Security Best Practices Roundtable – 9:15

Discussed topics:

1.

Notes

STUDENT DATA PRIVACY

- Hipaa, Ferpa, Cipa concerns
- Vendors - Create a document that is a copy of the current privacy agreement, so that you have a copy of the current agreement on file. Make sure the copy is dated and has a URL reference.
- Review privacy contracts annually
- If a contract is non-renewed, demand that the vendor purge all previously held data. That needs to be stated in the contract agreement.

Identity Management

- Are complex passwords necessary?
- Two factor authentication?
- Create a pass-phrase instead of a password
- Must be a top-down initiative (must be supported at the top)
- Have I been pwned - https://haveibeenpwned.com/

Physical & Digital Security

- Badging system with photo recording of entrances
- Limited access to MDF and IDF closets
- Limited access to staff after hours

Cloud Security

- SSL encryption and decryption
- Internet filters - Securly & iBoss

Ideas gathered during BrainStorm registration:

1. Cybersecurity

2. Phishing - Sonicwall phishing IQ test (https://www.sonicwall.com/phishing-iq-test/)
    a. Gophish (https://getgophish.com/)
3. Student data privacy
4. Network security
5. Blocking Crosh access on Chromebook:

    Press CTRL+ALT+T to open crosh, look at the URL and copy the part after chrome-extension://nkoccljplnhpfnfiajclkommnmllphnl/html/crosh.html

    Next open your Google domain management console and go to "Device Management > Chrome Management > User Settings".

    Next create a URL blacklist for the following entry nkoccljplnhpfnfiajclkommnmllphnl/html/crosh.html

    Then apply or reload the policy on the Chrome browser.

6. Identity Management
    a. https://haveibeenpwned.com/
7. Physical and Digital Security
8. Cloud Security