IT Forum on Cyber Security
Information Security Office

by

Calvin A. Krzywiec, CCNP, CCDA
Interim Director, Information Security

Ikram Muhammad, CISSP, PMP, CCNA, CEH
Information Security Engineer
Topics

• Information Security and its Importance
• Cyber Security vs Safety
• Malware
• Phishing/Examples
• Whaling and Spear Phishing/Examples
• Security Alerts and Notifications
• Online Safety tips
• Data Classification and Handling
• Additional Resources
• Questions
Information Security

- What is Information Security
  - The protection of information systems against unauthorized access to or modification of information.
  - The preservation of confidentiality, integrity, and availability of information
Information Security Services

- We are here for you!
- Protection:
  - Develop and coordinate policies and procedures
  - Consultation – best practices, data security, compliance
  - Policy Interpretation
  - Contract review – work closely with General Counsel
  - Technical security controls – Intrusion prevention
  - Vulnerability reporting
- Detection:
  - Monitoring – Intrusion detection
- Response:
  - Incident response
  - Forensic readiness
  - Policy violations – Copyright / AUP
  - Investigations – partner with UPD
Why is this important?

• Universities have lots of Personally Identifiable Information (PII) – SSNs, Drivers License, Financial Records, Credit Cards
  – Increasingly targeted by malicious actors – identity theft
• Laws and Regulations require protection of data
  – State data breach laws – PA SB 712
  – Federal regulations – FERPA
  – Industry regulations – PCI DSS
• Data Breach can result in:
  – Reputational impact - Compromised confidence of donors, alumni and parents; loss of business
  – Financial impact – fines, cost of recovery
  – Legal penalties
  – Service interruptions
HigherEd Data Breach Stats (2015)

- 22% Unintended Disclosure
- 14% Portable Device Lost/Stolen
- 12% Physical Loss
- 35% Hack or Malware (on the rise)
  - Phishing, Ransomware
- 8% Insider
- 9% Other

- Data breaches in Higher Ed up 50% since 2014
- Recovery costs per record rising: $300

- Source: Beazley Cyber Crisis Workshop – 4/2016
You are the key!

• 22% **Unintended Disclosure**
• 35% Hack or **Malware** (on the rise)

• Data security is a shared responsibility
• Technical controls aplenty…
  – Firewalls, Intrusion Prevention, Intrustion Detection, Reputational/Signature/Behavioral threat feeds, Antivirus, Privilege Management Software, Encryption, Email filters...

• **You are the last line of defense**

Division of Planning and Information Resources
Cyber Security vs Safety

**Cyber Security**: We must protect our computers and data in the same way that we secure the doors to our homes.

**Safety**: We must behave in ways that protect us against risks and threats that come with technology.

- Strong Password/Pass phrases
- Trust but verify
Importance of Security

- The internet allows an attacker to attack from anywhere in the Universe
Malware

What is it?

- Malware short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Types of Malware:
- Viruses, Adware, Spyware, Browser hijacking software

What is the risk?

- Restricted information is gathered and transmitted to interested parties.
- Encrypting your files so you cannot access them.

How does malware get through?

- Malware gets bundled with other software that you download
- Peer to Peer File Sharing
- Links in emails
- Malicious websites, Malware can exploit security holes in your browser as a way of invading your machine

Division of Planning and Information Resources
Malware

What are we doing to stop it?

• We have Microsoft Windows Defender for antivirus.
• Local admin access has been removed for Win7 machines.
• We have ViewFinity to help protect installation of software.
• Our IDS/IPS block known malicious sites.
• We quarantine machines that are infected to prevent the spread of malware.
• Our Technology Support Center scan machines that are infected to ensure malware is removed properly.
Phishing

• What is Phishing?
  – **Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity.
Phishing Example 1

Example 1
Subject: HELP DESK
URL: Non University Link

From: XXXXX
Sent: Tuesday, August 16, 2016 12:05 AM
To: in@msn.com
Subject: FW: HELP DESK

Your SCRANTON mail box has exceeded its Quota limit CLICK HERE to login for upgrade OR you will be deactivated permanently
Phishing Example 2

Subject: Email Maintenance Today
URL: Non University Link
Country: Italy

From: The University of Scranton <xx@scranton.edu>
Sent: Friday, July 29, 2016 6:20 AM
To: xxxxxxxx
Subject: Email Maintenance Today

Dear User,
Email Maintenance Today 10:00 PM - 3:00 AM (EDT)
New Secure Socket Layer (SSL) Thir [link to secure site]
Please confirm Your Email Status by [link to confirmation]
BEGIN YOUR E-MAIL MAINTENANCE
Thank you.
Email Client Administrator
The University of Scranton

Division of Planning and Information Resources
Whaling and Spear Phishing

• What is Spear Phishing?
  – **Spear phishing** is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC.

  "The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you."
Subject: Payment

From: Kevin Quinn [mailto:ceoexec@writeme.com]
Sent: Monday, October 17, 2016 11:41 AM
To: Ed Steinmetz <edward.steinmetz@scranton.edu>
Subject: Payment

Hi Ed,

I need you to help me make a payment via wire transfer. Revert back so I can provide the payment details.

Thanks,

Kevin Quinn
President

Sent from my Verizon 4G LTE Tablet
Stop. THINK CONNECT
(Single click can launch multiple web request)
University Of Scranton Security Alerts/Notifications

- Intelligence feeds
- Internal Intrusion Detection System Alerts
- Internal Intrusion Prevention System
- Advanced Threat information sharing with Universities
- External Notifications and Alerts
- Working with law enforcement
- End User Reports
Subject: Outbound spam notification - xxxx@scranton.edu blocked from sending outbound mail

This is an automated reply from the Exchange Online Protection Spam Analysis System.

You are being contacted because we have detected high volumes of email marked as spam, or other suspicious behavior, originating from your organization.

The following email accounts have been blocked from sending email (they can still receive email):

xxxx@scranton.edu

It is likely that this email account has been compromised. Please follow these steps:

1) Resolve this issue on your side by:
   • Changing the password of the account.
   • Determining how the account was compromised.
   • Taking precautions to ensure that this vulnerability will not be exploited again.
   • Confirming that your outbound mail queue has been cleared of all offending messages.
2) Contact Microsoft support by using your regular contact channel.
3) Explain that you have a user that is blocked from sending mail and that the problem has been dealt with.
4) The agent will create a support ticket with the information that you provide and escalate it to have the email address or domain unblocked.
5) After the address has been unblocked, and pending no other issues, you will be contacted and alerted to the unblocking.
University of Scranton accounts used for third party services

<table>
<thead>
<tr>
<th>Breach:</th>
<th>Modern Business Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of breach:</td>
<td>8 Oct 2016</td>
</tr>
<tr>
<td>Accounts found:</td>
<td>58,843,488</td>
</tr>
<tr>
<td>Your accounts:</td>
<td>41</td>
</tr>
</tbody>
</table>

- Avoid using @Scranton.edu email account with third party unless necessary
- **NEVER** reuse @Scranton.edu password with third party systems
### Intrusion detection and prevention system (7 days)

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>malware</td>
<td>8.1k</td>
</tr>
<tr>
<td>peer-to-peer</td>
<td>4.9k</td>
</tr>
<tr>
<td>phishing</td>
<td>461</td>
</tr>
<tr>
<td>Source Country</td>
<td>Count</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
</tr>
<tr>
<td>United States</td>
<td>11.1k</td>
</tr>
<tr>
<td>10.0.0.0-10.255.255</td>
<td>5.7k</td>
</tr>
<tr>
<td>China</td>
<td>828</td>
</tr>
<tr>
<td>192.168.0.0-192.168.255.255</td>
<td>165</td>
</tr>
<tr>
<td>Netherlands</td>
<td>45</td>
</tr>
<tr>
<td>France</td>
<td>39</td>
</tr>
<tr>
<td>Canada</td>
<td>37</td>
</tr>
<tr>
<td>Germany</td>
<td>17</td>
</tr>
<tr>
<td>Australia</td>
<td>12</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>9</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>9</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>5</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>5</td>
</tr>
<tr>
<td>Italy</td>
<td>4</td>
</tr>
<tr>
<td>Poland</td>
<td>4</td>
</tr>
<tr>
<td>Brazil</td>
<td>4</td>
</tr>
<tr>
<td>Japan</td>
<td>3</td>
</tr>
<tr>
<td>Taiwan ROC</td>
<td>3</td>
</tr>
<tr>
<td>Spain</td>
<td>2</td>
</tr>
<tr>
<td>Malaysia</td>
<td>2</td>
</tr>
</tbody>
</table>
Online Safety Tips

- Avoid using the same password for third party services and websites.
- Use Non-Administrator as much as possible while surfing the web.
  At UofS we have ViewFininity software to minimize this risk.
Online Safety Tips

• Trust but verify; When in doubt contact service provide and verify. Contact TSC x4357 or Information Security office x4226 infosec@scranton.edu

• Think before you click; Use UofS for university portal and announcements.

• UofS uses Windows Defender and updates it regularly.
Online Safety Tips

• Report Suspicious behavior/Phishing attempts/Spam
  – Contact TSC x4357 or Information Security office x 4226 infosec@scranton.edu
  – Run Malwarebytes as needed
    • UofS uses Malwarebytes Anti-Malware that finds and removes malware. This software is already installed on your system.

• UofS uses System Center Configuration Manager and Kbox software to deploy patches
That’s a lot information

Just remember –
Be a Good Cyber Citizen!

When you are online, think about whether you are being safe and secure.
Data Classification

• Defined in the University’s Information Classification and Protection Policy

• Three Tiers:
  1. Restricted Data
     • Makes University liable for costs or damages due to unauthorized disclosure under laws, government regulations, or contract
     • Example: SSNs, credit/debit card, drivers license, banking information, passwords
  2. Confidential Data
     • Private, internal University information
     • Examples: FERPA (non-directory), Donor records
  3. Public Data
     • All other data
Restricted Data

• Storage – encrypted at rest
  - RoyalDrive (except credit cards)
  - OneDrive
  - Consumer Services (Dropbox, Box, etc.)
  - University Desktop / Laptop

• Transmission – encrypted in transit
  - Password protected RoyalDrive Ticket (except credit cards)
  - University Email
    • Carrier Pigeon
Confidential Data

• **Storage** – access restricted to need to use/access
  
  ✔ RoyalDrive
  ✔ OneDrive
  • Consumer Services (Dropbox, Box, etc.)
  ✔ University Desktop / Laptop

• **Transmission:**
  
  ✔ Password protected RoyalDrive Ticket
  ✔ University Email

Division of Planning and Information Resources
Data Retention

– Don’t need it, don’t store it
– Follow University and regulatory retention polices
– Securely destroy data:
  • Physical: Shredder / shredding services
  • Electronic – delete data (don’t forget about the recycling bin!)
Identity Finder

- Identity Finder software is designed to locate restricted data on UofS desktops
- Relaunching scanning campaign over the next 6 months
- Help identify and safely store restricted data
- Can virtually “shred” sensitive data
Information Security Awareness

- Employees with access to Restricted data
- Provide guidance and education for safe handling of data
- Complete training by November 30th
TOR

– The Onion Router
– Allows for “anonymous” surfing of the Internet
– Various legitimate and non-legitimate uses
– Not appropriate for University staff machines
Additional Resources

- [http://scranton.edu/staysafe](http://scranton.edu/staysafe)
- Contact Technology Support Center x4357
- Contact Information Security Office x4226 [infosec@scranton.edu](mailto:infosec@scranton.edu)

- Artist formally known as...
  - [security@scranton.edu](mailto:security@scranton.edu)
  - [abuse@scranton.edu](mailto:abuse@scranton.edu)
Questions