

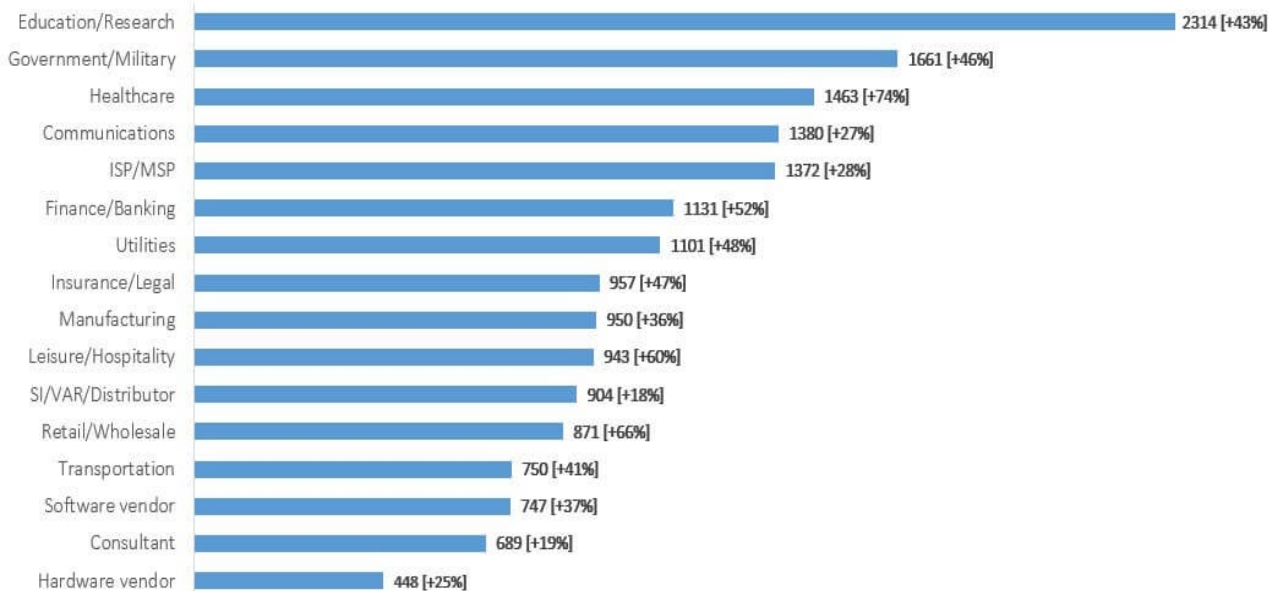


# Information Security

Lightning Talk

# Current Trends in Cybercrime

Avg. Weekly Cyber Attacks per Organization by Sector in 2022  
showing all sectors suffer double-digit increase compared to 2021



- ▶ Global cyber attacks increased nearly 400% post-COVID
- ▶ 90% of attacks are targeted at employees, not technology
- ▶ 82% of attacks involve social engineering or phishing techniques
- ▶ 80% of data breaches expose PII
- ▶ PII - Personally Identifiable Information

# What is “PII” Anyway?!

“‘Personally identifiable information’ (PII) covers a greater range than ‘personal identification,’ such as an individual’s name, address, telephone number, social security number, driver’s license number, email address, etc. PII connects you to what you bought with your credit card, what you checked out with your library card, and what websites you visited where your web browser saved cookies. More than simple identification, PII can build up a picture of your tastes and interests — a dossier of sorts, though crude and often inaccurate.” - [Privacy and Confidentiality Q&A, ala.org](http://www.ala.org/privacy/privacyandconfidentialityqanda)

# External Vendors

- ▶ Have vendor sign an access policy before onboarding begins
- ▶ Vendor IP addresses must be whitelisted
- ▶ Use SFTP to transmit extracts or other data to vendors
- ▶ Require the use TLS-SIP2 or other secured connection method
- ▶ Read Only access unless explicitly required
- ▶ Know where your data is going

# Securing SIP2 with TLS

- ▶ SIP2 is an industry standard for passing transactional data between server and client
- ▶ Passed over the internet in plaintext, potentially exposing PII
- ▶ Transport Layer Security (TLS) is a method of encrypting transmitted data
  - ▶ Key-pair is required to decrypt and view
- ▶ TLS-SIP2 encrypts SIP2 data, rendering it unreadable without matching security key

AOWMS | AA21140003533188 | AENOSEK, IAN |  
AQSWs | BZ0075 | CA0000 | CB0200 | BLY | BV15.00  
| BD800 QUAIL RIDGE DR WESTMONT IL  
60559 | BEian@swanlibraries.net | BHUSD |  
PD19830618 | PCSWS\_STAFF | PEMALE | PFADULT | PG

## PII Exposed:

- Name
- Gender
- Birthdate
- Home Address
- Email Address
- Barcode/PIN

# Securing Patron Interactions

“I didn’t bring my library card.”

- ▶ Verify patron with photo ID
- ▶ Maintain patron photos in user records
- ▶ Ask patron to write down information to confirm identity
  - ▶ Avoid asking for any information verbally
- ▶ Shred/destroy paper after assisting user

# Securing Patron Interactions

## “I forgot my PIN.”

- ▶ Patron PINs masked in system - staff unable to see
- ▶ Use last four digits of phone when setting/resetting PIN
- ▶ USB Keypads enable patrons to set their own PIN
- ▶ Self-Service PIN reset available via OPAC/Catalog
- ▶ Require PIN at self-service stations



# Keeping Holds Confidential

- ▶ Unless you know you're speaking with the correct person, do not provide title information
- ▶ Avoid leaving any item details in voicemail
- ▶ Open Hold Shelves?
  - ▶ Avoid printing entire patron ID or name on wrap
  - ▶ Affix hold wrapper to edge opposite title
  - ▶ Shelf items with titles facing backwards

<sup>I</sup> Pickup By:  
8/4/2023

R  
o  
b  
e  
r

42860



# End-User Awareness

- ▶ Be conscious of your interactions with external contacts
- ▶ Don't provide any sensitive information to unknown contacts
- ▶ Hover-over links in suspicious email - don't click unless you're sure
- ▶ Logging into a site manually is always safest!
- ▶ Do not provide credentials unless you know site is legitimate
- ▶ Pay attention to browser's address bar
- ▶ Did you ***REALLY*** book a flight that needs confirmation?

# Be Proactive!

- ▶ Contact support when offboarding staff
- ▶ Purge inactive patron records regularly
- ▶ Ensure passwords are complex or use password managers
  - ▶ Try using a passphrase!
- ▶ Do not transmit credentials via email - including screenshots!
- ▶ Avoid sharing accounts or update password regularly
- ▶ Enable Multi-Factor Authentication for accounts

# Mistakes Happen...

- ▶ Nobody's infallible - we ALL make mistakes
- ▶ Notify IT immediately if you:
  - ▶ Provided credentials or logged into a malicious site
  - ▶ Opened any attachments from a suspicious email
- ▶ Response time is critical





# Questions?

**Ian Nosek**

Information Technology & Systems Support Manager  
SWAN Library Services