Cyber and Physical Security

Background of Presenters

- Over 30 years experience in computer an cybersecurity
- Decades of experience in operations security and physical security (intelligence)
- Awarded the North American Information Systems Leadership Award (ISLA) by ISC2
- Certified Information Systems Security Professional (CISSP)
- Trained Department of Defense (DoD) in Cybersecurity
- Performed Operations Security during Cold War

What is Cybersecurity?

- Making your devices safe from tampering
- Helping YOU to prevent your devices from being used against you
- It is both offensive and defensive in nature
- This presentation will be defensive only (will not teach you to hack!)
- There are white hats, grey hats, and black hat hackers
- There are no grey hats (just used as a rationalization)
- Both grey hats and black hats have every intention of using info for their benefit
- White hats will sign a contract with you

Why Do We Need to Know This?

- The same reason that you need to know about locking your doors
- Security is something that is nice to know, but better to apply
- In most instances, if you do not take the appropriate measures to secure…
- …The insurance companies will not pay!
- As we move along in this presentation, think about how physical and cyber are the same
- There are people who want to take what belongs to you
- Your job is to make it as hard as possible for them to do so
- It is preferable that they move on to “softer” (easier) targets

Physical Security

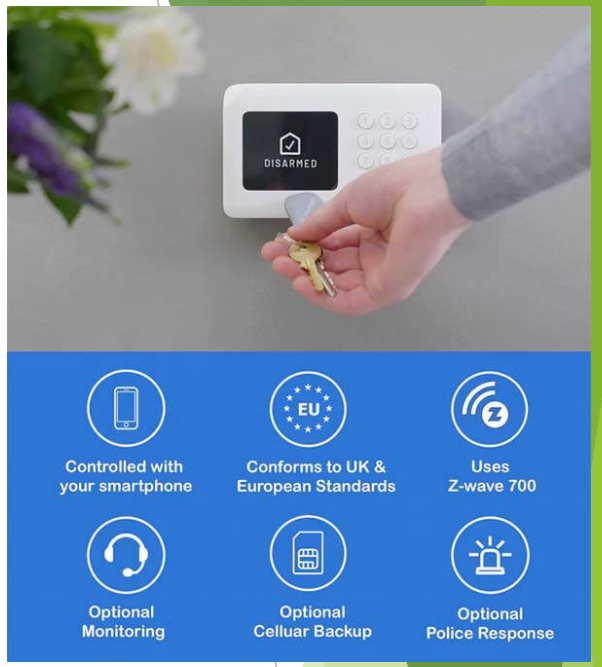
- Your home is an investment you want to protect
- Your car is an investment you want to protect
- Your family is THE THING you want to protect
- Physical security entails protecting your physical assets
- The first area of discussion will be your home
- The second area will be your car
- The third area will be your family
- The topics may combine physical and cyber security depending on the content

What Drives Criminals?

- Although many studies vary, criminals are driven by purpose
- The purpose may be to impress others, or to gain benefits from others
- In order to get results, the important thing is to not get caught
  - This means you want to get the most results from the least work
  - Simple is the keyword
- In order to be simple, it must be quick and easy
- If it is hard, the criminal will look other places
- They are not looking for a challenge, just results
- Your job is to make it hard for the criminal

Outer Perimeter

- First place to start is the outer perimeter of the property
- You want to deny the criminal access to this outer perimeter
- In many cases fencing the simplest way to deter and deny
- Fencing comes in two forms – physical and virtual
  - Physical Fencing is just that
  - Virtual Fencing is a set of webcams that cover all corners of property
- Web cams used to be expensive and hard to set-up
- They now come in a variety of forms (even solar powered!)
- They also have the option of cloud recording or local recording

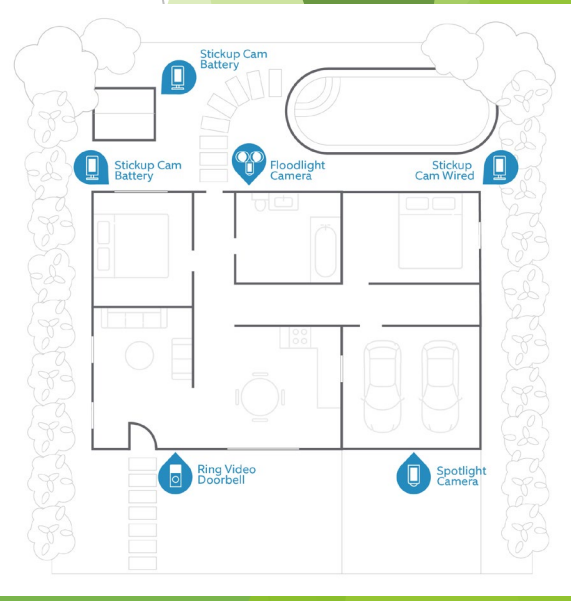


Word of Caution

- The world today is cloud-based data collection and retrieval
- Cloud-based means that a third-party collects your data
- This third-party retains the data (for a price)
- It also allows you to access your data at any time
- The cell phones have it, but so do web cams
- There is an old story about Ali Baba and the Forty Thieves
- The moral of this story is that one password or access allows for much data
- Local recording means that the recording stays within your control
- Just something to consider in any cloud-based scenario

What is the normal amount of coverage?

- This is an individual preference
- With one camera at the front of the house and one at the back of house, the coverage should be sufficient
- If you have a front doorbell camera, be wary
  - Proven hacking techniques to “pwn” (or own) your camera
  - Simple as taking the camera off the mount and reinitializing the wifi
  - The current cameras have some preventive measures (unique screws, etc.)
- The main thing to understand is that you have wifi and that can present issues
- More on that during the cyber discussion



What are the devices outside you must control?

- Your garage keypad
- Located outside, at the frame of your garage
- It has a four digit (normally) control that is easy to hack
- If the control has been there a while, the numbers are worn where they are used the most
- Someone can be on the road and video you pressing the control
- How would you control this?
  - Move the keypad (that's right! You can move the controller)
  - Move it to a place where a camera would pick up the person trying the keypad
- Basically, you want the person to try to intrude where you can record the intrusion
- https://www.deepsentinel.com/blogs/home-security/how-to-make-a-garage-door-more-secure/

What other things are outside?

- Fence gates
- Simple: Lock them when you go on vacation
- Key holders
- Again simple: attach to something they will have to work to get undone
  - Most key holder are put on doorknobs
  - They are hard to detach, but there is a hack to get them undone
- Make any attempt to enter the house a multi-faceted, multi-phased approach
- Even if the intruder beats one of your preventions, they will have others to beat
- What this means is that it will be hard to enter the house – move on!

Car Protection

- Lock your car (simple, but sometimes we forget)
- If you can, put your car in the garage
- If you cannot put it in the garage, then place it in well lit areas
- Light works the same for criminals as vampires (they both hate it)
- Car alarms do not work
- Loud car alarms are treated as a nuisance more than a deterrence
- Make sure you have the vin number copied (usually on title)
- Keep your key in a safe place and do not expose it unnecessarily
- Current tools that can clone keys from 3 feet or closer

What About Interior Protection?

- Cameras for the interior of the house are a good way of crime prevention
- Alarms are another method of ensuring protection
- Alarms can be local or cloud protection
  - Local means that you will be notified if there are any detections
  - Global means that law enforcement is called automatically
- False alarms that are given to law enforcement can be cited, so be careful
- If there are any detections, and you are local, just ensure that someone can get into the house to check or that you call law enforcement yourself
- Confirm with your camera before you do anything

Cautions about Interior Cameras

- If I told you that I had a microphone inside your home and it could hear you talking how would you feel?
- Microphones are part of the interior camera protection
- In most instances, turning the microphone off does not necessarily mean it is off
- Some companies that produce smart devices have already admitted that their microphones are on ALL THE TIME
- One of the ways to prevent this is to activate the cameras only if you are not home
- Don't believe me? https://www.usatoday.com/story/tech/columnist/2019/12/19/your-smartphone-mobile-device-may-recording-everything-you-say/4403829002/

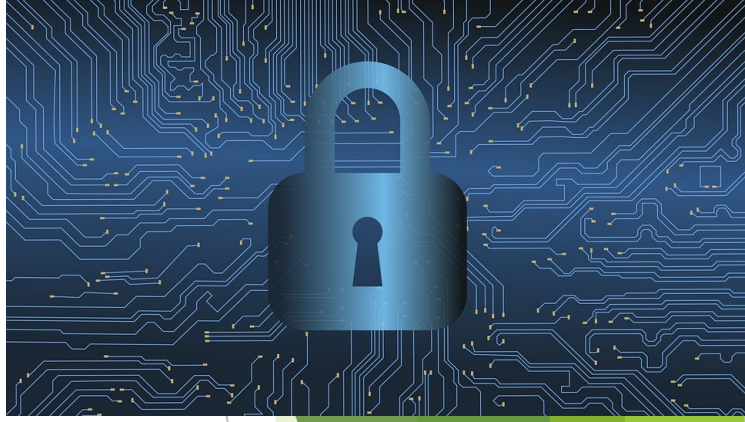
How Can you Prevent Listening?

- Turn the microphone off on your cameras
- Turn them on when you leave on vacation
- Turn the microphone off on your phones (Go through SETTINGS)
- Put devices where the intruder would not look first
  - Behind a plant
  - By a lamp or in a corner of the floor
  - Someplace the eye would not look first
- The intruder should only have about 10 seconds to look for something
- Make sure you have the detection feature so it records on detection

Now that we are inside….

- How about those smart devices?
- How many do you REALLY need?
- Are they giving you some relief, or are they just an annoyance
- There is as association between convenience and intrusions
- As convenience increases, risk also increases
- One researcher stated that “convenience and empowerment always seem a win for most people, even at some loss of privacy, control, or transparency” (https://www.pewresearch.org/internet/2017/06/06/theme-1-people-crave-connection-and-convenience-and-a-tech-linked-world-serves-both-goals-well/)
- What this means is that, the easier you THINK you make things, the more that you cannot control THOSE things

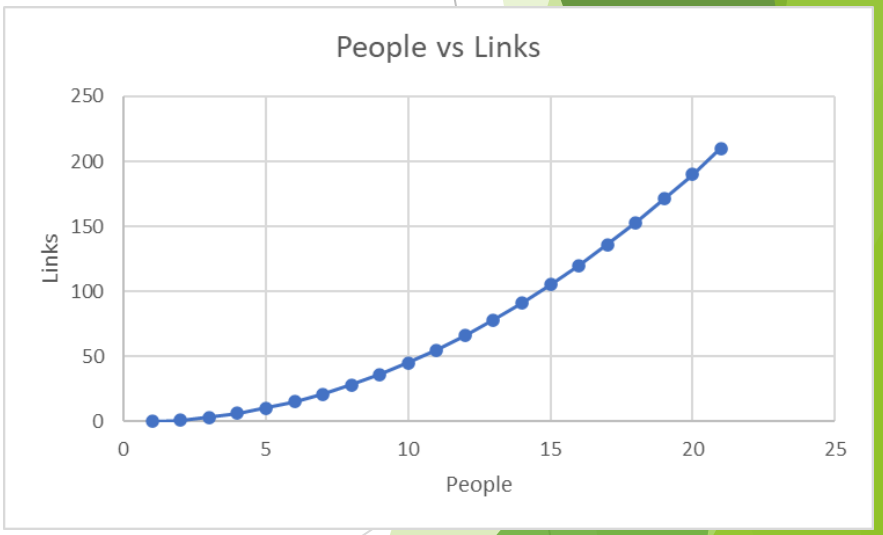
Moving to Cyber…



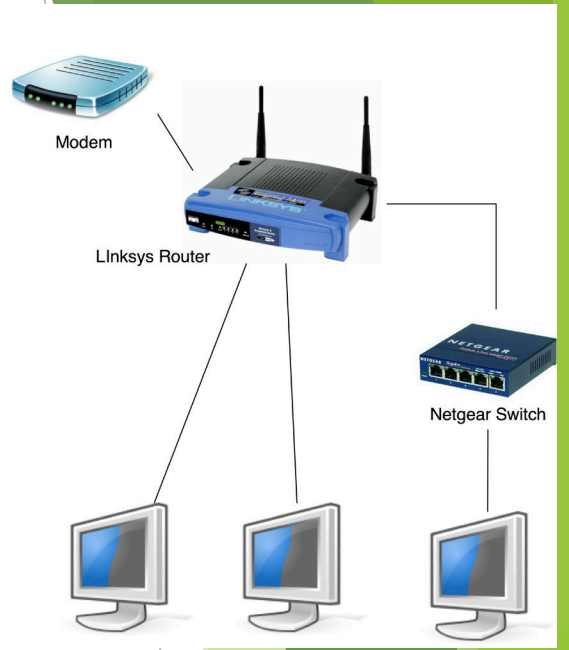
- Cybersecurity is part of the overall physical security, but is also a separate component of security
- If you do not have a router, you do not have smart devices
- If you do not have internet, you do not have smart devices
- Protecting your cyber will help protect your physical security
- With every device that you include in your network, there comes a risk
  - The risk of deceiving
  - The risk of denying
- What we will discuss here are ways to help you prevent intrusion through your network

So What?!

- The best way to understand the interaction of the internet is a formula
- n(n-1)/2 determines the number of links per number of people
- If you have two people, you have one link
- If you increase by one person, you increase the link by 2 links
- Increase by 3 people (to 5) and you increase to 10 links!
- There are over 4,000,000,000 (billion) people on the internet
- That translates to over a quintillion links (10^{18})
- Hundreds of thousands of light years!!
- That is the buffet from which the hackers go for dinner!
- Just a brief interlude to understand the extent of the threat!



The Heart of Your System

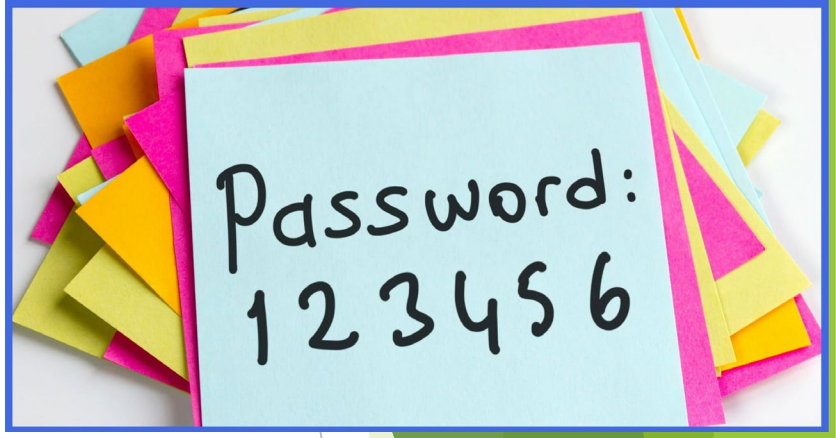


- The router is the heart of your local network
- Those that have “leased” routers are dependent on your Internet Service Provider (ISP) for service and maintenance
- Although advantageous from the point of convenience, some security issues
  - Your ISP knows your user ID and your password
  - Your ISP can access your network at any time
- We want to be able to trust our ISP but there are people that are not honest
- How do you prevent this?
  - Tell your ISP you want to set up your own ID and password and not have them access it
  - Get your own router and set it up yourself
- Also, reboot your router daily! This prevents malware through your system.

What About Devices on Your Network?

- The easiest way to control devices on your system is to set up a “guest” network on the router
- This guest network allows individuals that want and need access to your system to get that access
- HOWEVER, they do not have access to your main network or your files on the network
- This is great for family members to get on the internet without threatening your security
- It also allows the addition of devices without interfering with your main network

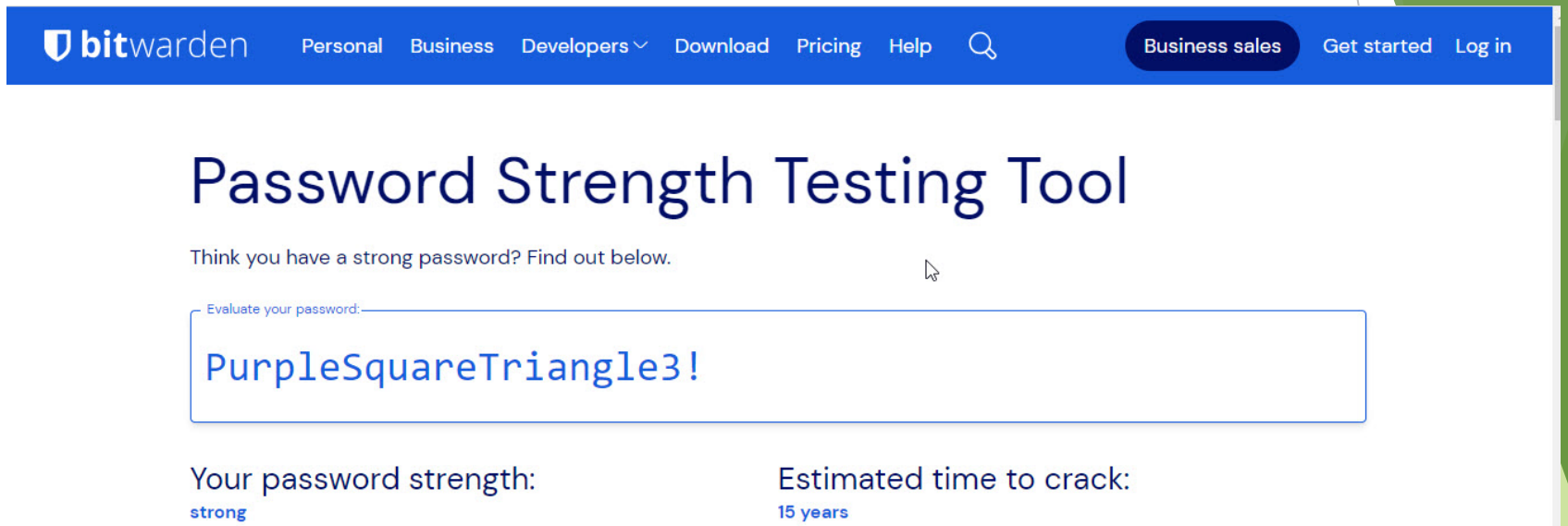
The BIG Question About Passwords

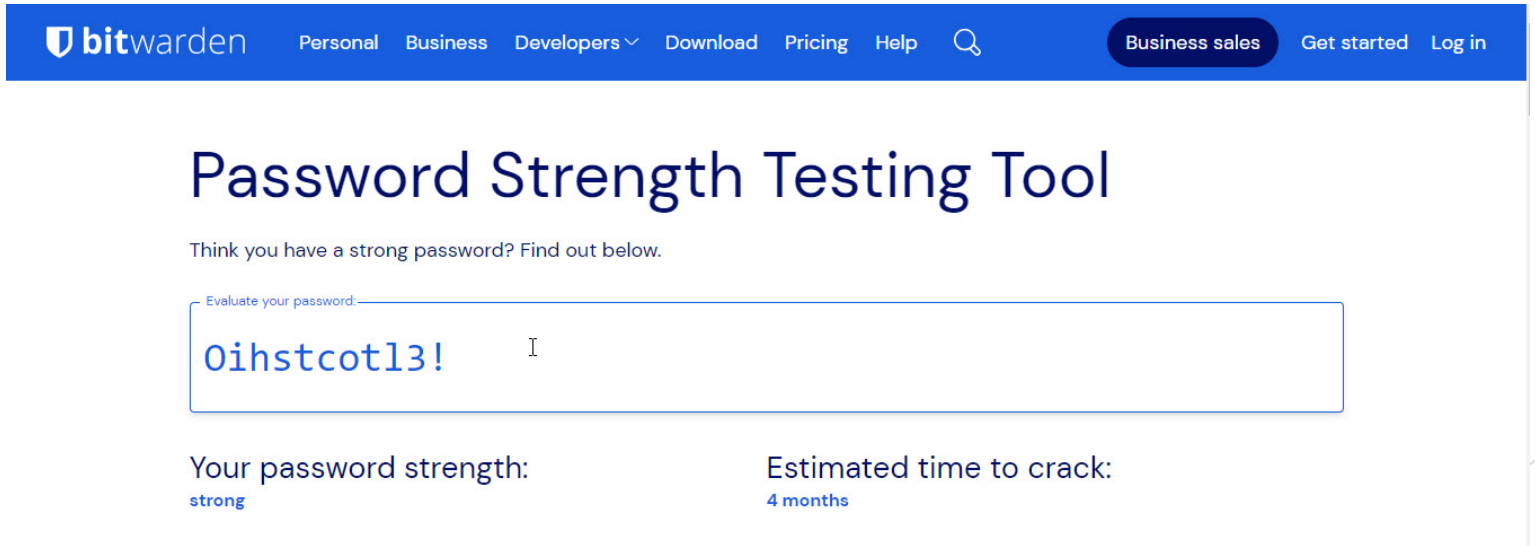


- Passwords are still here!
- They were supposed to go away with biometrics like face recognition, voice recognition and eye recognition
- NOPE! They are still here and they are still misunderstood
- Passwords take the form of complexity without recognition
- But in reality, you can make them just as strong AND remember them
- Take a color, add two shapes or objects and 2 numbers that mean something to you
- Make it something you can remember (The ORANGE HORSE ATE BUTTONS 3 times)
- That password is just as strong as a complex password!
- Don’t believe me? Just see the next slide.

Password Complexity

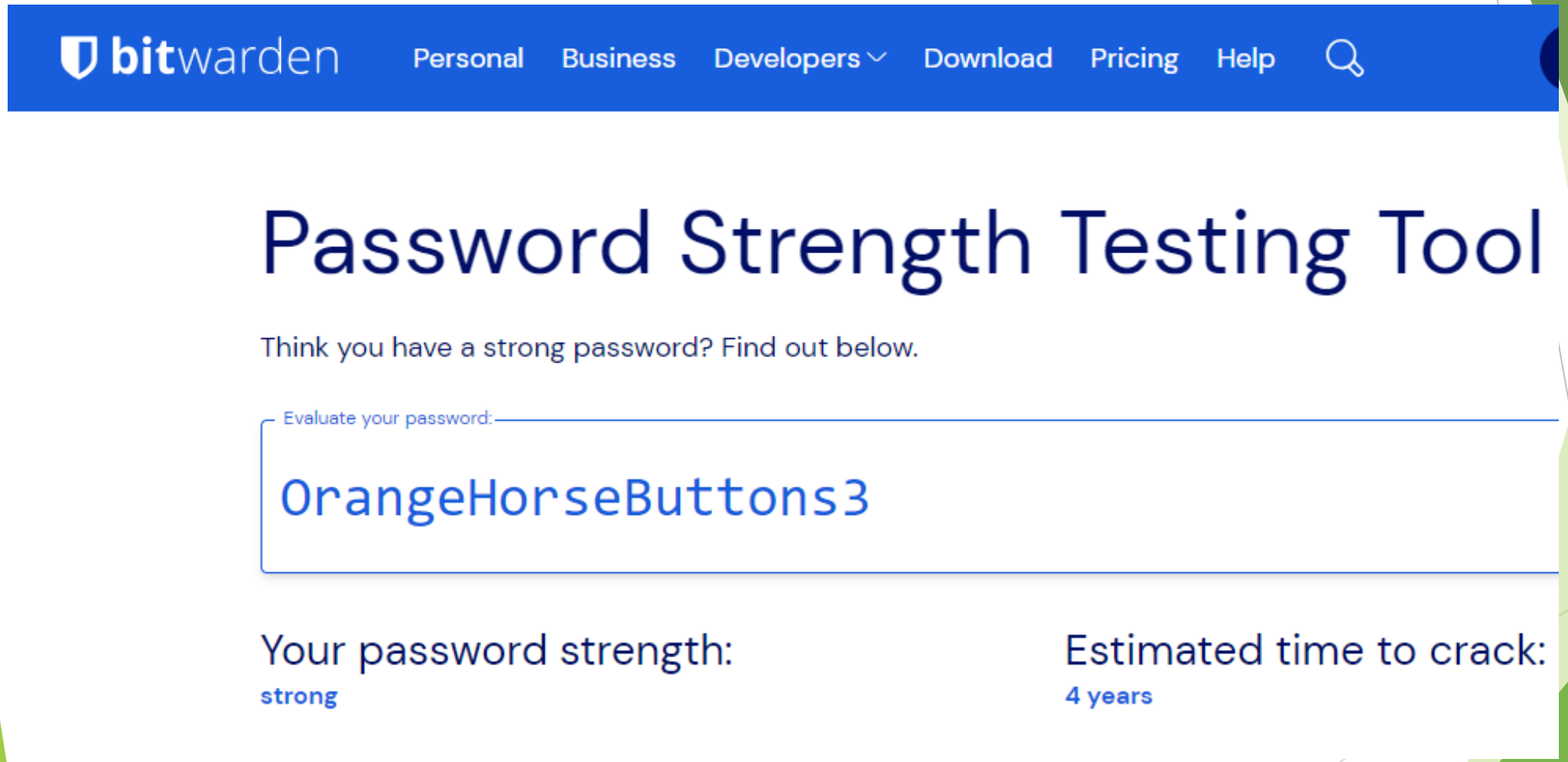
15 YEARS TO CRACK!!





4 MONTHS TO CRACK!

What About the Example?



Biometrics?

- Face recognition – Maybe good?
- Can use picture to fool the recognition
- Finger recognition – Maybe good?
- Gummy bear trick
- Voice recognition – Maybe good?
- Try it when you have a cold
- Multi-Factor authentication
  - Something you have, something you know, something you are
  - Cell Phone, Password, Biometrics
- Remember cell phone is rooted to YOU, not to an address

How About Keeping Safe Online?

- The main danger of online is succumbing to the BIG THREE
- Fear, Greed, Hope
- Fear example: IRS is coming for you! Send your ID and password
- Greed example: You just won a new iPad! Send your ID and password
- Hope example: You have been selected for a job! Send your ID and password
- In all three examples, the hacker evokes an emotion to get the job done
- In all three examples, it is easy to check whether these are real or not
- Think about it this way: If someone came to your door with these three situations, what would you do?
- The same way your protect your home you should reflect in your online behavior

Go To The Right Domain!

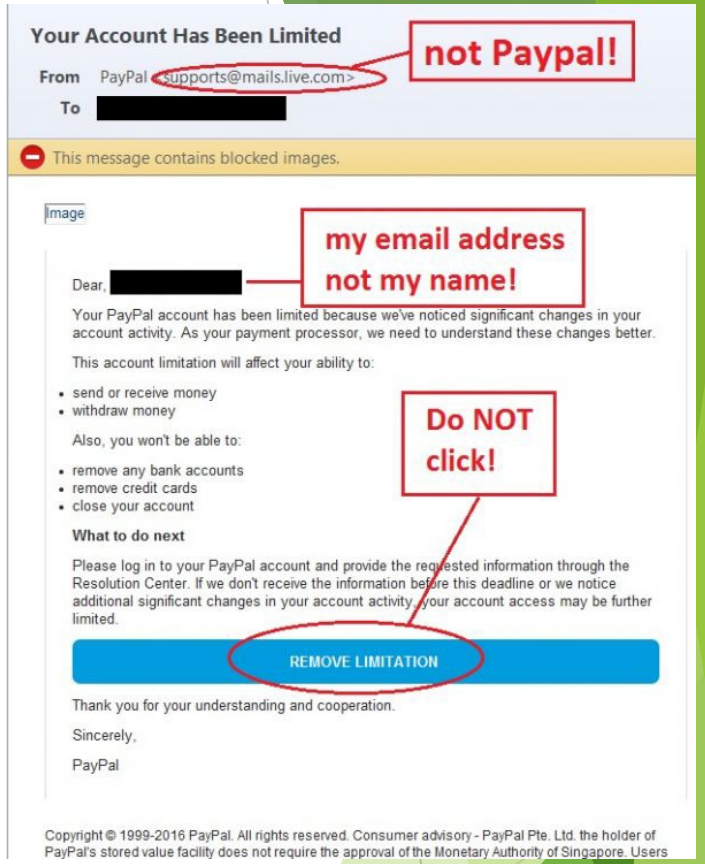
- There are several types of domains
- .com .org .edu .gov are just a few
- .edu and .gov are domains that the organization must verify before given
- Many people confused about where to go
- DO NOT go to what you THINK is the right domain – be certain!
- Example: irs.com is not IRS.GOV and will charge you for free items
- If you go to ssa.com you will not be at the government web site
- Ensure that you go to the proper website BEFORE you submit information
- Something simple can lead to a world of hurt – think before you click

What About the Family?

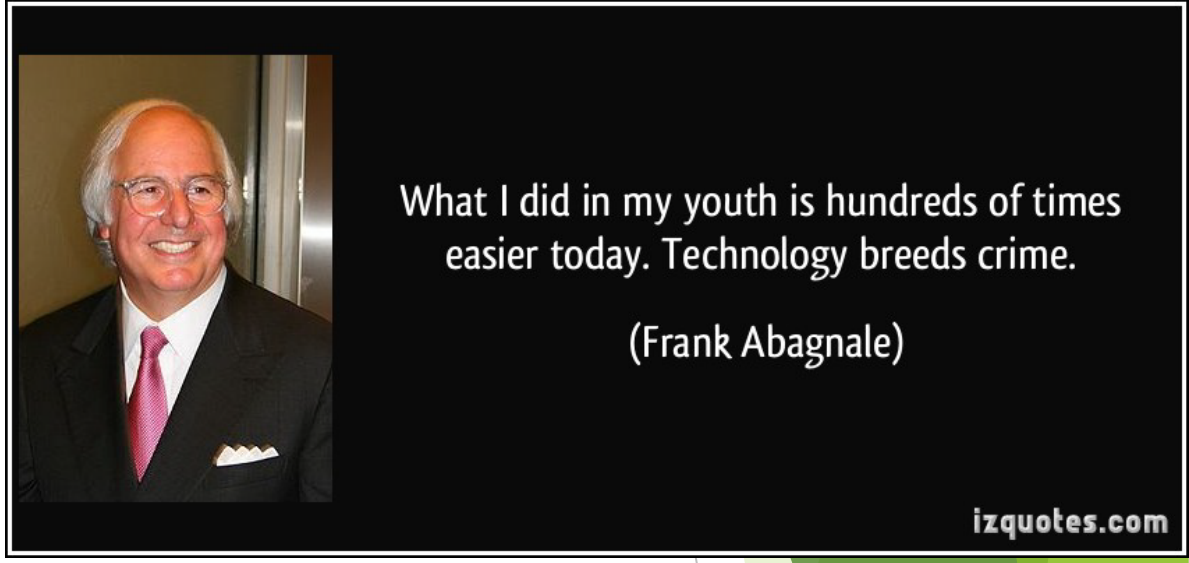
- You should NEVER reveal the “essential 3” online
  - Birthdate
  - Social Security Number
  - Mother’s Maiden Name
- NO commercial website can demand your REAL mother’s maiden name or real birthday
- They will accept any birthdate (within reason) as a way of verifying identity
- The trick is to REMEMBER the birthdate you put in the system
  - January 1 is a great universal month/day
  - The year can depend on whether you can remember that specific year
- Remember: If you only put your REAL birthdate as month/day and AGE, you have given them your birthyear!!

Can you be fooled?

- Examples of scams for the class
- Use the cell phone to show the type of scam
- Use the cell phone to show how to detect the scam
- In most cases you can tell your phone service about the scam
- You have heard it before
- DO NOT CLICK ON AN ATTACHMENT!
- DO NOT REVEAL YOUR USER ID AND PASSWORD!
- IF IT IS TOO GOOD TO BE TRUE, IT IS FALSE
- EVERYONE can be fooled. Everyone!



Catch Me If You Can



- Frank Abagnale
- Confidence man
- Fooled everyone into believing he was many people
  - Doctor
  - Teacher
  - Airline pilot
- AARP hired him as a consultant
- Why AARP would hire a known confidence man is beyond me
- The quote above says it all – technology enables crime
- Side Note: It is insane to think that GIVING a company access to your personal information will help keep you safe

Summary

- Covered how to keep your property safe
  - Physical means such as fences
  - Virtual means such as cameras
  - Observational means such as environmental awareness
- Covered how to keep your cyber safe
  - Password protection
  - Settings for privacy
  - Using proven scam prevention methods
- Places to seek help
  - FTC.gov, FBI.gov, DOJ.gov