Around 30,000 websites are hacked each day

Approximate 3.2 billion people use the internet and about 1.7 billion of them are Asians

The majority of internet traffic is not generated by humans but by bots and malware

Twitter has 250 million users

500 million tweets are sent every day

First cell phone call in 1973

24 hrs of video viewing time made each minute on youtube.

90% of text messages are read within three minutes of being delivered

Of the 60 billion emails that are sent on a daily basis 97% are considered spam

If Facebook were a country it would be the third largest population in the world

Sweden has the highest percentage of internet users at 75%

Attention

Tons of info!!!!!!!!!

* This is what our world is like. We are bombarded with new information all the time
* Our idea of privacy and how to protect it has not kept up with the advance of technology. In our technological era we went from computers as large as buildings to carrying them around in our pockets
* We need a new dialogue that is up to date on how we protect ourselves in the age of technology.

Need

* Corporate/ Government Invasion
  + Facebook is one of the largest source of privacy invasion
    - There are nearly 1 billion active facebook users (Source: <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>)
    - And approximately 250,000 accounts are expected to be fake
    - Everything you list as public is viewed by anyone
      * (This includes your friends, family, co workers bosses, murderers and anything else you can dream of.
      * Your friend lists can be seen by anyone, they can see who your grandmother is. A common security question is what is your grandmother's maiden name? Facebook is an easy way to find this out
      * Your profile Can also be viewed by government officials with no need of a search warrant)
      * A common process in hiring individuals involves looking at their social media profiles.
      * I was recently hired and was told that if i had a facebook profile that he would be looking at it.

\* In fact facebook proved to be a great source for information gathering by the SIC

* Social Intelligence Corporation (Database)
  + - Consists of images and all personal information you posted on any social media
    - One of Database’s services involves employment background screenings
      * According to SIC, 43% of hiring managers were dissuaded to hire someone because of what they found of their applicant through this database
    - The information in these databases are available to anyone including the government (Source: <http://www.consumerreports.org/cro/news/2014/03/how-to-beat-facebook-s-biggest-privacy-risk/index.htm>)
* NSA is another prime example of a data gathering organization
  + Conducted surveillance on millions on the communications of millions of americans since 2001
  + They intercepted phone calls and emails daily violating the privacy ensured to us by the Congress and US Constitution
  + What’s worse is that they were collaborating with the major telecommunications network AT&T to progress their efforts
  + The Electronic Frontier Foundation filed a case against NSA in 2008 to stop these privacy infringements
  + Julian Assange launched WikiLeaks in 2006
  + Chelsea Manning also used wikileaks in 2010 to reveal The Iraq War logs
  + Snowden caused an uproar with his wiki leaks on NSA revealed in  2013

* Cyber crime
  + 30,00 websites are hacked every day
  + 70% of americans will experience a cyber attack in a year=
  + Identity theft occurs 3,000 times a day in the US (fib.gov)
    - Hackers don’t just target you, they go for banks, schools, employers, merchants, and doctors. This provides them a higher yield if they get in (fib.com) remember the Target hack
      * 2014 Target was hacked and as many as 110 million customers were affected. The hackers got names, addresses, phone numbers, emails, and account #s
    - 64% of websites have questionable password  policies that leave their users without protection. 51% make no effort to block entry after 10 wrong tries (keygo.me)
  + But it’s not just identity theft that occurs over the web
    - Denial of service attacks -Anonymous
    - Cyber-bullying: 1 in 3 children have been a victim (nspcc.org/uk)
    - Child- abuse- 1,500+ child abuse domains
      * 58% within the US (enough.org 2008)

Satisfaction

* Classes
  + How do computers work?
  + What are cookies and an IP address
  + What is the best/most up to date antivirus
  + Learn about spyware and malware
  + Avoiding giving information to websites when you don’t need to
    - One obvious example was when the CEO of lifelock has fallen victim to identity theft 13 times when he revealed his social security number to the world (Source:<http://www.wired.com/2010/05/lifelock-identity-theft/>)
* International Cybercrime Division
  + A cross-borders organization that can track and stop cyber crime in a way that is not possible today
  + The FBI searches for cybercrime within the country, but cannot infringe upon the rights on citizens in other counties and they must rely on the other governments to track the criminal
    - We only get knowledge of US citizen committing cybercrime IF the other countries share that information

* US Privacy Law
  + We do not have a solid, legal definition of privacy
  + The closest Right to privacy that can be found is the 3rd and 4th amendment in The Bill of Rights.
  + The 3rd amendment says that “No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.”
  + And the 4th amendment states that “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
  + These amendments show that soldiers do not have the right to stay in our homes without consent and that the government may not search our possessions without a warrant given to them because of probable cause.
  + After the bill of rights we have laws about finances and health information, but no overall policy of privacy
  + So basically there is nothing protecting individuals from the information displayed on the internet.

An example of the government overstepping privacy

* + Patriot Act
    - It stands for: Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
    - Allows the government to forego sections of the constitution, when they believe terrorists may be involved.
    - It was hastily passed 45 days after 9-11 to prevent other terrorist attacks. It allows easy access to phone conversations, emails, and text messages.
    - Do terrorist have a right to privacy?
  + Apple vs FBI
  + Do corporations have a stronger duty to their customers or governments?
  + In December and man and his wife went to his work place and shot several people.
  + After his death, the FBI wanted to use his phone to find more information about who he was talking to and meeting
  + THey went to Apple, assuming they had a “skeleton key” and wanted them to use it
  + Apple not only does not have a

Visualization

* Access to resources like the classes will raise awareness to the issue
* If people are aware of the dangers then they will begin to care. When they care, they begin to act.
* Establishing a cyber crime division would allow us to feel more secure from threats online like harmful virus and also help prevent identity theft.
  + Keep your bank account, credit cards, your social security number, and other information secure and in encrypted servers
* Having socially responisble companies that care more for their customer’s privacy good or bad
* An example of this is apple not having a decryption key

Call to Action!

* Educate yourself! FBI.gov has TONS of information on cybercrime
* Look at privacy settings on social media, check browser settings and determine which websites are allowed to gather cookies)
* Ask your government what they are doing to prevent international cyber crime
* Change the way you see the internet as not just what is scrolling through your news feed but also how the internet is used
* These are strange conversations but they are conversations to be had.