Cybercrime 101

with an focus on

Identity Theft

Before diving in... (1)

- How many people have a:
  - Facebook account?
  - LinkedIn account?
  - Twitter account?
  - Email account(s)?
  - Online Banking/Brokerage accounts?
  - Smartphone?
  - Wireless Router?

Before diving in... (2)

- What other online accounts do you have???
- Across your online accounts, how many have the same user name and password???
- Where do you store your passwords???
- How "strong" are your passwords???
- How much personal info do you post online???
- Have you ever "googled" your name???

Before diving in... (3)

- For the remainder of this presentation:
  - Imagine yourself as the packets of digital data (1's and 0's) that comprise of your life such as
    - emails you send or the web pages you visit;
    - gas you buy with your credit card;
    - groceries you buy using your store bonus card;
    - which tv shows you watch and so on…
  - Also imagine that some of this data may or may not be intercepted intentionally or accidentally or not at all…

Introduction

This presentation is divided into two parts:

- Cybercrime
  - The high level (10,000 ft view) of the major subcomponents of cybercrime
- Identity Theft
  - We'll focus on identity theft specifically for this presentation

Cybercrime (1)

Cybercrime (2)

- We'll briefly discuss these areas:
  - Cybercrime
  - Psychology, drivers & motivation
  - Cryptography
  - Malware
  - Cyberactivists
  - Cyber-capability of World governments
  - Theft

Cybercrime (3)

- Cybercrime
  - Def: cyber attacks or theft, usage of malware to attempt to gain info
  - Origins – Russia
  - Silk Road – online drug marketplace
- Psychology, drivers & motivation
  - Risk aversion, Money ($**BILLIONS**$)!!!, low-cost tools, lack of legislation and understanding by politicians

Cybercrime (4)

- Cryptography
  - Def: a means to secure data using a key to encrypt/decrypt it
  - Weaknesses…
  - Quantum Cryptography

Cybercrime (5)

- Malware (1)
  - Def: unwanted software that performs unauthorized actions on a computer
  - Malware evolution, exploits/attacks, a/v industry, detection
  - Hacker Organizations – LOD, MOD…
  - Recent hacks – Target (70m compromised, terrible handling of unfortunate situation), Neiman Marcus, Michaels, Facebook, Twitter, SnapChat, etc...

Cybercrime (6)

- Malware (2)
  - Google Android on your phone and tablet tracking your every move... is this malware??? and what about ads popping up related to keywords in email, web searches or amazon searches... ??? Is there privacy any more ???
  - "Internet of Things" - connected devices spying on you?, better keep your clothes on...

Cybercrime (7)

- Malware (3)
  - Microsoft, Google, etc... – paying bounties per bug
  - New types of attacks emerging - TDoS

Cybercrime (8)

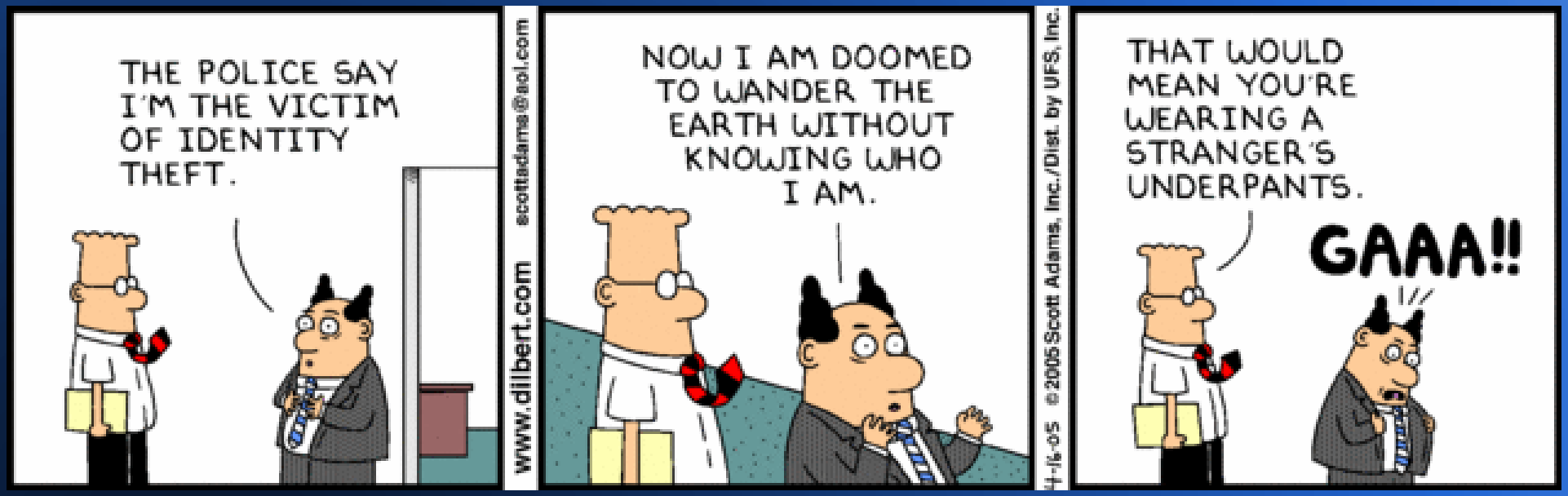
- Cyber-activists
  - Anonymous, The Peoples Liberation Front, LulzSec, AntiSec, TeaMp0ison, etc...
- Cyber-capability of World governments
  - NSA & GCHQ – in-depth media coverage, Iran's cyberwarfare czar assassinated (10/2013), Stuxnet, China (accounted for 41% of world's attack traffic during Q4'12), Countries spend $$$ in cyberware capabilities to gain intel, SEA brings down Twitter, Hezbollah...

Cybercrime (9)

- Theft
  - Identity Theft, Intellectual Property Theft, Medical Identity Theft, Aggravated Identity Theft, Sextortion...
  - Ransomware, etc...

Which leads us to the next topic of Identity Theft...

Identity Theft (1)



Identity Theft (2)

- Def. of Identity Theft:
  - Unauthorized or attempted use of
    - an existing account
    - personal info to open a new account
    - misuse of personal info for a fraudulent purpose

Identity Theft (3)

- We'll discuss these main areas:
  - Statistics
  - How to detect you've been victimized
  - What to do if you are victimized
  - How to protect yourself

Statistics (1)

- According to an Ipsos survey for Lloyds Risk Index 2013: "*Cyber risk is now the third biggest concern overall for company chiefs – ranking only after high taxation and loss of customers. In 2012, cyber risk was ranked as 12th…*"

Reference: "Cyber threats are now the third biggest worry for CEOs, Lloyds survey reveals"

Statistics (2)

- *"In 2012, more than 12 million people became victims of identity theft and fraud, with an estimated total of $21 billion losses for the year alone..."*

Reference: "Identity Theft Through Social Networking? Lessons to Take Now!"

Statistics (3)

- ~10% kids has had someone else use their SSN.
- Children targeted for identity theft 35x more often than adults.
- ~6M parents and kids improperly share identity information each year.

Reference: "How to Protect Your Child's Identity"

Statistics (4)

- *"In 2012 the highest percentage of consumer complaints (18 percent) were about identity theft. Consumers age 60 and older filed 52,610 complaints with the FTC about identity theft in 2012."*

Reference: "7 Identity Theft Prevention Tips for Seniors"

Statistics (5)

- *"The average annual number of identity fraud victims is 11,571,900 in the U.S. 7 percent of households reported some type of identity fraud. This translates to financial losses adding up to nearly $50 billion."*
- ***Reference: "And What's Your Mother's Maiden Name?"***

How to detect you've been victimized

- Alerted by credit card company that info has been changed
- Called by department store about an application you submitted
- Credit report shows credit checks or accounts are opened
- Bills for unfamiliar services
- Unusual charges on credit card

What to do if you've been victimized (1)

Take a deep breath…

What to do if you've been victimized (2)

What to do if you've been victimized (3)

- Get a copy of your credit report (free under these circumstances)
- File a initial fraud alert (free)
- Review credit report for fraudulant activity
- File a Identity Theft Victims' Complaint and Affidavit (FTC)
- File a police report

What to do if you've been victimized (4)

- File Form 14039, Identity Theft Affidavit (IRS)
- File Complaint with IC3 (if theft over state lines)
- File report with Office of Inspector General (SSA)
- File Complaint with Bureau of Consumer Protection (PA-AG office)

What to do if you've been victimized (5)

- If needed, credit freeze can be done (~$10)
- After 90 days, you may file extended fraud alert with credit agencies

What to do if you've been victimized (6)

- Call companies where charges were made to talk to fraud department
- Best to try to establish a timeline for fraudulent activity by getting any specific info the customer rep will provide (if possible)

How to protect yourself (1)

How to protect yourself (2)

How to protect yourself (3)

- Categories:
  - Computer usage
  - Information sharing
  - Smartphone usage
  - Credit & Financial
  - Other PII (Personally Indentifiable Information)

How to protect yourself (4)

- Computer usage:
  - Strong passwords with 2FA & no reuse
  - Operating system updates (*using XP?)
  - Latest A/V software
  - Router settings
  - Suspicious email? Delete it!
  - Embedded links in email? Don’t click!
  - Delete cookies – Watch 60 minutes?

How to protect yourself (5)

- Information sharing:
  - Shopping online? Use trusted retailer
  - Limit info posted online and check privacy settings
  - Limit what is shared in the "cloud" in the event there's a storm

How to protect yourself (6)

- Smartphone usage:
  - Password protect with a lock timeout
  - Use approved smartphone apps from the app stores and review permissions
  - Limit what is stored
  - Turn off bluetooth, NFC, wifi (unless in use)
  - Use A/V software?

How to protect yourself (7)

- Credit & Financial:
  - Check credit report at least annually
  - Credit card monitoring
  - Setup default alerts to be notified when a purchase is made on credit card
  - Don't use mother's maiden name
  - Add Security password on accounts
  - Add Security questions with cryptic answers

How to protect yourself (8)

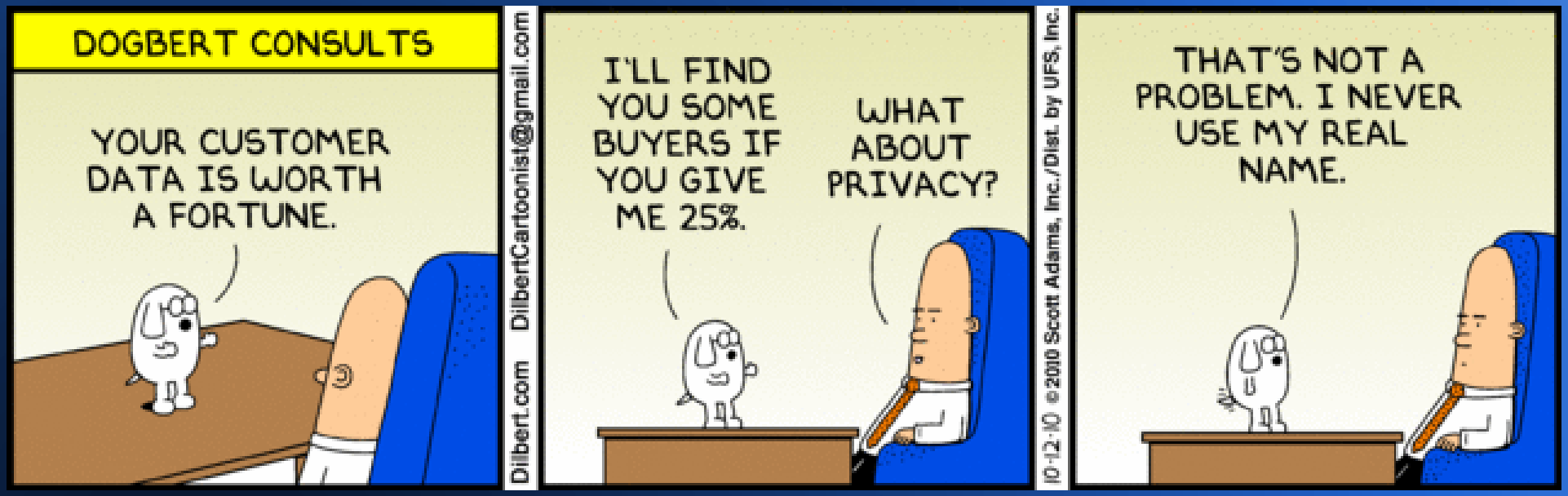
- Other PII (Personally Indentifiable information):
  - Limit personal info in wallet
  - Shred ATM receipts and snail mail
  - Keep financial, tax & medical records, social security number, passport, etc. in a safe place (a locked safe?)
  - Do not freely give out your SSN

How to protect yourself (9)

Summary (1)

- Identity theft is rising
- Businesses are tracking you
- The government may be tracking you
- BIG $$$ in data about you (think BIG DATA!!!)

Summary (2)


DOGBERT CONSULTS
YOUR CUSTOMER DATA IS WORTH A FORTUNE.
Dilbert.com DilbertCartoonist@gmail.com
I'LL FIND YOU SOME BUYERS IF YOU GIVE ME 25%.
WHAT ABOUT PRIVACY?
10-12-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.
THAT'S NOT A PROBLEM. I NEVER USE MY REAL NAME.

Quiz

- Which areas have you been a victim?
- What are three things you will address now with respect to pretecting your identity?
- Is any of this presentation shocking or eye-opening?

Interesting articles…

- "Do You Want the Government Buying Your Data From Corporations?",

http://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/

- "Metadata = Surveillance",
  https://www.schneier.com/crypto-gram-1403.html#3Article on big data tracking
- "What Big Data knows about you -- and how to keep your info safe"
- http://www.foxnews.com/tech/2014/03/01/what-big-data-knows-about-and-how-to-keep-your-info-safe/

Various References

- Gragido, Will; etal *Blackhatonomics: An Inside Look at the Economics of Cybercrime*. Waltham MA: Syngress, 2013.
- www.defensetech.org
- www.nakedsecurity.com
- www.schneier.com
- www.ftc.gov
- Various articles on the Internet

Q & A

Thank you!