Data Security, Encryption, and User Awareness

2020 Pritzker Summer Research Group

Keith Ehrlicher

Director, BSD Information Security, BSD ISO
Agenda

• **Who is Hacking Us and Why?**
  – Statistics of Recent Cybersecurity Trends
  – Cyber Threat Actors

• **Secure Computing Best Practices**
  – Secure Computing Practices Tips
  – Enabling Multi-factor Authentication (2FA)
  – Password Security
  – Data Encryption
  – Phishing User Awareness
  – Know Who to Contact
WHO IS HACKING US AND WHY?
Cybersecurity Trends

- 1 in 10 URLs are malicious
- Average user receives 16 malicious emails a month
- More than half of all emails in the world are spam
- 78% of organizations said they experienced phishing attacks
- 48% of malicious email attachments are Microsoft Office files
- 92% of all malware is delivered by email
- Supply chain attacks have risen by 78% since 2017
- Mobile ransomware has increased by 33% since 2017
Cyber Threat Actors

**Nation-States**
- Most sophisticated threat actors
- Dedicated resources and personnel
- Extensive planning and coordination

**Cybercriminals**
- Moderate sophistication in comparison to nation-states
- Planning and support functions
- Specialized technical capabilities

**Hacktivists, Terrorist Groups, and Thrill-Seekers**
- Lowest level of sophistication
- Often utilizes widely available tools that require little technical skill
- Actions usually have no lasting affect on target past reputation

**Insider Threats**
- Individuals working within their organization
- Dangerous due to unique access to internal networks and resources
- Can be associated as another threat actor in addition to being insider threat
Data Security, Encryption, and User Awareness

SECURE COMPUTING BEST PRACTICES
Secure Computing Practices Tips

1. Use a password manager to create strong passwords and store them.
2. Be on alert for signs of a phishing email. Don’t open attachments or links in an untrusted email.
3. Utilize multi-factor authentication to prevent account compromise
4. Ensure all ePHI or PII data stored on a device is encrypted
5. Ensure any ePHI or PII data is securely deleted when it’s no longer needed.
6. Keep your devices fully patched to avoid exploitation
7. Install an Anti-Virus program and keep it up-to-date
8. Ensure that your devices firewall is enabled and configured
9. Backup your data to a secure location regularly
10. “90/10” Rule:
    - 10% of security safeguards are technical
    - 90% of security safeguards rely on the computer user (“YOU”) to adhere to secure computing practices
Enabling Multi-Factor Authentication

What is Multi-Factor Authentication (2FA)?

When a user logs into an account, that account uses one or more authentication factors in order to verify the identity of an authorized user.

You are required to enroll in 2FA.
Applications you can’t access without 2FA: Workday, UChicagoBox, VPN

UChicago:
- Secures your CNet account for cVPN and other secured applications
- Sign up at https://2fa.uchicago.edu

BSD:
- Secures your BSDAD account for BSD VPN and other secured applications
- Sign up at https://2fa.bsd.uchicago.edu/
- FAQ sheet is on the BSD ISO website at http://security.bsd.uchicago.edu/bsd2fa/
Password Security

Creating Strong Passwords

- A strong password has at least 12 characters.
- Utilize a password manager to create and store passwords. The University utilizes the password manager, LastPass.
  - LastPass or 1Password are recommended password managers.
- For a better understanding of password strength visit, http://www.passfault.com/. However, DO NOT enter any real passwords into this website.

The table below shows how fast your password can be guessed

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Calculation</th>
<th>Result</th>
<th>Time to Guess</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 chars: lower case alpha</td>
<td>$26^8$</td>
<td>$2 \times 10^{11}$</td>
<td>&lt; 1 second</td>
</tr>
<tr>
<td>8 chars: alphanumeric</td>
<td>$62^8$</td>
<td>$2 \times 10^{14}$</td>
<td>3.4 min</td>
</tr>
<tr>
<td>8 chars: all keyboard</td>
<td>$95^8$</td>
<td>$7 \times 10^{15}$</td>
<td>2 hours</td>
</tr>
<tr>
<td>12 chars: alphanumeric</td>
<td>$62^{12}$</td>
<td>$3 \times 10^{21}$</td>
<td>96 years</td>
</tr>
</tbody>
</table>
Encryption vs. Passwords

- Encrypting data is not the same as having a password.
  - Passwords themselves do not scramble information.

- If something is only “password protected,” it’s not necessarily protected. Someone could bypass the password and read the information directly.
Types of Sensitive Data

- **Restricted / Confidential**
  - ePHI or electronic Protected Health Information (Personal + Health)
    - Names, Medical Record Numbers, reports, test results, or appointment dates etc.
  - PII or Personally Identifed Information
    - Name, SSN, driver’s license number etc.
  - Clinical Research Data
  - Privileged & Confidential Information (legal)

- **Sensitive / Internal Use Only**
  - Policies and Procedures
  - IT schematics, diagrams, configuration documents
  - Contracts not subject to confidentiality agreements

- **Public**
  - Content approved for posting to the web
  - Directory Information listed on a public website

- When the classification is not clearly defined, default to Sensitive unless defined in writing by your supervisor.
Data Exposure Costs

This table shows how much an incident costs the University both in time and money.

<table>
<thead>
<tr>
<th>Incident Description</th>
<th>Encrypted Device with ePHI/PII</th>
<th>Unencrypted Device with ePHI/PII</th>
<th>Unencrypted Device without ePHI/PII</th>
</tr>
</thead>
<tbody>
<tr>
<td>User’s computer stolen from his/her car. Device had ~400 patient records.</td>
<td>1 Hour</td>
<td>50 hours</td>
<td>35 hours</td>
</tr>
<tr>
<td>User forgot laptop in cab. Device had ~400 patient records.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User left tablet on plane. Device had no patient health information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigation time (combined hours for incident response team – legal, HR, IT, security, etc.)</td>
<td>$0</td>
<td>$2,000</td>
<td>$800</td>
</tr>
<tr>
<td>Security Forensics Costs</td>
<td>$0</td>
<td>$2,000</td>
<td>$800</td>
</tr>
<tr>
<td>Reputation Damage Costs</td>
<td>$0</td>
<td>Priceless</td>
<td>$0</td>
</tr>
</tbody>
</table>
# Data Encryption

<table>
<thead>
<tr>
<th>Type</th>
<th>Encryption Solutions</th>
<th>Cost/Impact</th>
<th>How</th>
</tr>
</thead>
</table>
| **Apple** | **File Vault 2** | Encrypt the contents of your entire drive.  
Solution will work for personally-owned and BSD-owned laptops.  
Strong AES 128 based encryption.  
Can store recover key with Apple; well-documented install guide. | 1. Choose Apple menu () > System Preferences, then click Security & Privacy.  
2. Click the FileVault tab.  
3. Click the Lock button, then enter an administrator name and password.  
4. Click Turn On FileVault. |
| **Windows** | **BitLocker** | Encrypt the contents of your entire drive.  
Solution will work for personally-owned and BSD-owned laptops.  
Strong encryption for data protection.  
Some hardware and software dependencies. | 1. Click Start, click Control Panel, click Security, and then click BitLocker Drive Encryption.  
2. On the BitLocker Drive Encryption page, click Turn On BitLocker on the operating system volume.  
3. If your TPM is not initialized, you will see the Initialize TPM Security Hardware wizard. Follow the directions to initialize the TPM and restart your computer.  
4. Select one of the following recover options from the recovery password page, you will see the following options:  
   - Saves the password to a USB flash drive.  
   - Saves the password to a network drive or other location.  
   - Print the password |
### Data Encryption

<table>
<thead>
<tr>
<th>Type</th>
<th>Encryption Solutions</th>
<th>Use/Features</th>
<th>How</th>
</tr>
</thead>
</table>
| External Storage| Apricorn Aegis USB   | • Secures the transport of data, documents, and presentations.  
• Strong, 256-bit AES hardware-based encryption;  
• unlocks with onboard PIN pad;  
• PIN activated 7-15 digits -Alphanumeric keypad.    | 1. Purchase through University procurement or on you own from Amazon, Staples or any other major IT equipment provider. |
| Apple Phone/ Tablet | IOS                     | • Work for personally-owned and BSD-owned devices  
• Native security feature, enabled by default with the use of passcode; vendor-supported  
• Strong, 256-bit AES hardware-based encryption  
• Can store recover key with Apple | 1. Set a passcode on phone  
2. Scroll down to the bottom of the Passcode settings page. You should see a message that says “Data protection enabled.” This means that the device’s encryption is now tied to your passcode. |
| Android Phone/ Tablet | Android               | • Work for personally-owned and BSD-owned devices  
• Easy setup, but not enabled by default  
• Strong, 256-bit AES hardware-based encryption  
• Well-documented install guide. | 1. Your device’s battery must be at least 80% charged or won’t start.  
2. Your device must be plugged in throughout the entire process.  
3. Unroot phone if rooted before continuing.  
4. Following your manufacture’s steps to complete the encryption. |
Phishing User Awareness

• **DO NOT** click on any links or attachments in an email that you do not recognize.

• If you are unsure of the intent of the email and it looks suspicious, forward it as an attachment to security@bsd.uchicago.edu.

• If you receive an email prompting you to login to a known service, do not navigate to that service through the email. Instead, navigate to that service using a trusted method.
  
  – An example would be if you receive a Google alert about your account, navigate to Google using your browser like you would normally rather than clicking on the link in the email.

• Links in a phishing email will often attempt to grab a copy of your credentials by leading you to a “cloned website” login.

• Make sure to check the domain of a URL. Often phishing emails use similar domains (i.e. google.com vs. google.com).
Know Who to Contact

- It’s important that if you **observe anything suspicious** occurring that you **reach out to the BSD ISO** as soon as possible.

- Send us any suspicious emails you receive so that we can investigate them.

- We’re here to help you, reach out to us if you have any questions regarding anything.

- We can help you secure your data so that you can focus on your work.

---

**How to reach us:**

- **Web Site:** [http://security.bsd.uchicago.edu](http://security.bsd.uchicago.edu)

- **BSD ISO Team Email:** security@bsd.uchicago.edu

- **UCM ISO Team Email:** security@uchospitals.edu

- **Remote Work\Learning Guidelines.** [https://bsdis.uchicago.edu/remotework/](https://bsdis.uchicago.edu/remotework/)

---

**The University of Chicago**