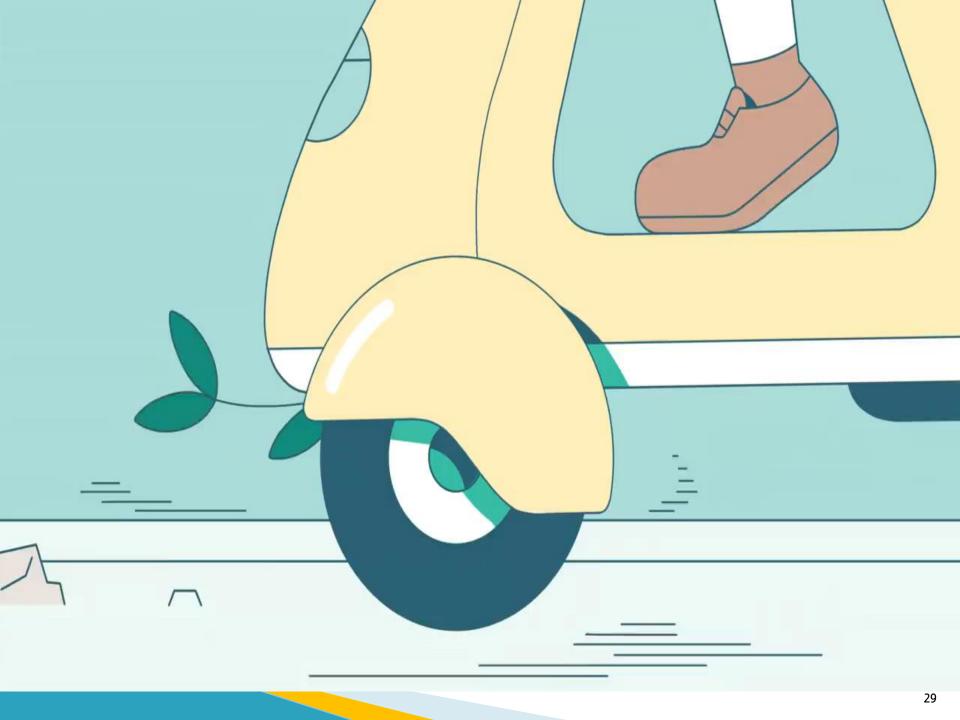
- 3G and 4G networks uses Signaling System 7 (SS 7) as an underlying protocol.
- SS7 handles the process of call-establishment, billing, routing and information-exchange functions.
- If one can tap in to SS7, one can manipulate the call.

Text Messages

- Don't use the native text messaging service that goes through your wireless carrier.
- Native mobile text is sent unencrypted, in the clear, to a Short Message Service Center, part of the mobile network designed to store, forward and deliver the text messages.
- Check for data at rest policy
- Skype will retain your information as long as is necessary to (1) fulfill any of the purpose as defined in article 2 of this Privacy Policy or comply with applicable legislation, regulatory requests and relevant order from competent courts.

Text Message – 3 Flavors

- No encryption at all
- Encryption but not end to end meaning that the communication can be intercepted by third parties such as the service provider which has knowledge of the encryption keys
- Those that provide encryption from end to end meaning that the communication can't be read by third parties because the keys are stored on the individual devices.



End to End Encryptions



Signal



WhatsApp



Telegram



Silent Phone

Now you see me.. Now you don't

Is your browser safe against tracking?

https://panopticlick.eff.org/

How perfectly am I being tracked geographically?

http://benwerd.com/lab/geo.php

Search History

- Deleting browser history on desktop, laptop or moble device. A copy of your search history remains in cloud.
- In Boston Marathon bombing investigations federal agents interrogated a couple for searching "Pressure Cooker" and "backpack".

Search Securely

- Search in Incognito Mode
- Turn off personalized ad tracking
- Use startpage.com or duckduckgo.com for search

Someone is watching your browsing activity

A simple search of "Back pain" on webmd.com builds an URL as follows:

https://www.webmd.com/search/search_results/defau
lt.aspx?query=back+pain

- My Browser
- My ISP
- My Cellular Carrier
- Canvas Fingerprinting
- And, back pain related ads starts showing up.

Block ads and confuse online profilers

- Ad Block Plus plug-in to block ads
- Facebook privacy list for Ad Block plus
- Create multiple email accounts dilutes the privacy impact of having one identifiable address.
- Do not link your social media account to other accounts.
- Use commercial VPN

Wifi

Free is not always FREE

https://www.youtube.com/watch?v=EMqEqJ7TEEw

Trustworthy Website - Really?

DHRM Website Demo

Questions?