How would you feel if you discovered that:

1. The NSA has taken photos of you engaged in sexual activity in your own bedroom?

(In a program called Optic Nerve, the NSA intercepted millions of Yahoo! Video chats and snapped photos every 5 minutes including "sexually explicit pictures containing nudity", p. 121)

2. There are images of child pornography stored on your computer's hard drive put there by cyber criminals?

(*Using "botnet" malware like ZeroAccess, which is sold on the "dark net", criminals regularly use millions of "zombie" computers (possibly YOUR computer) for all kinds of illicit activity, p.218.)*

3. For $100, criminals can buy a digital file on the internet which contains your personal information including name, address, telephone number, credit card info, SSN, passwords, and bank account info?

(There may well be one or several such files which are bought and sold every day on criminal websites such as Crimeazon.com....that's a real name, by the way, but a Google search won't take you there.)

So, how do you feel about that?

Future Crimes

Everything Is Connected
Everyone Is Vulnerable
And What We an Do About It

By Mark Goodman
2015

DEFINITION of 'Fullz'

A slang term that criminals who steal credit card information use to refer to a complete set of information on a prospective fraud victim. Fullz include, at a minimum, the victim's name and billing address; credit card number, expiration date and card security code; and Social Security number and birth date. Criminals can sell fullz for about $100; incomplete sets of consumer data sell for less. Criminals buy and sell fullz in the black market, usually online, and use them to commit credit card fraud, tax refund fraud, medical identity theft and other types of fraud. (from investopedia.com, emphasis added)

As we become more connected and dependent on digital technology, we are ALL Increasingly vulnerable to losses of: 1. wealth, 2. privacy, 3. identity.

As individuals, we stand in the middle of a host of vulnerabilities, roughly divided into two major camps:
1. hackers, etc. and 2. irresponsibly poor software.

The following groups are committed to gathering, legally or illegally, as much information about us as possible and using it for their profit:

1. individual hackers
2. hacker groups
3. transnational organized crime syndicates
4. governments
5. internet companies, and more and more often, brick-and-mortar businesses
6. data brokers
7. terrorists

Software security is lax or lacking as profits trump security every time:
“Either openly or behind closed doors, the majority of the software industry operates under a variation of the motto “Just ship it” or “Done is better than perfect.” Many coders knowingly ship software that they admit “sucks” but let it go, hoping, perhaps to do better next time.”

”The general public would be deeply surprised at just how much of the technology around us barely works, cobbled together by so-called duct-tape programming....”

Just how vulnerable are we?

In 2010 the German firm AV-Test estimated 49 million strains of malware in the wild.

In 2011, McAfee reported 2 million new pieces of malware every month.

In 2013, Kaspersky reported nearly 200,000 new malware samples every single day.
(chapter. 2, p. 14)

Based on research, “the antivirus software you are running on your own computer is likely only catching 5 percent of the emerging threats targeting your machine” (p. 15).

“...Criminals and virus writers are completely out-innovating and outmaneuvering the antivirus industry established to protect us against these threats” (p. 15)

We are vulnerable as individuals, and we are vulnerable as a country.

“The problem is worse than you think: in a July 2014 study of critical infrastructure companies across multiple sectors [e.g., water, sewage, emergency services, electrical grid], nearly 70 percent of them had suffered at least one security breach that led to the loss of confidential information or the actual disruption of operations during the preceding twelve months” (p. 22).

The Wall Street Journal reported that “cyber spies had 'penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system.' The same officials went on to say that spies from Russia and China have allegedly mapped the American grid so that in times of crisis or war with the United States its entire electrical network 'could be taken out.'” (p. 23)

Hackers at an annual German gathering “demonstrated how to get full control of industrial infrastructures in the gas, chemical, oil, and energy industries. Equally troubling is...that hackers share this information with each other and have even created fully searchable public databases of known exploits....” (p.24)
[A website called Shodan has effectively become the hackers' equivalent of Google.]

Our personal digital devices will only become more vulnerable to hacks as the software becomes more complex going forward.

One rough way to estimate vulnerabilities is to look at the lines of code (LOC) in a software program/app. The more LOC, the more errors and bugs which can be exploited by hackers. Microsoft Office 2013 has 45 million LOC. One study suggested 20-30 bugs per 1000 LOC for commercial software in general. By that criterion, Office may have 1-1.5 million vulnerabilities.

“It is unsettling but true that to date no computer system has been created that cannot be hacked.” (p. 43)

After discussing all the great apps (e,g, browsers, e-mail, Google Earth) that we get for free from online companies, Goodman then asks, “Did you ever stop and wonder why Google never sends you a bill?”

The disconcerting answer: because “**you are not Google's customer, you are its product.”**

While it does make some money from advertising, Google, and thousands of other companies around the world, make the bulk of their income from collecting as much information about you as possible and then selling it to advertisers. “In early 2012 Google announced it was merging its data across all of its seventy products and services. The result: a unified, profound, and unprecedented view of you and your world.... Many have even argued that Google knows you better than you know yourself.”

Google indefinitely (permanently?) stores all your
Searches (websites, Google Earth, Street View)
E-mails, phone and browser settings,
Voice mails, translations, maps,
Photographs, documents,
Videos (including YouTube),
Locations (based on Android smart phone GPS data)
Contacts (and all their data)
Appointments and calendar entries.
In other words, almost EVERYTHING you do online.

“In 2013, Google admitted that its bizarre-looking Street View cars were not just taking photographs of streets...but also pilfering data from computers inside our homes and offices, including passwords, e-mails, photographs, chat messages, and other personal information from unsuspecting computer users.”

[Apparently not content to milk only its own customers, Google was stealing from pretty much <u>everybody</u> using a digital device.]

And Facebook is just as bad: “Advertisers know every last intimate detail about a Facebook user's life....”

How about Apple? “...Every time you speak a query into Apple's Siri artificial intelligence agent, your voice recording is analyzed and stored by the company for at least two years.”

<u>Who buys all this data?</u> Advertisers, governments (think NSA), cyber criminals, terrorists—basically, anybody who can afford it. Its all about PROFIT. (“Google's consolidated revenue for 2013 was more than $59 billion.” p. 55))

[No wonder the phrase “corporate ethics” is considered by many to be an oxymoron.]

“But how can they get away with this?

The answer is simple: you said they could.”

You gave them permission when you clicked on “I agree” to the ToS (Terms of Service).” (aka the user agreement)

[If you haven't already, please look up the new ToS for Windows 10—it is appalling, although in reality only slightly worse than previous Terms of service.]

“The fact is, its the Wild, Wild West out there, and there is little or no regulation that protects you and your data.... By sharing millions of names and contact details with its app vendors, Google increases the likelihood that your data will leak, be stolen, or be misused.” (p.62)

Chapter 5: The Surveillance Economy

Subheading: “You Thought the Hackers Were Bad? Meet the Data Brokers” (p.66)

“The Acxiom company... operates more then twenty-three thousand computer servers that are collecting, collating, and analyzing more than 50 trillion data transactions every year. Ninety-six percent of American households are represented in its data banks, and Acxiom has amassed profiles on over 700 million consumers worldwide.”

“Data brokers get their information from
ISPs
Credit card issuers
Mobile phone companies
Banks
Credit bureaus
Pharmacies
Departments of motor vehicles
Grocery stores
And increasingly our online activities.”

Chapter 6: Big Data, Big Risk

“Facebook, Google, Linkedin, and others ...are routinely hacked, and the data taken are yours. How often does this happen? Way more than you might ever imagine.”

“Facebook's own security department has shockingly acknowledged that over 600,000 accounts are compromised **every day**.”

“These data can be used for identity theft, criminal impersonation, tax fraud, health insurance scams, and a host of other criminal offenses.”

Not only hacking but human error can also compromise our data:
“In 2013, the data broker Experian mistakenly sold the personal data of nearly two-thirds of all Americans to an organized crime group in Vietnam....The Social Security numbers of 200 million Americans were then available to thieves around The world.” (p.89)

Chapter 10: Crime, Inc.

Organized crime is big business; it “is believed to account for up to 15 to 20 percent of Global GDP.” [which is roughly equal to the U.S. GDP at 18% of global GDP.]

Not only is cyber crime extremely profitable, it is low-risk: “prosecutions are exceedingly rare, perhaps occurring in less than one one-thousandth of 1 percent of all cases.”

Hacking is a growth industry, and skilled hackers are often professionals. “A full 80 percent of hackers are now working with or as part of an organized crime group.” (p.176)

The largest criminal syndicates are as big as, and function much like legitimate international corporations. They use the “latest cutting-edge business practices taught at Wharton and Harvard Business School.... Within these criminal syndicates, there are divisions of labor, supply chain management, department heads, outside consultants, and team deliverables. Their organization is sophisticated .
CEO
CFO
CIO (Chief Information Officer)
CMO (Chief Marketing Officer)
Middle management
Worker bees/infantry
R and D
Coders, engineers, and developers
Quality assurance
Affiliates, Technical support, Director of Human Resources, Money mules

“There are at least fifty such online “Crime, Inc”. organizations currently in operation around the World.

Goodman describes working with the Brazilian Federal Police in the favelas (slums) outside Rio de Janeiro. Street dealers sold DVDs with tens of thousands of compromised credit card numbers and user details. “The crime start-ups sold their DVDs to other criminals, offering discounts when bought in bulk. They also included service-level agreements with their software, assuring that at least 80 percent of the stolen credit card numbers would work or 'your money back.'”

“CRIME U
Hackers are not born; they are trained, supported, and self-taught by an enormous amount of free educational material in the digital underground. Crime, Inc. is a learning organization, and there are online tutorials for everything from defeating firewalls to cloning credit cards. Criminals have access to their very own massive open online courses where they can learn how to launch phishing and spamming campaigns as well as how to use crimeware exploit kits. All of this training amounts to a sort of online criminal university (Crime U)....” (p. 187)

Chapter 11. Crime U exists on the “dark net”, which is also where much of the buying and selling of illegal products and services occurs. On the dark web you can buy:
Pirated content, stolen luxury goods/electronics (sort of like ebay),
drugs (all the usual suspects plus rare products like a zombification drug),
counterfeit currency, cards/accounts, identity theft, documents (including passports),
weapons, ammo, and explosives, hit men, child sexual abuse images, human trafficking,
human organ trafficking, [and others too disturbing to present in this forum] (p. 208)

Crime as a Service (CaaS)--almost incredibly, you can also hire people to commit crimes for you.

Discussion

What Can We Do About It

WHAT CAN WE DO ABOUT IT?

1. Reduce your data trail (avoid surveillance)
2. Anonymize your data trail (as much as possible)
3. Use as many safety products as possible

Because most of us have a “problem with technical literacy”, we will need to spend some time and energy educating ourselves about computer terminology and technology related to online security.

For example,
see library Gale courses
Alison.com course “Protect Yourself from Identity Theft”
Read chapter 15, “Solutions For the Rest of Us” in Data and Goliath
Definitely read “Ultimate Privacy Guide” at **BestVPN.com** (you can also check out VPNs on that website).
Multiple books on internet security for the layman available from Amazon.com

Yes, its not the most exciting stuff to research, but consider that there is an inverse relationship between knowledge and security: the less you know about this stuff, the more vulnerable you are.

1. use cash for most purchases. This both reduces your data trail (no credit card record that can potentially be hacked) and is anonymous (nobody has a list of stuff you buy).
2. Use gift cards/pre-paid credit cards online (or whenever cash can't be used).
3. Spoof when filling out forms (i.e., provide fake data) to protect your identity.
4. change all your critical passwords (e.g. online bank website) to 20 digits and use a password manager/wallet so you don't have to remember them.
5. turn off your computer when not using it, especially overnight. You have reduced your chances of being hacked by a third.
6. Better yet, turn off your wi-fi (routers can be hacked too); just unplug the power cord.
7. Encrypt your data on your hard drive (research how to do this online).
8. Encrypt your internet traffic by using a VPN (virtual private network), TOR, or at least an anonymous web browser like DuckDuckGo or Startpage (forget Google search).
9. If possible, avoid Windows OS. If you need a new computer, get a Mac, or better yet download a Linux OS (or buy a computer with Linux pre-installed).
10. Use FOSS (free open source software) vs. proprietary software (who knows what's inside, e.g., NSA “backdoor”). FOSS code is open to public scrutiny and can be checked for bugs, malware, backdoors, etc. plus its FREE. Not completely secure but better. Examples of FOSS: Firefox web browser (forget Internet Explorer), OpenOffice (replaces Microsoft Office Suite).
11. Cover up your computer's camera with, e.g., a Post-It note, when not in use (cameras can be turned on remotely to watch you). Also do this with your “smart” TV and phones.
12. Update your OS and plug-ins automatically or frequently.

13, Download from official sites only (a lot of “free” software from third-party sites is infected with malware.)
14. Do not use an administrator account for everyday work and online browsing. Instead use a standard user account. (helps prevent the downloading of some malware.)
15. Warn your kids about the dangers of social media. YOU be very discreet when using social media. Comments left there can be used by exes, stalkers, burglars, pedophiles, bullies, divorce lawyers, potential employers, and others.
16. Never open an e-mail if you're not 100% sure where it came from. If not sure, verify with a phone call.
17. Learn about and use the security features on your OS, but do not rely on them exclusively. Research and download security apps like HTTPS Everywhere, Privacy Badger, etc.
18. Other examples of encryption apps: Off The Record--chat encryption, Spideroak for cloud encryption, Silent Circle for encrypted VOIP (forget Skype if you have privacy concerns). Remember that these kinds of services become obsolete as technology progresses, so periodically search for new, improved products.

Issues in the Later Chapters (not discussed tonight**)**

Chapter 12 focuses on IoT (Internet of Things). “In late 2013, Google sent a letter to the Securities and Exchange Commission noting 'we and other companies could [soon] be serving ads and other content on refrigerators, car dashboards, thermostats, glasses and watches, to name just a few possibilities.'” p. 234

Chapter 13: Home Hacked Home. “Dozens of demonstrations by hackers and security researchers have proven it is entirely possible for criminals fifteen hundred miles away to seize control of your car when you are driving sixty-five miles per hour down the highway. ...In July 2014 the FBI warned in an internal report that driverless cars could be used as 'lethal weapons'....”

Chapter 14: Hacking You. (“The internet of You”) Wearables, implantables, embeddables, and ingestibles mean that to one extent or another we will all join the cyborg nation—opening up our physical bodies to cyber attacks for the first time.” p.288
[Enlarge your vocabulary with a new word: “teledildonics”] (p. 287)

Chapter 15: Rise of the Machines:When Cyber Crime Goes 3-D. Good robots, hacked robots, killer robots; 3-D print your own guns, hand grenades and mortar rounds; bio-fabrication printers can print human tissues and organs; so-called “chemputers” can print drugs on demand.

Chapter 16: Next-Generation Security Threats: Why Cyber Was Only the Beginning. Weak AI to strong AI. Neuroscience--”Under laboratory conditions, it has already been possible to record a person's memories, engage in telepathic communication, video record dreams, and perform telekinesis, with new discoveries emerging all the time.” (p.328) Hacking DNA.