Data, Data Everywhere - What Are You Doing to Protect Yourself?

How to protect yourself from personal data theft

May 29-30, 2013
What data should you be worried about protecting? – protect ‘your personal’ critical infrastructure

Types of protection measures – preventative, during and after an incident ( translating business continuity and disaster recovery to a personal level)

Why is news important?
information and alerts, natural disasters – where are your critical documents and data?

Regulatory and ethical obligations – do what is ‘right’ ( not easy necessarily ) and when in doubt ‘ask questions’

Empower yourself
Why protect the data?

- Person/Organization
- Revenue
- Reputation
- Regulation
## RRR – Business vs. Individual Risks

<table>
<thead>
<tr>
<th>Risks</th>
<th>Business</th>
<th>Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>Sales, Profits, Repeat Business, Shareholder’s trust</td>
<td>Damage to Credit, Financial Loss</td>
</tr>
<tr>
<td>Regulation</td>
<td>Fines, Liability, Indemnity, Risk of Incarceration</td>
<td>A person may sometimes intrinsically and inseparably associated with the brand or be the ‘business’</td>
</tr>
<tr>
<td>Reputational</td>
<td>Loss of credibility in the market, loss of goodwill</td>
<td>Stalking, bullying, blackmail, loss of privacy and credibility</td>
</tr>
</tbody>
</table>
Here are some of the ways that we create data:

<table>
<thead>
<tr>
<th>Personal Information</th>
<th>Identity Verification</th>
<th>Legal and Financial Information</th>
<th>Medical History</th>
<th>Social Interaction</th>
<th>Technology Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>How much does the baby weigh?</td>
<td>Certificate of Death</td>
<td>Education</td>
<td>Resume</td>
<td>Confidential</td>
<td>Browsing behaviors</td>
</tr>
<tr>
<td>Where were you born?</td>
<td>What’s your name?</td>
<td></td>
<td></td>
<td></td>
<td>Directory record</td>
</tr>
<tr>
<td>It’s a girl!</td>
<td>Your Social Security Number.</td>
<td></td>
<td></td>
<td></td>
<td>Criminal record</td>
</tr>
<tr>
<td>It’s a boy!</td>
<td>Sign your passport.</td>
<td></td>
<td></td>
<td></td>
<td>Background check</td>
</tr>
<tr>
<td>What’s your name?</td>
<td>Travel visas</td>
<td></td>
<td></td>
<td></td>
<td>Drugs Testing</td>
</tr>
<tr>
<td>Your Social Security Number.</td>
<td>Travel Insurance</td>
<td></td>
<td></td>
<td></td>
<td>Survey</td>
</tr>
<tr>
<td>Sign your passport.</td>
<td>Auto Insurance</td>
<td></td>
<td></td>
<td></td>
<td>Donations</td>
</tr>
<tr>
<td>Travel visas</td>
<td>Health Insurance</td>
<td></td>
<td></td>
<td></td>
<td>Student Records</td>
</tr>
<tr>
<td>Travel Insurance</td>
<td>Home Insurance</td>
<td></td>
<td></td>
<td></td>
<td>Contracts and Agreements</td>
</tr>
<tr>
<td>Auto Insurance</td>
<td>Renters’ Insurance</td>
<td></td>
<td></td>
<td></td>
<td>Negotiations</td>
</tr>
<tr>
<td>Health Insurance</td>
<td>Personal networking</td>
<td></td>
<td></td>
<td></td>
<td>Forensics – for example fingerprints</td>
</tr>
<tr>
<td>Home Insurance</td>
<td>Driver’s License</td>
<td></td>
<td></td>
<td></td>
<td>Incident reports</td>
</tr>
<tr>
<td>Renters’ Insurance</td>
<td>Immunization</td>
<td></td>
<td></td>
<td></td>
<td>Conversations (voice, electronic)</td>
</tr>
<tr>
<td>Personal networking</td>
<td>Hospital Discharge record</td>
<td></td>
<td></td>
<td></td>
<td>Pictures and Videos</td>
</tr>
<tr>
<td>Driver’s License</td>
<td>Military Record</td>
<td></td>
<td></td>
<td></td>
<td>Cellphone location services</td>
</tr>
<tr>
<td>Immunization</td>
<td>Employee Record</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What data should you be worried about protecting?

Examples:

Medical – diagnosis, prescriptions
Financial – credit report, credit card, bank account information
Personal – wills, inheritance, family heirloom data (historical letters)
Informational – location, vacation itineraries
Identity – SSN, name
Intellectual – innovations, research, creativity
<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit card details</td>
<td>From $2-$90</td>
</tr>
<tr>
<td>Physical credit cards</td>
<td>From $190 + cost of details</td>
</tr>
<tr>
<td>Card cloners</td>
<td>From $200-$1000</td>
</tr>
<tr>
<td>Fake ATMs</td>
<td>Up to $35,000</td>
</tr>
<tr>
<td>Bank credentials</td>
<td>From $80 to 700$ (with guaranteed balance)</td>
</tr>
<tr>
<td>Bank transfers and cashing checks</td>
<td>From 10 to 40% of the total $10 for simple account without guaranteed balance</td>
</tr>
<tr>
<td>Online stores and pay platforms</td>
<td>From $80-$1500 with guaranteed balance</td>
</tr>
<tr>
<td>Design and publishing of fake online stores</td>
<td>According to the project (not specified)</td>
</tr>
<tr>
<td>Purchase and forwarding of products</td>
<td>From $30-$300 (depending on the project)</td>
</tr>
<tr>
<td>Spam rental</td>
<td>From $15</td>
</tr>
<tr>
<td>SMTP rental</td>
<td>From $20 to $40 for three months</td>
</tr>
<tr>
<td>VPN rental</td>
<td>$20 for three months</td>
</tr>
</tbody>
</table>

So, how much is it worth?

Courtesy: Pandasecurity.com
· **Contact:** Via ICQ, Messenger or similar or via email (generic addresses).

· **Try & Buy:** Most offer tests or free demos. They also use online sites for checking algorithms to guarantee the authenticity of the card details.

· **Minimum orders and bulk discounts:** Minimum orders are established (5 or 10 units in the case of credit card or bank details). There are discounts for bulk buying.

· **Specialized online stores:** Once contact has been made, many use online sites set up as stores for distributing their products (which can’t be accessed without a username and password).

· **Methods of payment:** Western Union, Liberty Reserve, WebMoney or similar.

· **Customer services and support:** They offer service guarantees. If the product does not work (if the numbers, login credentials are not valid, etc.), they will be changed for others that are operative.

· **Promotion:** These services are mainly advertised through underground forums, although some of the boldest use social media and have accounts on Facebook and Twitter, etc.

Courtesy: Pandasecurity.com
How can you protect your data?

- People
- Process
- Technology
‘People’ based controls

- Reveal information on a ‘need to know’ basis
- Verify recipient before sharing data
- Robocalls – NEVER disclose information, don’t entertain these, ask to be taken off the list
  

- Protect your passwords
- Be ‘phish-aware’
- Trust your 6th sense
Process Controls

- Take precautions while travelling – inform the bank, credit card companies, monitor statements, understand and respect the laws of the land

  http://mcaf.ee/cryptolaw *

  * Courtesy Simon Hunt

- Do not disregard news snippets that talk about identity theft. It can happen to anyone.

- Take advantage of county, bank or city organized shred events

- Double check purses, wallets, pockets before you donate or dispose.

- You get access to free credit report once every year, use it

- Read your credit card bill and your bank statements
Technology Controls

- Keep your computing devices’ antivirus definitions and software (applications and Operating System) updated
- Encrypt – 7 Zip, Winzip, TrueCrypt
- Use strong passwords, two-factor and two-step authentication whenever possible
- Captcha (although annoying) is good
- Keep your antivirus definitions and software versions up-to-date
- Use firewall and filtering
- Always back up your data on a hard drive or storage device that YOU control, and encrypt sensitive data
Scripps News Says It Uncovered Unsecured Lifeline Personal Data

Part of investigative series on data security; targets of investigation say Scripps was the one breaching security

By John Eggerton -- Broadcasting & Cable, 5/20/2013 1:08:15 PM

Scripps News, which serves the company's broadcast, newspaper and online properties, Monday began publishing stories on what it says it has uncovered data security lapses affecting thousands of customers whose data was collected by companies participating in the government's Lifeline phone subsidy program. The FCC is testing an expansion of that program to broadband subsidies.

According to the news service, its Privacy on the Line investigation turned up 170,000 records containing personal data -- Social Security numbers, financial account information -- widely available online from two companies participating in the program.

Scripps says that lawyers for the two companies, TerraCom and YourTel, counter that Scripps accessed the records illegally. Scripps denies the charge. YourTel and TerraCom have posted virtually identical notices on their respective websites saying their data was breached by Scripps and "possibly by other unauthorized persons," although they say that "there appears to be no evidence to indicate that a malicious attack occurred on our computer systems, nor does it appear that any applicant has been injured as a result of the unauthorized accessing of personal data files by the news organization or any others."

"Contrary to the claims by Scripps Howard that this information was all 'publicly posted data online' and tens of thousands of Lifeline applicants' personal data was available through 'simple Internet searches,' a digital forensics investigation by TerraCom has revealed that the news service used sophisticated computer techniques and non-public information to view and download the personal
Regulations

- HITECH - Health Information Technology for Economic and Clinical Health Act (2009)
- PCI DSS – Payment Card Industry Data Security Standard
- GLB - Gramm–Leach–Bliley Act OR Financial Services Modernization Act (1999)
Security Objectives

Confidentiality
Integrity
Availability

Disclosure
Destruction
Disruption
**Due Care** is the development and implementation of policies and procedures towards mitigating the risks to an acceptable level.

*Employees should exercise due care when transmitting confidential data by using secure means such as email encryption (GWemail Encryption Service)*

**Due Diligence** is the act of investigating and understanding the risks.

*Employees should engage appropriate departments to review and assess contracts and system deployments*
Due Care:
• Sharing information on a ‘need to know’ basis
• Verify authority (Identification, callback)
• Safe deposit box, backup data, encrypt, strong passwords
• Shred securely
• Degauss or destroy electronic storage

Due Diligence:
• Scrutinize contracts and agreements
• Insurance, liability and indemnity
• Terms and Conditions
• Engage competent trust advisors
• Understand breach notification policy and processes
• Research, investigate and datamine
Reality Check Resources

Panda Security Report 2011

An app that tells you the same information but in an interesting way
http://www.creditcards.com/credit-card-news/credit-card-fraud-price-list-1282.php

NPR Podcast

Imperva Blog

FBI – Common Fraud Schemes
http://www.fbi.gov/scams-safety/fraud/internet_fraud

Internet Crime Complaint Center
Learning Resources …and they are free for you

Teach Privacy Videos:  http://my.gwu.edu/mod/itsecurity_video/

SANS Secure the Human Training
https://gwu.securingthehuman.org/mod/client/auth/login.php *
• Please send requests to infosec@gwu.edu to create a new account

Security Awareness Presentations and Articles
http://it.gwu.edu/security-awareness-presentations-and-articles

Security Blog
http://it.gwu.edu/security-blog

https://www.privacyrights.org/
GW context :
Notify Chief Technology / Information Security Officer via the IT Support Center at 202-994-4948
Don’t try to fix it yourself.

Personal context:
Notify the law enforcement, banks, credit monitoring agencies, social security administration (if SSN stolen) and any other critically connected departments or entities immediately.
Keep logs of all communication.
http://www.fbi.gov/about-us/investigate/cyber/identity_theft > What To Do if You’ve Been Victimized
Questions?

Presented by:

Noor Aarohi  
Senior Analyst - Risk and Compliance  
GWIT Information Security and Compliance Services  
infosec@gwu.edu

703-726-3664