IT SECURITY

Protecting Your Systems on Campus

Engineering IT Brownbag Series
27 October, 2015

Brian Lee
Associate
IT Specialist

Palmer Buss
IT Specialist

Mark Smylie Hart
Research Technology Facilitator
WHAT WE’LL COVER TODAY

• Why security is important
• Cautionary tales from our peers
• The **DO’s** and **DON’Ts** of computer security
• Phishing and Social Engineering
• Best practices for online safety
WHY IS SECURITY IMPORTANT

Everything you touch, touches everything

SERVER

INTERNET

COMPUTERS
WHY IS SECURITY IMPORTANT

• It doesn’t take much to gain access and cause trouble

• Bad guys are smarter
  – Stealing login info
  – Ransomware
  – Fake AV software
  – Banking

SEVERAL PEOPLE ARE SCANNING US RIGHT NOW!
You’re never more than 10 feet from a spider at any time.

-howstuffworks.com
LET’S NOT BE PENN STATE

• College of Engineering had a massive breach

• Detected 11/2014, but likely there since 9/2012
  – 18,000 individuals notified
  – No evidence of data theft

• PSU Engineering ‘went dark’ for several days
  – Ended up doing a re-install of ALL systems
  – 20,000 Man-hours to recover systems
LET’S NOT BE PENN STATE

“Engineering faculty, staff and students will need to learn to work under new and stricter computer security protocols...and all of us will need to change the way we operate in the face of these new and significant challenges.”

- PSU Pres. Eric Barron
LET’S NOT BE UCONN

• College of Engineering had a massive breach
  – Sound familiar?

• Detected 3/2015, but likely there since 9/2013
  – Roughly 2,000 users assisted with ID Protection
  – No evidence of data theft

• UCONN had to notify roughly 200 research project sponsors in Gov’t and private industry
LET’S NOT BE UCONN

“The unfortunate reality is that these types of attacks are becoming more and more common, which requires us to be even more vigilant in protecting our University community.”

- UCONN CIO and Vice Provost Michael Mundrane
Let’s Not Be These Guys Either

- Ohio State – 2010
  - 750,000 Names, DOB’s and SSN’s compromised
- Virginia – 2013
  - 18,000 valid SSN’s auto-filled and mailed out
- Maryland - 2014
  - 310,000 names, DOB’s and SSN’s compromised
LET’S BE US
WHY IS SECURITY IMPORTANT

Everything you touch, touches everything

SERVER

INTERNET

COMPUTERS
DO’s and DON’Ts
DO LOCK YOUR DEVICE

• Just a few minutes away are enough to:
  – Send email from your account
  – Tamper with and delete your files
  – Access and download confidential data

• 🗝️ + L to lock Windows machines
HOW TO LOCK YOUR MAC
DON’T SHARE YOUR PASSWORD

A password is like a toothbrush

Choose a good one

Don't share it with anyone

Change it occasionally
DON’T SAVE YOUR PASSWORD
DON’T SAVE YOUR PASSWORD
This includes writing it down on a sticky note
DO USE MULTIPLE PASSWORDS

"my_awesome_password234"
DON’T CLICK ON SUSPICIOUS LINKS

• Be careful what you click
• Never click on things unless you are certain of the source.
• Phishing emails typically hide the actual URL by displaying a different URL.
DO KNOW THE SOURCE

- Know where everything comes from
- Verify the URL of links.
  - Verify the underlying link to the URL is the same
- Don’t click on emails from unfamiliar senders.
  - Verify that known senders have not been hacked after receiving suspicious emails.
1. **Forged URL.** Even though the name "eBay" appears in the domain name, it's not the real site.

2. **No "https".** The real eBay login page will always use "https" indicating a secure login.

3. **Different font and design elements from the real eBay login screen.**

4. **Low graphic resolution.**
1 Forged URL.
Although this domain uses “https” it is clearly not a Yahoo! domain.

2 Poor grammar.
Unclear and grammatically incorrect text on a page is usually a clear giveaway of a phish.

3 Scare tactics.
It’s highly unlikely your email provider will delete your account due to “congestions.”

This Email is from Yahoo! Customer Care and we are sending it to every Yahoo! Email User Accounts Owner for safety. We are having congestions due to the anonymous registration of Yahoo! accounts so we are shutting down some Yahoo! accounts and your account was among those to be deleted. We are send this email to you so that you can verify and let us know if you still want to use this account. If you are still interested please confirm your account, click bellow to verify your mail
* Required
DO KNOW THE SOURCE (Downloads)

• Verify the URL of links.
  – Verify the underlying link to the URL is the same

• Make sure your download is what you want.

• Verify the extension (.jpg, .zip, etc.) of the file is correct.
  – Be extra careful with .exe files
DO RUN ANTI-MALWARE
DO KNOW YOUR WI-FI
DO KNOW WHAT ‘NORMAL’ IS
DO

ASK QUESTIONS
PHISHING

I have emailed everyone I can possibly find, my Prince, but no-one wants to help you move your money.
PHISHING ON CAMPUS

Subject: RE: HELP-DESK

To All Faculty\Staff
We currently upgraded to Saver to 50GB inbox space. Please log-in to your user account to validate E-space. Your emails won't be delivered by our server, unless email account is confirmed.

protecting your email account is our primary concern, for account update (Web Mail) click on Outlook Web Access
should you have any questions please contact the IT Helpdesk.

Copyright ©2015 ITS Help Desk.
BEST PRACTICES TO AVOID FALLING FOR PHISHING

• Ask questions
  – If you’re not sure about an email ask your local IT professional if it is legitimate.
• Pay attention to where the email came from.
• Pay attention to where links are taking you.
• Don’t share your password.
• Report phishing and spam emails to report-spam@illinois.edu
SOCIAL ENGINEERING
SOCIAL ENGINEERING

Security Questions

What is the name of your childhood pet?
Snuffles

What is your mother’s maiden name?
Armitage
<table>
<thead>
<tr>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Overview: Engineering IT &amp; Campus</td>
<td></td>
<td>Research IT Support Contracts and You!</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Using Skype for Business</td>
<td></td>
<td>Purchasing: Hardware and Software</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Using Outlook to Manage Email and Calendaring</td>
<td></td>
<td>File Service: Options, Backups and Best Practices*</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>IT Security: Protecting Your Systems on Campus</td>
<td></td>
<td>Introduction to Cluster Computing</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Wireless Networking Clinic</td>
<td></td>
<td>Research Group Access Control: Using the Portal Groups Tool*</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Engineering Managed Linux Environment</td>
<td></td>
<td>No Brown Bag</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Data Center Shared Services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* will be in Deere Pavilion, MEL