Is it Safe to Click?

Staff Association Council

Sean Sweeney, Information Security Officer
March 13, 2014
Agenda

- We are targets!
- Who are we up against?
- What are we up against?
- What can YOU do about it?
We Are Targets!
University = Target-rich Environment

- Size and speed of network
- Collaborative nature of research—open access
- Diverse information-rich environment
- Fluid user population
Higher Education Breaches

Hacker accesses UF dental patient data

Data breach at Indiana University may affect 146,000 students
Top Ten Higher Education Breaches

- University of California Los Angeles – 800,000 (2006)
- Ohio State University – 750,000 (2010)
- University of Nebraska – 654,000 (2012)
- University of North Carolina, Charlotte – 350,000 (2012)
- University of Florida College of Dentistry – 330,000 (2008)
- University of Maryland – 309,079 (2014)
- Arizona State University – 300,000 (2012)
- Ohio University – 300,000 (2006)
- Northwest Florida State College – 279,000 (2012)
- University of North Carolina, Chapel Hill – 236,000 (2009)
By Type

Throughout the past eight years, hackings and malware have caused nearly a third of all educational data breaches.

- 219 Breaches: Hacking or Malware
- 198 Breaches: Unintended Disclosure
- 123 Breaches: Portable Device
- 52 Breaches: Physical Loss
- 47 Breaches: Stationary Device
- 21 Breaches: Insider
- 12 Breaches: Unknown or Other
- 1 Breach: Payment Card Fraud
Threats to Pitt

• Failure to adhere to established policies and guidelines
• Increased spear phishing
• Malware Attacks
• Web Application Attacks
• Mobile Threats
• The Unknown
Who Are We Up Against?
Who Are These People?

- Organized Crime
- Script Kiddies
- Terrorist
- Hacktivist
- Nation States
What Are We Up Against?
Compromised Credentials

1. NYTimes.com
Targeted Malware
Spear Phishing
Social Engineering via Facebook

OMG  OMG  OMG... I can't believe this actually works! Now you really can see who viewed your profile! on http://bit.ly/WatcherR
about a minute ago via Privacy+

OMG  OMG  OMG... I can't believe this actually works! Now you really can see who viewed your profile! on http://bit.ly/MyProfile
4 minutes ago via ePrivacy

OMG  OMG  OMG... I can't believe this actually works! Now you really can see who viewed your profile! on http://bit.ly/WatcherR
7 minutes ago via Privacy+

OMG  OMG  OMG... I can't believe this actually works! Now you really can see who viewed your profile! on http://bit.ly/WatcherR
14 minutes ago via Privacy+

yes
I need your help?
sure... what can I do?

Our return flight leaves in a few hours to this time and we are having a problem in sorting the hotel bill and get a cab down to the airport.
Wondering if you can loan me some few $$$ I promise to refund it back to you as soon as we get back home tomorrow

Absolutely.
How can I get the money to you?
One Ring Scam
Iframe Vulnerability

1. User with vulnerable computer visits compromised Web page with invisible Iframe
2. Iframe embedded in page secretly loads another page
3. The page redirects to another page containing an exploit
4. If the exploit succeeds, malware downloads from another server to the victim’s computer
HTML Injection

```html
set_url https://online.wellsfargo.com/login GP
<input type="password" name="password"/>
3. ATM PIN
<input type="password" name="uspass" id="atmpin" size="20" maxlength="14" title="Enter ATM PIN" labindex="11" accesskey="A"/>
</table><tr>data_end
```
What Can YOU Do About It?
Defense in Depth
Educate Yourself: Be Skeptical

http://www.iamaboutohackyou.net/
Ctrl+Click to follow link

WWW.PITT.EDU
Install Symantec Endpoint Protection
Update, Update, Update

Software update

Status
Phone number, signal, etc.

Battery use
What has been using the battery

Legal information

Model number
LG-P920

Android version
2.2.2

Baseband version
L6260_MODEM_SIC_01.1042.00

Kernel version
Choose and Use Strong Passwords

<table>
<thead>
<tr>
<th>Weak</th>
<th>Medium</th>
<th>Strong</th>
</tr>
</thead>
<tbody>
<tr>
<td>All numbers or all letters</td>
<td>Alphanumeric</td>
<td>Alphanumeric with a mix of upper and lower case letters</td>
</tr>
<tr>
<td>beckeriscool</td>
<td>becker2cool</td>
<td>B3cker2C00l</td>
</tr>
</tbody>
</table>
Use SecureZip
Identify Sensitive Data
Avoid Suspicious Websites

Ad related to seattle housing authority

Apply For Section 8 - Section 8 Housing Vouchers.
www.housing-voucher.com/
Learn how to get Section 8 Online.

Seattle Housing Authority - Rental housing and rental assistance for ...
www.seattlehousing.org/ Share

Seattle Housing Authority provides long-term rental housing and rental assistance to more than 26,000 people with low incomes. Learn more. We do not provide ...
1 Google review - Write a review

800 Jefferson St Seattle, WA 98104
(206) 223-5357

Housing
Seattle Housing Authority provides housing assistance to more ...

Jobs
Job Programs - Section 3
Employment - Open Enrollment
Keep Your Laptop Secure
Contact Us!

• Call: 412-624-HELP
• Email: helpdesk@pitt.edu
• Visit: technology.pitt.edu
Questions?
Thank You!