Security of Personal and Financial Information

Randy Marchany
Chief IT Security Officer
Director, IT Security Lab
VA Tech IT Security Office & Lab

www.security.vt.edu
grouply

See Thomas Barber's profile and list of groups!

You're just a few steps away from seeing Thomas Barber's profile page and list of groups!

First Name: [Blank]
Last Name: [Blank]
Email Address: [Blank]

Yahoo ID: [Blank]
Yahoo Password: [Blank]

- We use your Yahoo ID to automatically connect to your Yahoo Groups. (FYI Grouply is not part of Yahoo.)
- Why does Grouply need this?

- Use my Yahoo ID and password as my Grouply ID and password.
- I have read and understand Grouply's Terms of Service.
- I am also a Google Groups user.

Next >>
5 Things You Need To Know

• What/Where is it?
• Who’s responsible for it?
• How sensitive is it?
• Who has access to it?
• What if it gets into the wrong hands?
What/Where Is It?

• WHAT - Define Sensitive data
  – Easy (PIRN – Personal Info Requiring Notifications)
    • Ssn, ccn, DMV#, passport #, bank account #, Debit card #, name in combination with date of birth (DOB)
  – Hard
    • Information that could cause embarrassment to the institution
    • Information on info that could cause issues if disclosed prematurely
    • Violation of Regulations or Compliance requirements

• WHERE IS IT?
  – Before you can protect it, you need to find it.
  – Use Freeware tools
    • VA Tech Find_SSN, Cornell Spider, UT-Austin SENF
  – Commercial Tools
    • IdentityFinder, Content Sentinel, Safe Vantage Technologies Deep Scout
  – FALSE POSITIVES!
How Sensitive Is It?

- Does the information fall under the privacy protections of federal or state statutes or regulations? Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and related regulations and policies, including university policies.

- Is the information subject to privacy or confidentiality protections of private agreements? Examples are non-disclosure agreements and other contractual agreements.

- Does the information require confidentiality through professional ethics or through procedural requirements? Examples are unpublished research findings, the identity of research subjects, and examination questions.
Regulation Compliance

- **FERPA** – mandates appropriate security of the education record
- **HIPAA** - privacy protection for health records
- **G-L-B** - the security and confidentiality of customer nonpublic financial information records
- **PCI** - Payment Card Industry (PCI) Data Security Standard for credit card usage
- **SOX** - Sarbanes-Oxley Act dealing with financial applications
- **Patriot Act** – gives the federal government the ability to investigate threats to the national security
- **Red Flags Rule** – provide identity theft prevention program required by the Federal Trade Commission
- **Copyright laws** – legal right to exclusive publication, production, sale, or distribution of literary, musical or artistic work
  - Software; Publications; Music/Movies
- **Additional Federal and State regulations** – dealing with day-to-day activities from purchasing items to personnel issues to reporting structures to what’s legal to access
Who Has Access?

• Does access to the information require approval? Examples include Banner access, access to confidential files, and access granted to and required by computer system administrators.

• Could the personal information potentially cause harm to a person or persons? Information about large numbers of individuals, such as applicants for admission to a university program. Information about one or two people, for example, someone who makes travel plans for others might have another person’s personal credit card number to make hotel reservations.
What If It Gets in the Wrong Hands?

• You will write a lot of notifications letters
• You will pay for Identity Protection services for those affected
• You will take a major hit in the media
• You will have to answer to your Board and explain what happened
Why Discuss IT Security?

- Because we don’t want to end up here!

<table>
<thead>
<tr>
<th>Chronology of Data Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 29, 2010</td>
</tr>
<tr>
<td>April 30, 2010</td>
</tr>
</tbody>
</table>

Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2008: 354,140,197

What does the total number indicate?
Simple Strategy

- Protect Your Data
- Protect Your Machine
- Protect Yourself

- Easier said than done
IT Security and YOU!

Common excuses for not caring about IT Security

• My computer is brand new…
  - The internet is flooded with thousands of attacks every second

• I don’t have enough time..
  - Is there time to recover from an incident

• There's nothing important on my machine
  - Hackers aren't picky, any vulnerability is a launch pad for an attack
You’re Being Probed Constantly
Virginia Tech Policy 7010

- This policy will help ensure that all technology resources and services are as stable, secure and trustworthy as possible to help ensure security for individuals, departments, and the university.

- Departments and individual users must adhere to security standards.
Virginia Tech Policy 7025

- Policy 7025 helps Virginia Tech comply with the Gramm-Leach-Bliley Act and calls for the protection of nonpublic personal financial information.
Other Important Policies

- **1060** Policy on Social Security Numbers
- **7000** Acceptable Use of Computer and Communication Systems
- **7010** Policy for Securing Technology resources and Services
- **7025** Safeguarding Nonpublic Customer Information
- **7030** Policy on Privacy Statements on Virginia Tech Web Sites
- **7035** Privacy Policy for employees Electronic Communications
- **7040** Personal Credentials for enterprise Electronic Services
- **7100** Administrative Data Management and Access Policy
- **7200** University IT Security Program
- **7205** IT Infrastructure, Architecture and Ongoing Operations
- **7210** IT Project Management
- **7215** IT Accessibility

or visit [www.it.vt.edu](http://www.it.vt.edu)
Protect Your Data
Know Your Data!

• What is sensitive data?
  – Social Security Numbers, Medical Records, Student Grades, Human Research material (IRB approved), Credit Card Numbers, etc.

• What are the risks to my data?
  – Information theft and fraud
  – Deletion and changing of information
  – Unintentional exposures and misuses
Finding Your Secure Data

So where is your data at?

• Use the PII Search tools
  – Find SSN and Find CCN, Cornell Spider, UT-Austin SENF, IdentityFinder

• These tools find Social Security Numbers and Credit Card Numbers on your machine

• Watch out for false positives!
Data Protection Solutions

- **Encryption**
  - Best way to secure data, converts data into unreadable form
  - Use True Crypt [www.truecrypt.org](http://www.truecrypt.org)
  - Consider using Microsoft Rights Management Service
  - Consider using commercial products like PGP Netshare, Credant, etc.
  - Full Disk Encryption (FDE) isn’t the best solution!

- **SSL**
  - Make sure all interactions are done over a secure network (e.g. https)

- **Back up your data and store in a secure location**
Protect Your Machine
First Line of Defense

• Make sure of the following:
  – Firewall is turned on
  – Turn on Windows Update if it is off
  – Install Antivirus if it isn’t installed
  – Install the root certificates
Physical Security

• Don’t assume physical security!!
• Key component is location and accessibility of computers
• Keep areas locked when necessary and consider restricted access
• Laptops and PDAs require additional security measures – especially if those devices contain confidential data
• Disable Auto-Logon on any computers
Wireless Security

- **Always use encryption when sending sensitive data**
  - Make sure website is secure (e.g. https)
  - Use Webmail/Outlook/Eudora for e-mail transmissions

- **Use encryption tool to encrypt files or folders**
  - For example, use True Crypt to encrypt data being sent

- **Use Secure wireless networks**

- **Make sure connection is the real deal**
  - Is Mcdonalds1234 the real McDonalds wireless network?
Using Secure Web Sites

Make sure the website you are using is https and shows a lock in the lower right corner before any sort of transaction.

Simply put, you don’t want your personal or confidential information broadcast to the world for all to see, especially important on wireless.
Change Your Password

• All PID, HOKIES, Oracle/Banner passwords must be changed by 6/30/11

• Why?
  – Because they haven’t been changed in some cases for at least 10 years
  – Easy to guess
  – New password strength rules in effect
Password Management

• DON’T SHARE YOUR PASSWORD!

• If a person does something malicious while logged on as you, it will likely be credited to you

• If you think someone knows your password – CHANGE IT!
Selecting Good Passwords

• Don’t use any actual word or name in ANY language.

• Don’t use consecutive letters or numbers (abcdefg) or adjacent keys on the keyboard (qwerty).

• Using the first letter: “Pay no attention to the man behind the curtain,” becomes the password – PnAttMBtC
  – A special event: “I went to Ft. Lauderdale in 85!” becomes IwtF.Li85! or use the last letter and reverse caps for iTOT.eN85!

• Football might become F00t8a77 or sneakers might be 5n3ak3r5.
Social Networking

What is Social Networking?

• Social Networking – Facebook, Myspace, Second Life, etc.

Good and Bad

• The good things:
  – Keep in touch with colleagues at a distance
  – Useful in distance classes
  – Find others with your interests or peers in your field

• The bad things:
  – Can be used to harvest personal information
  – Difficult to remove the information when you no longer want it displayed
  – Employers are using it for references more frequently
Social Engineering

- **Social engineering** is the practice of obtaining confidential information by manipulation of legitimate users
  - Impersonation of a user to gain physical access to a machine or data.
  - Gain information to customize a phishing email
Phishing

Be aware of unexpected email, messages, and attachments.

No legitimate business will ever ask for your credentials by email!
Resources and Contact Information
Helpful Sites

VA Tech IT Security Office and Lab Homepage
www.security.vt.edu
Contact Information

IT Security Office and IT Security Lab
1300 Torgersen Hall
Randy Marchany – marchany@vt.edu

IT Security Homepage  www.security.vt.edu