IDENTITY THEFT

I. INTRO

1. Thank everyone for coming out tonight

2. I hope by the time you leave here tonight, I will have been able to share some important information that you may have not know about when you came in here.

3. We know who we are, and friends and family know who we are, but to the rest of the world that doesn’t know you, you are what’s on paper, like your birth certificate, or SSN.

4. Before the age of convenience, people had to wait until they actually had physical money in their possession to pay for goods and services.

5. Today in the digital age you can walk into a store and swipe a little plastic card, or even better, you can order goods online from the comfort of your home with that same card number, plus the 3 digit security code on the back, that really isn’t secure once you have to give it out.

6. This convenience is only possible because of your well established credibility with banks and lenders. This is what criminals are after, your credibility, whether to use it for themselves or to sell it to the highest bidder on the black market.

7. To a thief, a credit card number is good, but it has to be sold or used quickly before a customer knows about it and cancels the card.

8. Your identity on the other hand is a gold mine, because If they can impersonate you by stealing your identity, they can not only make purchases, but also open new lines of credit, activate utility services, or even open a car loan in your name.

9. The thief is betting that you don’t monitor your accounts in hopes they have more time to have some fun with someone else’s money.

10. By the time you notice the fraudulent activity, your credibility is already affected, and can take many frustrating months to repair the damage.
II. DATA BREACH

A. Data Breaches in the News

1. If you've seen any of the news in the past few months, you'll be aware of a growing epidemic of major companies and retail stores being hit with Data Breaches, some in upwards of 200 Million accounts of customers or employees data being stolen in a single attack.

2. A survey of data breaches in the first six months of this year shows an alarming number of incidents in which data, including names, addresses, credit cards, Social Security numbers and medical records were lost to criminals or exposed.

3. Last year's Target breach left 110 million shoppers credit card numbers exposed on the internet for sale.
   a) Just a few months ago, Home depot was hit and 56 Million customer card numbers were also exposed.
   b) That means if you shopped their in the last 6 months, you should have already contacted your bank and gotten that card number replaced.

4. Lot's of these breaches are from hackers or cyber criminals, but they can also be internal within the company.
   a) As one example that Home Depot learned the hard way, is that they didn't perform a proper background check on it's security employees.
   b) Their Senior Architect of IT Security who was hired in 2012, while working for his previous employer, took their security systems offline for a month when he found out he was being fired. How's that for revenge on your boss?

5. Employees at Home Depot frequently requested extra training and resources to keep customers data safe, but their managers always gave the same response: "We sell hammers."
   a) How confident does that make you feel leaving your account information on the servers of every place you've ever shopped?

6. In the battle to keep your personal information private, it's not just hackers you have to worry about, but lax security and human error.
   a) In some cases, there is nothing more than a simple password on the security employees computer protecting customer and employee data.
   b) As one recent example of this, the huge JP Morgan Chase breach of 76 Million customers data, which included names, addresses, phone numbers and e-mail was the result of a compromised employee password. Ouch!
7. It’s not just retail stores getting hit either. Banks, Insurance Services, Government & Military, Healthcare, Universities, Nonprofits like the Red Cross, and even just recently the United States Post Office have had some sort of security hack or breach of data.

8. The companies you see here are just a few of the more well known brands that have had their data breached in the last few years:

Twitter Facebook Sony eBay Target Home Depot JP Morgan Chase Evernote UPS Adobe Skype LinkedIn Google

B. Data Breaches / POS vs Online

1. Point of Sale
   a) This type of breach often involves hackers installing malware known as “Backoff” which targets retailers POS systems, basically the checkout terminal, letting hackers remotely steal credit and debit card data.

   b) This malware has been used against more than 1000 U.S. retailers so far. It is mostly limited to the information stored on your card, such as the card number, full name, expiration date, and the PIN you entered if a debit card was used.

   c) Unfortunately for you, a lot of retailers are still using older more vulnerable software and hardware for their sale terminals.

2. Online
   a) When you sign up for goods and services online, you enter in a lot of personal information such as your name, address, credit card number, and you also have to create a username and password.

   b) All this information is stored on companies’ servers which are the target for online criminals.

   c) Much more personal information can be stolen online because you submit more data online than you do at a retail store.

   d) If you use that same password for other online accounts, than you’re at greater risk of having those other accounts not related to the breach being compromised.

C. Data Breach Stats

1. Nearly 1 in 3 data breach victims also become a victim of identity theft in the same year.

2. Homeland Security reports that more than 800 Million people worldwide have had their private information stolen just in the past year.

3. 51 Days: The average amount of time criminal is misusing a customers information

4. 17 Days: The average amount of time it takes to stop the crime from occurring after it has been detected.

5. In 2013 39% of customers who had their credit or debit card breached suffered identity theft
6. Top 3 reasons for a data breach
   a) Malicious or criminal attack
   b) Human error
   c) System glitch

III. HACKING

A. What happens after a Data Breach?

1. Depending on what kind of data was stolen, criminals will need to phish for the rest of the information from you.
   a) They will often try to disguise themselves as the company that had its data breached, informing you that they need to verify your account information and assure you that they are keeping your data safe.
   b) Here are a couple of examples
      (1) Call you, asking you to personal verify your information (very persuasive!)
      (2) Email you, asking you to click on a link to verify your account info (usually looks urgent!)
      (3) Some criminals are great graphic designers, making the email look almost identical to the one the real company sends out, including the companies logo.
         (a) Look for misspelled words or wrong company info.
         (b) One great example of this is the Facebook notification email. In the early days of Facebook when it was only available via the web, they would send you an email notification for just about anything, and you could click the link to take you right to the post.
         (c) Hackers got really good at making a very convincing looking email, and would blast it out to thousands of random email accounts to see if they could bait anyone.
      (4) They may even pose as a debt collection agency trying to guilt you into paying them over the phone. So make sure you know exactly who you owe money to.

2. Major companies have stated that they will never call or email you asking you to verify personal info that they already have on file.

3. A large percentage of people don’t take the necessary steps after their accounts have been exposed, and few even sign up for the free year of credit monitoring that the breached company offers it’s customers.

B. Malware / Viruses

1. Once you click on a link in a phony email, you can be redirected to a fake website that disguises itself as the legitimate one.
a) Hackers only need to make a single convincing page of the website, and make every clickable area a trap.

2. This then gives the hacker access to uploaded malicious software on your computer without you even knowing it.

3. One such malware is called a Key Logger, which will send back to the hacker what you actually have typed on your keyboard (including your password, credit card number, etc.)

a) Here the major information hackers are looking for:
   (1) Your real name
   (2) Birthdate
   (3) Social Security Number
   (4) Home address
   (5) Phone number
   (6) Email address
   (7) User names and passwords
   (8) Security questions and answers (your mother’s maiden name)

C. HeartBleed

1. (Maybe ask by a show of hands who knows what HTTPS (or green lock) is and if they have heard of HeartBleed)

2. Is a security bug discovered in April of this year

3. SSL (Secure Socket Layer)

4. HTTPS encrypts data on that page

IV. IDENTITY THEFT

A. Old Paper Days vs High Tech

1. Paper
   a) Digging through trash
   
   b) Stealing credit card offers out of the mail
      (1) Opt out of pre-screened offers (Later)

   c) One person at a time

2. High Tech
   a) Stealing your data from companies rather than individuals

   b) Millions of people at once

   c) Much more efficient for the criminal
B. Most Common Types of Identity Theft

1. Driver's license
   a) This may be the easiest form of ID theft to commit. It's also the quickest to detect, as you know very quickly when your purse or wallet gets stolen. (1) (Guy’s especially with the pocket pat)
   b) With you license in hand the thief can use it to get other forms of ID in your name. This type of ID theft spreads to others, especially criminal identity theft.

2. Social Security Number
   a) Keeping your Social Security number private is among the first items on any checklist for preventing identity theft. If an identity thief gets a victim's Social Security number, damages can be considerable.
   b) Thieves can use this information to obtain new Social Security cards (claiming the old one was "lost"), to obtain Social Security benefits you worked all of your adult life for, welfare benefits, including housing vouchers, and medical and dental care.

3. Tax Fraud
   a) A big one these days with a SSN is tax fraud.
   b) Imagine, for instance, that an identity thief files a fraudulent tax return on your behalf. If the IRS receives the fraudulent return before you file, the IRS will send your hard-earned refund check to the first person to file the return: the identity thief!

4. Medical ID Theft
   a) The deadliest form of identity theft. Medical identity theft occurs when someone uses a person’s name and/or insurance information without the person’s knowledge or consent to obtain medical services or goods, or to make false claims for medical goods or services.
   b) Medical identity theft frequently results in erroneous entries being put into the victim’s medical records, which in turn may lead to inappropriate and potentially life-threatening decisions by medical staff.

5. Character / Criminal ID Theft
   a) Many identity thieves use their victim's Social Security number to apply for driver’s licenses.
   b) If a criminal is arrested and uses a license in your name, they can create a nightmare that extends far beyond your credit score and financial reputation.
   c) Consequently, you could get pulled over by the police for a burned out tail light on your car, and end up getting arrested for some felony you know absolutely nothing about.
d) It then becomes your difficult job to try to convince the local police and court that you are really the victim and are indeed innocent of the crimes committed in your good name.

6. ID Theft of the Deceased

a) Surprisingly, these next two forms of theft are not commonly known, but can go for years without being detected.

b) Identity theft doesn’t just happen to the living.

c) Unfortunately, the deceased are highly targeted by criminals, as the death of a loved one is a life-altering event and the surviving family members probably aren’t immediately concerned with the risk of identity theft, making personal documents and sensitive information vulnerable to theft.

d) How

(1) When someone passes away, there are plenty of ways for criminals to access his or her personal information including obituaries, hospitals and even funeral homes.

(2) If the criminal is a pro, they will likely use public records at their disposal. They can find out the age and birth date of the deceased, towns they’ve lived in, family members’ names and info just from the obituary alone.

e) Effects

(1) Once a criminal has their hands on private information, most commonly they head to the bank to borrow money against their victim’s name, whether through a loan or credit cards. Relatives can go years without the slightest clue of any debt.

(2) In the same way a criminal can commit tax fraud on you or I, they can also collect refunds with a deceased person’s information.

(3) The IRS reports that false tax returns on the deceased are part of tax fraud that costs billions of dollars each year.

f) Precautions (Steps you can take)

(1) When a loved one passes away, the family should immediately start a log of all accounts, and notify everyone of the person’s death.

(2) Using an ID theft protection service to organize and secure the deceased victim’s information and financial information can help with this process.

(a) Identity theft experts recommend using services like this to monitor financial and credit accounts for up to a year after death to prevent fraud, as well as initiating a credit freeze by notifying the three major credit bureaus, Equifax, Experian, and TransUnion to flag accounts with a “deceased” status, and canceling the deceased’s driver’s license with the state’s DMV.

(3) It’s important to report the death to the Social Security Administration, as well as all financial institutions including banks, insurance companies, and credit accounts.
(a) Be very careful about obituaries, avoiding publishing anything with personal identifying information, especially their actual birth date, mother's maiden name, home address, relatives' last names, or their middle name.

7. **ID Theft of Children**

a) Kids are one of the biggest targets for identity theft.

b) A child's identity can be stolen when criminals create what is known as a "synthetic identity," a process by which crooks combine a child's Social Security number (SSN) with a different date of birth.

c) Using an actual SSN, the most crucial piece of every American's identity, confuses the credit issuers and they think it's a new person.

d) **How it's different than an adults:**
   1. Child identity theft is a crime in which criminals have specifically targeted children for personal data such as their SSN, date of birth, and name.
   2. Children are being targeted more because their info is more difficult to detect, so it's more lucrative.
   3. Criminals can steal a child's information at birth and abuse that information for up to 18 years before the child even knows they've been victimized.
   4. When an unauthorized person uses your credit card number to make unauthorized purchases, most banks will contact you the moment they suspect suspicious activity.
   5. But when an unauthorized person uses your child's name successfully to get a credit card, it is highly unlikely that anyone will contact you.
   6. As far as the bank or credit bureau is concerned, the false identity is real because thieves use a child's clean slate to establish a new credit history.

e) This can seriously effect your child’s credit history for years.
   1. As one example, a 19-year old victim had 1.5 million dollars in fraud committed against her starting when she was 9.

f) Children with the same name as the parent are frequently confused with their parents file for a several reasons:
   1. Certain information is reported and does not contain a SSN
   2. Collection agencies have been known to report debts only under a name and address

g) You can protect your child in the same you would yourself, by using a Credit Monitoring Service.
   1. Some of the monitoring services offer a discounted rate for your child when you already have an account.
V. TECHNOLOGY

A. The Art of Making Life Easier

1. There is so much information on this topic, that I would take up your entire evening, so I just going to cherry pick a few topics.

2. There are over 160 Million people using a smartphone just in the U.S. alone, and it’s growing.

3. All the things that used to be reserved for waiting until you got to your computer at home, like shopping, banking, checking your email, and even using social media, can now all be done from your smartphone.

4. There is a huge transition in the way we access our personal data now, with more information being viewed via our phones than on the web in from of a computer.

5. Smartphones have become our hub for accessing our entire digital life, with apps that let us access our bank account, social media, shopping, email, and many other personal accounts with only having to sign in once.

6. Yet less than half of smartphone owners lock their phone with a passcode or security swipe.

7. Smartphones have made life easier for us in so many ways, and we take them just about everywhere we go.

8. Underneath that glassy surface lies a device capable of transmitting lots of sensitive data, including your location.
   a) We all know that this is useful when getting driving directions, but did you know that every photo you’ve taken and posted online will have location data on it, if you didn’t turn that option off in the settings?
   b) That’s nice for your vacation photos, but what if you or your child are posting pictures they took at home and posting them online?
   c) You guested it, anyone viewing those photos can access your home address.
   d) Most companies are getting better at making privacy options more easily accessible and easier to understand
   e) Wether your a fan of Apple, Google’s Android, or Windows phones, get to know your phone and it’s privacy settings, as there are too many to go through here.

9. As I mentioned earlier, there is a huge shift in the way people are using their mobile devices much more than their home computers for surfing the web, banking, email, and of corse social media.

10. Criminals know this so they have been changing their focus more towards mobile attacks through text, email, and even downloads of fake apps.

11. Be more cautious and don’t click on any strange links in a text or email, and always download apps from the devices official store
B. NFC

1. One of the ways companies are trying to help protect its customers information from data breaches, is the advancement of NFC chips in smartphones.

2. This technology lets you pay for things at a register without having to take out your credit or debit card.

3. This technology is great, but I want to show you a quick comparison about how not all tech is created equal.

4. Let's take a look at the way 3 different companies are taking on NFC payments:
   a) Google Wallet (Android Devices)
      (1) Stores your actual card number and only secures it with a PIN code
      (2) Only available where MasterCard PayPass is excepted
      (3) Works just like the NFC chip in your credit card
      (4) Still vulnerable
   b) Apple Pay (Apple iPhone 6)
      (1) Creates a unique 16 digit card number securely on the phone
      (2) The merchant never sees you ID or card
      (3) Works with most major bans and credit cards
   c) CurrentC (Coming in 2015)
      (1) Uses QR code
      (2) Checking account only, trying to eliminate credit card fees
      (3) They store your account info, which defeats the purpose of keeping your account data anonymous and away from retailers

5. So, don't just take any technology at face value, find out what goes on behind the scenes.

6. I would like to talk more about privacy in the digital age, but I'll have to save the rest for another presentation.

7. I will give you this small piece of advice to ponder:

8. If the service is free, you are not the customer. I'm looking at you Facebook.

VI. SECURITY

A. What you can do to protect yourself?

1. Here's some of the things you can do to keep the hackers from doing digital karate on your personal info.

2. Passwords
a) Yes, we’re going to start here since I know how everyone loves trying to create and remember passwords to all the places you visit online.

b) The average person has 26 online accounts, and only an average of 5 passwords to protect them.

c) Your digital identity spans much further than it did several years ago. You’re no longer just using passwords for email, and shopping.

d) You’re using online accounts for banking, insurance, taxes, investments, social media, cloud storage and monthly bills.

e) Do you really want to be using the same password for your bank account that you use to sign in to Facebook?

f) Not the best idea.

g) So, what’s your method for creating and remembering a password?
   (1) Pets name?
   (2) Favorite sport?
   (3) Superhero?

   (4) Or do you ever feel like it’s getting tough coming up with new ones and just use the word “password”?

   (5) Then it shows up in red saying there needs to be at least one number in it, so you use “password1”, or “passw0rd”?

h) Maybe it starts to get hard to remember all those different password, so you start reusing ones from other sites?

i) That is exactly what hackers are hoping you’ll do, because then they’ll try to gain access on other sites with that same password.

j) Here’s a list of some of the most used passwords that have been exposed in data breaches over that last few years.
   (1) password
   (2) 123456
   (3) 12345678
   (4) qwerty
   (5) abc123
   (6) monkey
   (7) trustno1
   (8) baseball
   (9) 111111
   (10)iloveyou
   (11)sunshine
   (12)passw0rd
   (13)superman
   (14)football
   (15)welcome
   (16)password1
k) The first 3 passwords in this list have helped the top 3 spots for the last 4 years.

l) Many users create passwords related to the site.
   (1) In the case of Linkedin, link, work, job and career were some of the passwords exposed in their data breach.

m) Hackers can guess as many as 200 word combinations a second, with the help of software of course.

n) Most tech companies have stressed the importance of a long alphanumeric password with punctuation to increases the time it takes to crack your password.
   (1) dietcoke (instantly)
   (2) di3tcoke (11 minutes)
   (3) di3tcoke! (6 days)
   (4) ili3kedi3tcokealot! (125,000 years)
   (5) ili3kedi3tcokealot!! (2 quadrillion years) (or 1,000,000,000,000,000,000,000,000 for non nerds)

o) It’s very important to make all your passwords long, complex, and unique, and use different passwords for every site.

p) Many users still think a number sequence like 12345 trailing a phrase is secure.

q) Now, how do you keep track of them all?
   (1) A notebook at home?
      (a) Very unsecured, plus how does that help you when you want to log in from your smartphone while you’re away?

   (2) The notepad app on your computer or phone? How secure is that if someone steals it?

   (3) Emailing yourself a list of all of them?
      (a) When your email gets hacked, you’re in big trouble!

r) How about something to help you not only store all your passwords securely, but help generate unique strong passwords for every account and let you access all of them either on your computer at home, or on your smartphone?

s) These are called Password Managers

t) There are lots of password managers available, but I’m going to single one out that I found to be the best called 1Password, which I use.
   (1) Encrypted

   (2) Generates unique strong passwords

   (3) You only have to remember one password

   (4) Can be synced to your smartphone through cloud sync or WiFi

   (5) These tools take all the guess work out of trying to create and store all of the many passwords you need for all your accounts.
3. **Identity monitoring services**

   a) The next thing you shouldn’t be without is an Identity monitoring service.

   b) You can receive a free copy of your credit report once a year, but you have to contact the 3 bureau’s individually.

   c) What good is that if you find out 6 months later that someone opened a fraudulent account in your name?

   d) Americans will regularly spend money at their favorite coffee shop, or pay for subscriptions to their favorite media services like Netflix or Spotify, but not give a second though to pay for a service that monitors their identity for fraud.

   e) There are many players in this market, such as Life Lock or Identity Guard.

   f) They offer a wide range of services at different price points.

   g) You’ll want to find one that not only monitors your identity, which should include your name, SSN, addresses and public records, but also give you access to your credit report on a monthly basis, as well as notify you of any changes including when a new account is being opened.

   h) As I mentioned earlier, many of these companies offer protection for you children.

4. **Two step verification**

   a) This next one is free, and most tech companies such as Apple, Google, Microsoft, Facebook, Twitter, Yahoo, and Dropbox have already jumped on board.

   b) Two-step verification is designed to prevent anyone from accessing or using your account, even if they know your password.

   (1) It also eliminates the need for security questions.

   c) How this works is pretty simple.

   (1) It’s the same as when you go to the bank and they ask you for two forms of identification.

   (2) In this case, your second form of ID is your phone.

   (3) When you log in to an account with your password, you phone will be sent to your phone via text, which you then enter.

   (4) No code, no entry.

   (5) One very good example for using this, is if you own an iPhone and have Find My Phone enabled.

   (6) Using this feature allows you to track and wipe you phone remotely from the iCloud website when you sign in with you password.
5. Email accounts

a) Now let’s talk about email accounts.

b) Does your email inbox look like this? (Slide)

c) If you only use one address for all your incoming email, than you could be missing some important alerts from your bank or fraud protection service.

d) When your data is exposed in a breach, it could include your login credentials, which in most cases is an email and a password.

e) Just as using the same password for multiple accounts is not safe, the same is true for email accounts. The thief would have access to all the rest of your digital life just from you single email address.

f) Now I’m not suggesting you need a separate email for every account, that would be overkill.

g) The trick is to use a few email addresses and segregate your accounts bases on their categories.

h) Here’s an example of how I categorize my email accounts:
   (1) Email 1
      (a) Banking and Identity services

   (2) Email 2
      (a) PayPal (This is all by itself because the email address is visible on every transaction)

   (3) Email 3
      (a) Shopping

   (4) Email 4
      (a) Major accounts (Insurance, Bills etc)

   (5) Email 5
      (a) Social media and misc junk

   (6) Email 6
      (a) Freelance

   (7) Email 7
      (a) Friends & Family

i) Benefits to segregating you emails:
   (1) Have to do this on the fly
j) It’s also a great way to keep track of what credit or debit cards and are used at each site/merchant in the case you get news of a data breach.

k) Be careful using an email address from your cable or internet provider as your main email, especially for bank accounts.

(1) Some reasons why:
   (a) There security is questionable
   (b) They don’t offer Two step verification
   (c) Almost no options as far as categorizing your emails
   (d) The biggest reason is that as soon as you cancel your service, they close the email account and you lose access to every single email you’ve received and sent.

l) Email accounts with alias’s can help keep things organized

6. Public WiFi

   a) Public Wifi is just that, public.

   b) Why keep strangers off your home network, but be willing to use a stranger’s network to access sensitive data?

   c) Thieves can spy on the sites you visit or data you transmit including passwords from any device you use (tablet, laptop, or smartphone) while you are connected to a public WiFi.

   d) Best advice:
      (1) Set all your devices to not connect automatically to unknown networks
      (2) If you must use public WiFi, limit your activity to things that don’t require you to sign in or fill out personal information

7. Some random last minute advice

   a) Paperless statements / I received someone else’s credit card statement in the mail!

   b) Update your software!!

   c) Check out with PayPal whenever possible, as the merchant won’t store any of your personal information other than your login credentials.

   d) Check the sender of the email before clicking on any link
      (1) Ex. info@facebook.com, billing@amazon.com

   e) Don’t just give out your personal information blindly, especially you SSN.
      (1) Ask them why they need it
      (2) What they are going to do with it
(3) And how they are going to keep it secure

(4) When companies ask for your SSN, ask them if they will take your Drivers License number instead.

a) Be careful of links on websites and flashy inciting offers to click on
(1) Turn the option on in your browser that lets you see where the link will take you when you hover over it

VII. CLOSING

A. We live in an age where data can be transferred anywhere in the world in a matter of seconds. That means every piece of your personal data is already online somewhere.

B. It’s stored in more places and with more companies than you may realize or even know about.

C. People make mistakes, even those running huge fortune 500 companies.

D. There are always going to be criminals out there that would love to steal what you work hard for.

E. In the end, you can’t control where your personal data ends up, but you can be proactive and intentional about protecting yourself and your family.

Thank you all for coming out.
Questions?