Cyber crime effects Education - How can we be ready?

Data Collections Conference 2013
Do you hear the warning?
What do Hackers look Like?!
**Cyber Threats!!!**

### ThreatStats
Six million Facebook users may have had their personal data exposed

<table>
<thead>
<tr>
<th>Malware</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail &amp; wholesale</td>
<td>152%</td>
</tr>
<tr>
<td>Education</td>
<td>124%</td>
</tr>
<tr>
<td>Health care</td>
<td>92%</td>
</tr>
<tr>
<td>IT &amp; telecommunications</td>
<td>72%</td>
</tr>
<tr>
<td>Food &amp; beverage</td>
<td>68%</td>
</tr>
<tr>
<td>Banking &amp; finance</td>
<td>56%</td>
</tr>
<tr>
<td>Government</td>
<td>36%</td>
</tr>
</tbody>
</table>

### Top breaches in June

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>Facebook discovered a bug that may have allowed unauthorized users to view the personal contact information of Facebook members.</td>
</tr>
<tr>
<td>Florida Dept. of Education</td>
<td>The personal information of Florida teachers was publicly accessible for 14 days after a data transfer at Florida State University.</td>
</tr>
<tr>
<td>Champlain College</td>
<td>During the weekend of June 3, a hard drive – left unattended in a computer lab for about two days in March – was discovered to have been misplaced.</td>
</tr>
</tbody>
</table>

The chart above reflects the encounter rate in June of web malware across a selection of industry verticals. Rates above 100 percent reflect a higher-than-median rate of encounter; and rates below 100 percent reflect a lower-than-median rate.

### Index of cyber security

**Perceived risk**

- Rate of change (continuously compounded)
- Same value

**Total number of records containing sensitive personal information involved in breaches in the U.S. since January 2005:**

608,278,176 (as of July 15)

Source: Privacy Rights Clearinghouse (data from a service provided by DatatreasuryDB.org, hosted by the Open Security Foundation)
Dr. John D. Barge, State School Superintendent
“Making Education Work for All Georgians”
www.gadoe.org
“Improved” Phishing

• Phishers often use legitimate sites to host their phishing pages. This quarter saw evidence of a further method used by phishers to cut costs and streamline the phishing process. The following stages are involved in a traditional phishing attack:

• 1. Create the phishing page – either hidden within a legitimate site or hosted on some temporary server.
• 2. Send out carefully socially engineered phishing emails including the link to the phishing page.
• 3. Collect data submitted to the page by deceived recipients. In the attack shown below this stage is streamlined.
HomeAway holiday rentals.
Spam Topics

- Pharmacy, 28.0%
- 419 fraud, 13.0%
- Dating, 12.0%
- Enhancers, 10.0%
- Pornography, 6.0%
- Software, 4.0%
- Phishing, 3.0%
- Replicas, 2.5%
- Weight Loss, 1.5%
- Degrees, 2.0%
- Other, 18.0%
Valentine’s spam

- February brought along typical outbreaks of Valentine’s Day spam. In fact Valentine’s themed subjects had already started appearing in late January. The subjects ranged from dating to replicas to fast cash offers – some examples:
  - happy st valentine™s with mydatelab.com!
  - valentine day sale now on
  - the best valentines gifts
  - valentine day jewelry sale
  - valentine’s day gift! 50% off on water resistant wrist watch
  - need cash for valentine’s?
  - save 25% on valentine’s day flowers

Destination sites were suitably dressed for the occasion.
When is Spam worse?

- Spear phishing attacks increase when enterprise security operations centers are lightly staffed or understaffed, particularly during holidays. The figure below illustrates the daily count of malicious email attachments identified by the FireEye Email MPS appliances across our entire US-based customers. These levels reflect the daily count of incoming malicious attachments that were able to successfully evade initial SPAM and AV filters, as they arrived from outside the target organization.
When is Spam worse?

Figure 6: 2H 2011 malicious email attachments by relative volume

Dr. John D. Barge, State School Superintendent
“Making Education Work for All Georgians”
www.gadoe.org
Where are you Conficker?
What can we do?

Defense in Depth

- Anti-Virus
- Anti-Spyware
- Encrypted Communication
- Session Controls
- Host
- Strong Passwords
- Application
- Physical Security
- Data
- Limit Use of “Privileged” Accounts
- OS and App Patches

Dr. John D. Barge, State School Superintendent
“Making Education Work for All Georgians”
www.gadoe.org
What can we do?

• **Defense in Depth or Layers of Defense**

• **Equate this to home security** - My house (front wall with a gate, security iron on windows and doors, a large dog, 2 locks on door)

• Versus My neighbor (No wall or gates in front, No security Iron and oh yeah and let’s not forget their Chihuahua)

• Which house would a thief be more likely to break into?

• If you have some (ideally all) of these measures in place (personal firewall, anti-virus, up to date software, strong passwords as well as education in now knowing that you really can’t trust everything you get via email) versus someone that does not have security practices, who is more likely to have their computer compromised?

• It’s not that they absolutely can’t get in - it will just take more time and effort.
Where is the Weakest point?
Where is the Weakest Point?
What can we do?

- **Passwords**
  - Strong
  - Not Shared
  - Storage

- **Accounts**
  - Limit use of Privileged Accounts

- **Session Controls**
  - Password protected screensaver
  - Ctrl-Alt Delete (enter) or Windows L
What can we do?

• We are the weakest point on our computer networks. It is up to us to guard our computers, data and children.

• Passwords.....if I could get you to think differently about one thing today it would be to have a better understanding as to the importance of creating (AND NOT SHARING) a strong password. A password is essentially the last layer of defense to your computer and personal information. You can have every other safeguard in place, if someone gets your password they are now able to access the information.
What can we do?

Other Ways to Protect Your PC

- Back up your files regularly
- Think before you click
- Read website privacy statements
- Close pop-ups using red “X”
What can we do?

Surf “safer” w/ SiteAdvisor

Free Software Foundation of India | Why we leave our own code. Together.
Free Software Foundation - India. The FSF’s goal is to ensure the long term adoption of free software, and aim for the day when all software will be free.
fsf.org.in/ - 16k - Cached - Similar pages

Why Open Source Software / Free Software (OSS/FS, FOSS, or FLOSS...)
This paper provides quantitative data that, in many cases, open source software / free software is equal to or superior to their proprietary competition.
www.dwheeler.com/oss_fs_why.html - 690k - Cached - Similar pages

Freeware / Download Free Software / New Freeware - Today
Freeware downloads, we only list the top 15 in each category so as to guarantee that only the best software is listed. Download the likes of Firefox, ...
www.freesoftware4all.co.uk/ - 45k - Cached - Similar pages

Free Statistical Software
A large collection of links to interactive web pages that perform statistical calculations.
statpages.org/javasta2.html - 120k - Cached - Similar pages

WinSite Freeware Selections
We rely on our software submitters to properly label their software, so if you find a program in this area that is not free, please contact us giving the ...
www.winsite.com/free/ - 24k - Feb 20, 2007 - Cached - Similar pages

free statistical software
StatSci list of free software http://www.statsci.org/free.html also lists some ... communication on developments, plans, infos on free GIS software and free ...
gsocology.icaap.org/methods/soft.html - 48k - Cached - Similar pages

Freeware Pro / Free Software Downloads
Freeware Pro, a collection of free software downloads for Windows that doesn’t include trials or spyware.
www.freewarepro.com/ - 22k - Cached - Similar pages
What can we do?

Think Before You Click

- Don’t open e-mail attachments unless you know what they contain and who sent them
- Only download files from websites you trust
What can we do?

Close Pop-ups Using Red “X”

- Always use the red “X” in the corner of a pop-up screen.
- Never click “yes,” “accept” or even “cancel”, because it could be a trick that installs software on your PC.
New Tech for New World

Key safe enablement requirements:

- **Identify applications, not ports.** Classify traffic, as soon as it hits the firewall, to determine the application identity, irrespective of protocol, encryption, or evasive tactic. Then use that identity as the basis for all security policies.

- **Tie application usage to user identity, not IP address, regardless of location or device.** Employ user and group information from enterprise directories and other user stores to deploy consistent enablement policies for all your users, regardless of location or device.

- **Protest against all threats—both known and unknown.** Prevent known vulnerability exploits, malware, spyware, malicious URLs while analyzing traffic for, and automatically delivering protection against highly targeted and previously unknown malware.

- **Simplify policy management.** Safely enable applications and reduce administrative efforts with easy-to-use graphical tools, a unified policy editor, templates, and device groups.

Safe application enablement policies can help you improve your security posture, regardless of the deployment location. At the perimeter, you can reduce your threat footprint by blocking a wide range of unwanted applications and then inspecting the allowed applications for threats—both known and unknown. In the datacenter—traditional or virtualized, application enablement translates to ensuring only datacenter applications are in use by authorized users, protecting the content from threats and addressing security challenges introduced by the dynamic nature of the virtual infrastructure. Your enterprise branch offices and remote users can be protected by the same set of enablement policies deployed at the headquarters location, thereby ensuring policy consistency.
App Control
Take Steps to Help Protect *Information*

1. Practice Internet behavior that lowers your risk
2. Manage your business information carefully
3. Use technology to reduce nuisances, and raise the alarm when appropriate