Computer and Data Security for PCs and People

Cyber Security Presentation
Cyber Security Month
Curtis McNay, Director of IT Security
# The IT Security Office (ITSO)

## What We Do?

<table>
<thead>
<tr>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Network and System Security Monitoring</td>
</tr>
<tr>
<td>Vulnerability Scanning and Penetration Testing</td>
</tr>
<tr>
<td>Enterprise Encryption Solution</td>
</tr>
<tr>
<td>Computer Incident Response</td>
</tr>
<tr>
<td>Computing, Network and Data Policy Compliance</td>
</tr>
<tr>
<td>Awareness Training</td>
</tr>
</tbody>
</table>
What Is The Threat

- **Who are the Hackers**
  - Sophisticated criminal organizations in China, Eastern Europe, Russia, Asia and elsewhere.
  - State Sponsored Industrial or governmental espionage – China, Russia, Iran, North Korea, Etc.
  - Someone who has taken a personal interest in you
  - Property thieves

- **What Motivates Hackers**
  - Financial gain from using or selling your data
  - Using your PC to attack others
  - Industrial or governmental espionage
  - Occasionally the motivation is personal
  - For physical theft the motivation can be data theft and resale of hardware
How and Why

How Do They Do It

• Exploiting Human Behavior
• Exploiting System Vulnerability
• For Mobile Devices - Physical Theft

What are They After

• Data: CC#s, SSN#s, ID Theft, Banking Info, Contact Lists
• Access: Your work, financial, social, cloud storage accounts
• Malicious use of your computer: To target someone else.
• The Hardware: For it’s resale value.
Statistics

- About 63% involve exploits of user account
  [http://www.channelbiz.co.uk/2012/06/12/internal-security-breaches-cause-businesses-most-concern/](http://www.channelbiz.co.uk/2012/06/12/internal-security-breaches-cause-businesses-most-concern/)

- Worldwide about 23% of people will respond to spear-phishing attacks, with 70% of people responding to directed phishing attacks
More Statistics

- 96% of all data breaches were not technically difficult
- 97% were avoidable through simple or intermediate controls
- 69% incorporated malware
- 81% of incidents used a form of hacking (through phishing, drive-by downloads, etc)
- 79% of victims were targets of opportunity

From( http://www.verizonbusiness.com/about/events/2012dbir/ ):
Something Old.. Zeus

- Steals confidential information
  - Online credentials
  - Banking data
  - Can be customized for specific data targets
- Malware package is generated via a tool kit that sold in markets for online criminals
- Typically distributed via an email with a link to malicious website for distribution
- Bot controlled...and is waiting for the next command.
Something new….Crypto Locker

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Foreign Attacks- Week of 7/14

Foreign Sources of Attacks - Top 20, Week of July 14, 2013
Protecting Highly Sensitive Data

- Do not store HSD on your PC unless you have requested to do so and its been approved by Chief Data Steward.
- Understand how to securely delete data
- Do not transmit highly sensitive data unencrypted. (HTTP, Email, FTP. Removable media)
- Be aware of legacy data and do regular housekeeping
- Read and understand the Data Stewardship policy #1114([http://universitypolicy.gmu.edu/policies/data-stewardship/](http://universitypolicy.gmu.edu/policies/data-stewardship/))
# Highly Sensitive Data

<table>
<thead>
<tr>
<th>Identity Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security number</td>
</tr>
<tr>
<td>Driver’s license</td>
</tr>
<tr>
<td>Background checks</td>
</tr>
<tr>
<td>Health Data (HIPAA)</td>
</tr>
</tbody>
</table>
### Other Highly Sensitive Data

#### Access Control & Technology Information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords/PINs</td>
<td>Encryption Keys</td>
</tr>
<tr>
<td>Network/System Info</td>
<td>Security Configuration Info</td>
</tr>
</tbody>
</table>

#### Financial data

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Numbers</td>
<td>Financial aid/scholarship info</td>
</tr>
<tr>
<td>Bank Account Info</td>
<td>Personal Tax return data</td>
</tr>
</tbody>
</table>
Mitigating Risk: What Can You Do

- Use Current OS - Window 7 or latest Mac OSX build
  - 64 bit is better

- Install a comprehensive Host-Based Security Suite
  - Firewall, Host Intrusion Prevent, and Antivirus

- Configure Web Browsers for Safe Browsing
  - No Scripts, Manage plugins

- Keep everything updated

- Manage your passwords
More Security Tips

- Don’t store highly sensitive data on your computer.
  - Store offline and locked up and/or encrypted

- Limit Use of the Administrator Account-
  - Create a standard user account and use it for most of what you do.

- Become sophisticated about web browsing and email security

- For your mobile devices pay attention to physical security.
Password Management

- Use a secure password
  - Length first, then complexity
    - At least 10 characters, consider pass phrases
    - Mixed alphanumeric, upper/lower and special characters
- Periodically change your passwords
- Use a password safe to store your passwords
- Use different passwords for different accounts
  - Mitigates threat of chained attacks
Understand Phishing

- What is phishing?
  - Phishing is a form of social engineering that uses e-mail or malicious websites to solicit personal information by posing as a trustworthy organization.

- What does a phishing email look like?
  - False Sense Of Urgency
  - Suspicious-Looking Links
  - Not personalized
  - Misspeld or Pooooorly Written
  - Sender not known
We've noticed some unusual activity in your gmu.edu. To help protect you and everyone else, we've temporarily blocked your account. To unblock it, verify your account. By clicking on the link below or copy and paste the link on your web browser.


Please you have to login for the verification of your account.

Your email account will be terminated if you have not verified your email account.

Failure to do this your email account will be suspended fully.
Phishing (cont’d)

- What can happen?
  - Phishing Attacks Lead to Identity Theft - When users respond with the requested information, attackers can use it to:
    - Empty your bank account
    - Open new credit cards
    - Gain employment
  - Specific to Mason, Malicious access to:
    - Patriotweb/Internet Native Banner
    - Student/Employee Personal information
    - Financial information
    - Mason Money
    - MyMason
Web Browser Security

- Understand what risky behavior is
  - What is an untrusted web site
  - Don’t click that button - FakeAV
  - Downloading plugins and add-ons without consideration.

- Learn how to secure your internet browser
  - Disable/Uninstall unused plugins
  - Keep necessary plugins patched
    - 40% of drive-by-downloads exploit unpatched vulnerabilities in Adobe Flash and PDF reader
  - Disable Java, JavaScript and ActiveX
    - Or, for browsers that support it, enable for web sites that you trust
FireFox Security Settings

1. Select Tools
2. Then, Select Add-ons.
Select Extensions.

Then, Search for "NOSCRIP"T."
Firefox - Installing NoScript

Select “Install” for “NoScript”.

NoScript 2.5.7
The best security you can get in a web browser! Allow active content to run only from...

Download Flash and Video 1.17
Download Flash and Video is a great download helper tool that lets you download FI...

RequestPolicy 0.5.27
Be in control of which cross-site requests are allowed. Improve the privacy of your b...

QuickJava 1.8.0
Allows quick enable and disable of Java, Javascript, Cookies, Image Animations, Flash...
Firefox- NoScript Install Confirmed

Restart Firefox and it’s installed!
FireFox – What Success Looks like
Options for controlling scripts
Select Tools

Select Internet Options
Trusted Sites

- Trusted sites
- Medium Setting
- High Setting

Internet

- Internet
- Medium Setting
- High Setting
Unpredictable Behavior

Site was in “Trusted list”. Imbedded content was from another site
IE – Privacy Settings

Settings Level

Privacy Access For individual Sites
Other IE Security Settings

Select Safety

ActiveX, SmartScreen and other controls

Access Configuration
Chrome Security Settings

1. Access Controls

2. Select Tools
Chrome - Managing Extensions

Select get more extensions
Chrome - Installing NotScripts

Search for “NotScripts”

Select “Add to Chrome” for NotScripts for Crome OS
Chrome-NotScripts: Instructions to Set Password

Setting your NotScripts password is simple ?. Simply follow these steps:

Step 1: Navigate to the NotScripts Folder
Open the NotScripts Google Chrome extension folder. The location of this folder is shown below. You can go there by directly copying and pasting the appropriate address below into the location bar of a folder:

Windows XP: %userprofile%\Local Settings\Application Data\Google\Chrome\User Data \Default\Extensions\odjhifogjcknibkahlpidmdajjppkkcfn
Windows Vista or 7: %userprofile%\AppData\Local\Google\Chrome\User Data\Default \Extensions\odjhifogjcknibkahlpidmdajjppkkcfn
Mac OS X: ~/Library/Application Support/Google/Chrome/Default/Extensions/ odjhifogjcknibkahlpidmdajjppkkcfn
Linux: ~/.config/google-chrome/Default/Extensions/odjhifogjcknibkahlpidmdajjppkkcfn

Note: For Windows users, change YOUR_USER_NAME to the user name to you are logged onto under Windows. If you're using Windows Explorer to navigate to the folder, you might need to set Show hidden files and folders in Tools > Folder Options... > View.

For convenience, it is recommended that you make a shortcut to this folder on your desktop or somewhere handy so that you can quickly reset the NotScripts password after an update.
Chrome – NotScripts Install
Simple Steps? Continued...

**Step 2: Open the NotScripts Password File**
Open the file `CHANGE__PASSWORD__HERE.js` for editing. For Windows users, do this by right-clicking on the file and selecting *Edit* from the right-click menu. This will open up the file in NotePad for you to enter your NotScripts password.

**Step 3: Set the NotScripts Password**
Choose a password for NotScripts with the following restrictions:
- **Length:** 20 minimum, 100 maximum
- **Allowed Characters:** `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_1234567890`  
- **Spaces:** Allowed

Put the password in between the quotes of the line that reads:

```javascript
const ENCRYPTION_PASSWORD = "";
```

Example: `FNqzJmJBA1GQFhuXBmEqz20MqEqbn55w3MtT`
It should look like this after (except with your own password):

```javascript
const ENCRYPTION_PASSWORD = "FNqzJmJBA1GQFhuXBmEqz20MqEqbn55w3MtT";
```

Save the file and close it when finished.

**Step 4: Restart Google Chrome**
Close and restart Google Chrome for the new password to take effect in NotScripts. You are done!
Chrome - What Success Looks Like

Success!

Manage scripts for each site
Safari Security Settings

Web content:
- Enable plug-ins
- Enable Java
- Enable JavaScript
- Block pop-up windows

Accept cookies:
- Always
- Never
- Only from sites you navigate to
  For example, not from advertisers on those sites.

Default database maximum size: 5 MB

Ask before sending a non-secure form to a secure website
Managing User Accounts

- Consider creating and using an account with limited privileges instead of an 'administrator' or 'root' level account for everyday tasks.
- Depending on the operating system, administrator level access is only needed when installing new software, changing system configurations, etc.
- Malware (e.g., viruses, Trojan horses) is executed with the privileges of the user that runs them —making it far more risky to be logged in as an administrator all the time.
- A default user account does not have the permissions to install malware or make system changes.
Managing your Windows PC

Find “Computer”

Select Manage
Managing Users and Groups

Find Local Users and Groups
Adding a New User

Right Click on Users and Select "New User"
Account Creation

Fill it out. Use a strong password

Select Create
“New User” in users group
Elevating Your Permissions

When logged on as “NewUser” select an application, right click and choose “Run as administrator”