Cyber Hygiene for Librarians

Weiqing Sun

March 7, 2022

Self Introduction

- **UToledo Appointments**
  - Professor, Computer Science and Engineering Technology
  - Program Director, Master's Programs in Cyber Security
  - Cyber Security Fellow, Division of Technology & Advanced Solutions
- **Education**
  - Ph.D. in Computer Science, Stony Brook University.
  - B.S., M.S. in CSE, Tongji University.
- **Research Interests**
  - Computer and network security
    - Malware defense, security policy development and security enhancement of critical systems
- **Contacts:**
  - http://www.eng.utoledo.edu/~wsun

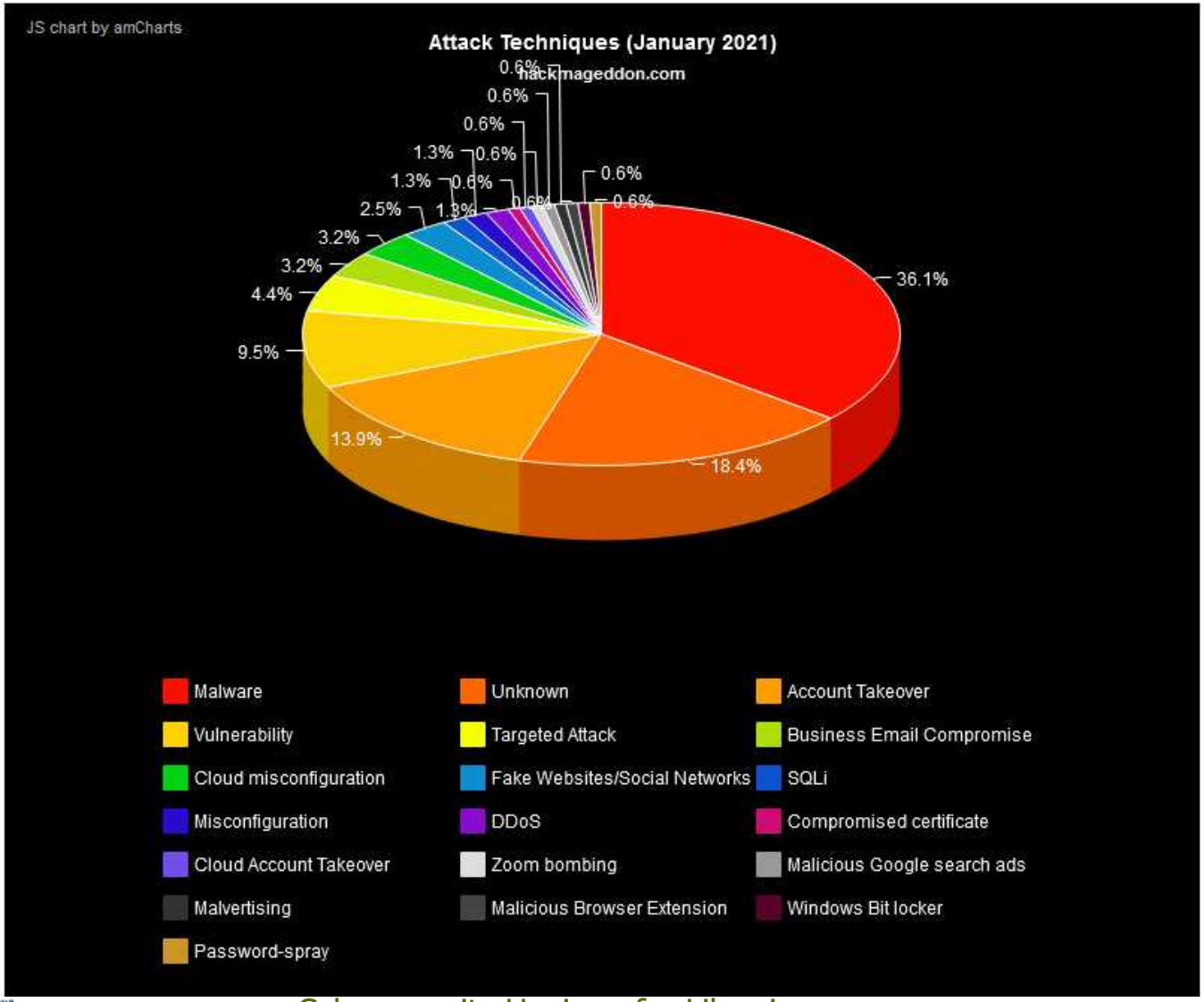
Research Projects

Motivation and Background

- **Can you live without the following?**
  - The Internet
  - Smart phone
  - Social network
  - Cloud
  - ……
- **Cyber threats/attacks**
  - More (quantity, scale)
  - More organized (underground organizations)
  - More intelligent (e.g. powered with AI)
  - ……

Cyber Threats

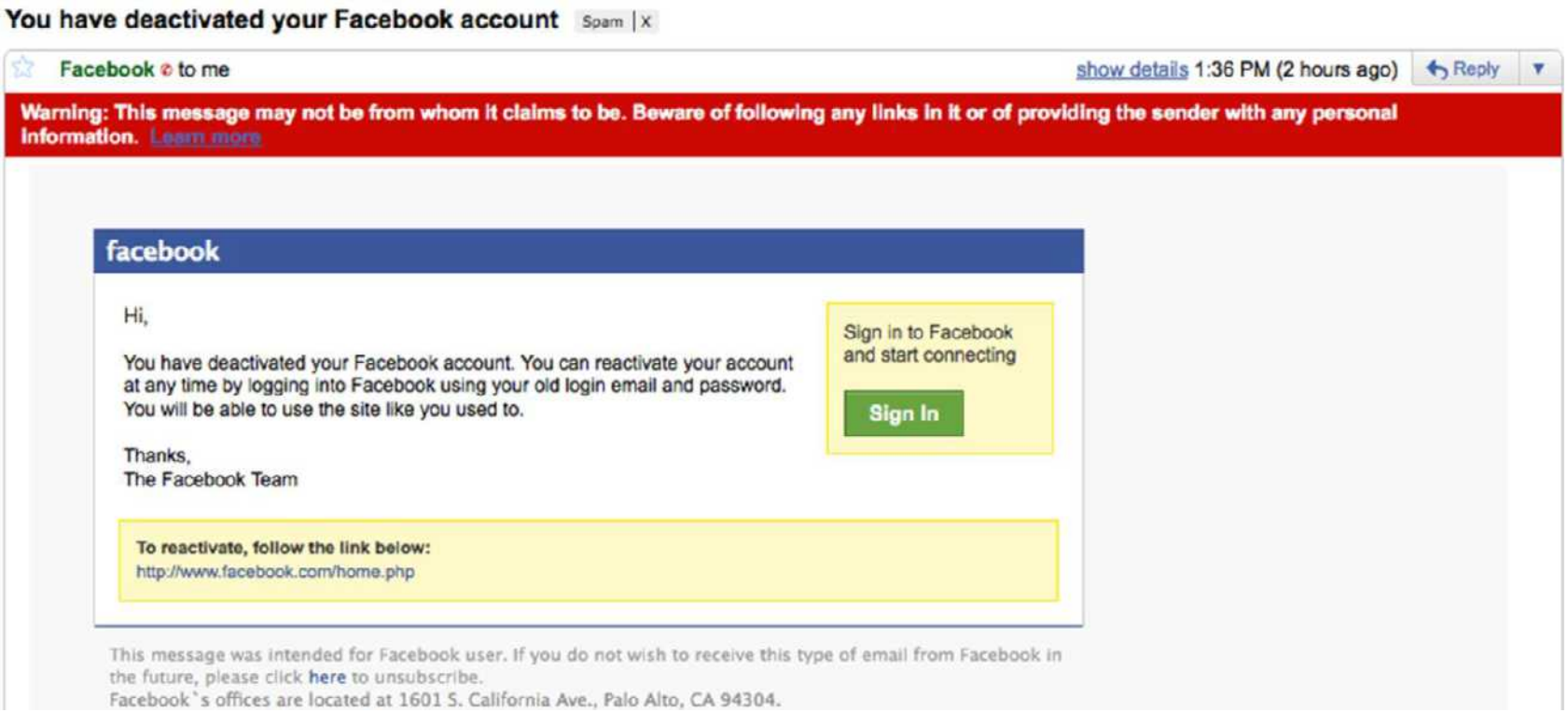
Cyber Attacks Statistics



Phishing

- **A form of fraud with attacker pretending as reputable party in various communication channels → login info leaking, etc.**
- **Spear Phishing**
  - Target at "powerful" users, such as librarians, doctors, administrators, finance workers
  - Mostly through emails, e.g.
    - Email from University President to chief of staff for transfer of funds
    - Email from financial manager to request users update payroll deposit information

Phishing


You have deactivated your Facebook account
Spam | x
Facebook to me
show details 1:36 PM (2 hours ago)
Reply
Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more
facebook
Hi,
You have deactivated your Facebook account. You can reactivate your account at any time by logging into Facebook using your old login email and password. You will be able to use the site like you used to.
Thanks,
The Facebook Team
Sign in to Facebook and start connecting
Sign In
To reactivate, follow the link below:
http://www.facebook.com/home.php
This message was intended for Facebook user. If you do not wish to receive this type of email from Facebook in the future, please click here to unsubscribe.
Facebook`s offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Malware

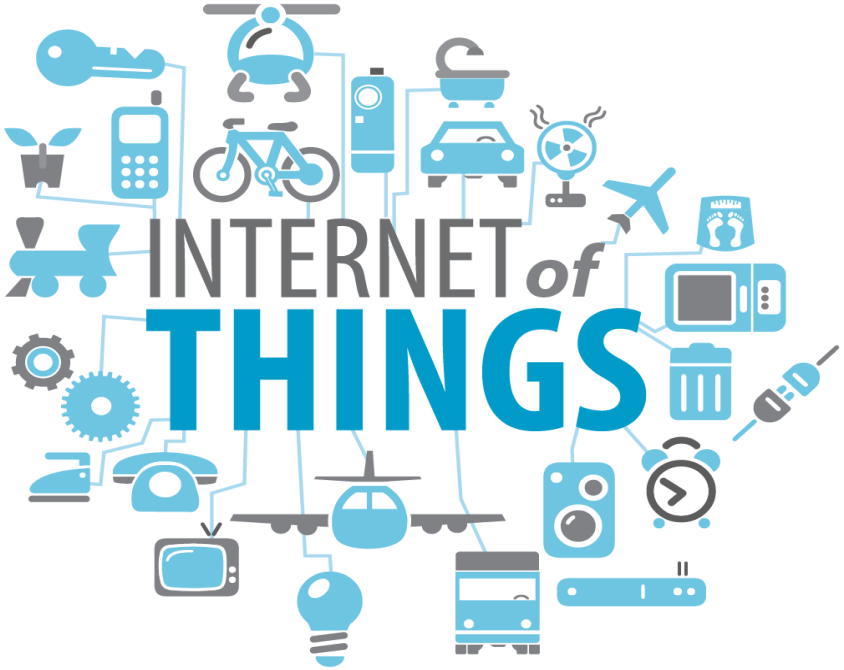
- **Malicious software**
  - Ransomware
    - Encrypted data → bitcoin for ransom
      - Healthcare organizations, universities/schools top target
  - Trojan Horse
  - Computer virus
  - Computer worm
  - Rabbits
  - Logical bomb
  - ……

Ransomware


DMA Locker 4.0
All your personal files are LOCKED!
WHAT'S HAPPENED?
* All your important files(including => hard disks, network disks, flash, USB) are encrypted.
* All the files are locked with asymetric algorithm using AES-256 and then RSA-2048 cipher.
* You can't restore your files because all your backups have been deleted.
* Only way to recover your files is to pay us 1 BTC
* As a proof you can decrypt 1 file FOR FREE by clicking here: CLICK
HOW TO PAY US AND DECRYPT YOUR FILES?
1. If you are OFFLINE you can contact us via e-mail: dma4004@zerobit.ex and we will provide you instructions about how to decrypt your files.
2. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
* https://coincafe.com/
* https://www.bitquick.co/
* https://www.coinbase.com/
3. If you already have Bitcoins, pay us 1 BTC to the following Bitcoin address:
* Ransom increase time:
If you don't pay us within this time, the amount you will have to pay will increase to: 1.5 BITCOINS
4. If you have paid, enter following site to get your transaction id.
Click this button to show tutorial how to locate your transaction id: SHOW
5. When you have located Transaction ID, paste it to'TRANSACTION ID' field below and, click the "CHECK PAYMENT" button. Confirming your payment by our servers can take up to several hours (we require some bitcoin transaction confirmations). When your payment has been confirmed, the 'DECRYPT FILES' button will enabled, just click it to decrypt your files.
TRANSACTION ID:
CHECK PAYMENT
PAYMENT STATUS:
DECRYPT FILES

IoT Devices

- **Smart devices in part of organizational/home network**
  - Can potentially affect other part of the network if not properly segmented
  - Smart TV, smart meter, wearable devices can be potentially subverted



Social Networks

- **Privacy Issues**
  - Tools available to mine information posted on social networks
- **Integrity Issues**
  - Weak account protection leads to account subverted and private information leaked
- **Fake news, Spams**

Legacy Systems

- **Still a good number of existing legacy systems**
  - Not patchable, not updatable, e.g., XP system
  - Vendor slow in providing new version of software or too expensive to replace
  - With full network connectivity
  - Defenses
    - Sandboxing such systems
    - Network partitioning
    - Vulnerability scanning

Brute Force Attack

```
192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish1' with password:'1212'
192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashish1' with password '1212'
192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish1' with password:'123321'
192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashish1' with password '123321'
192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish1' with password:'hello'
192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashish1' with password 'hello'
192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

Insider Attacks

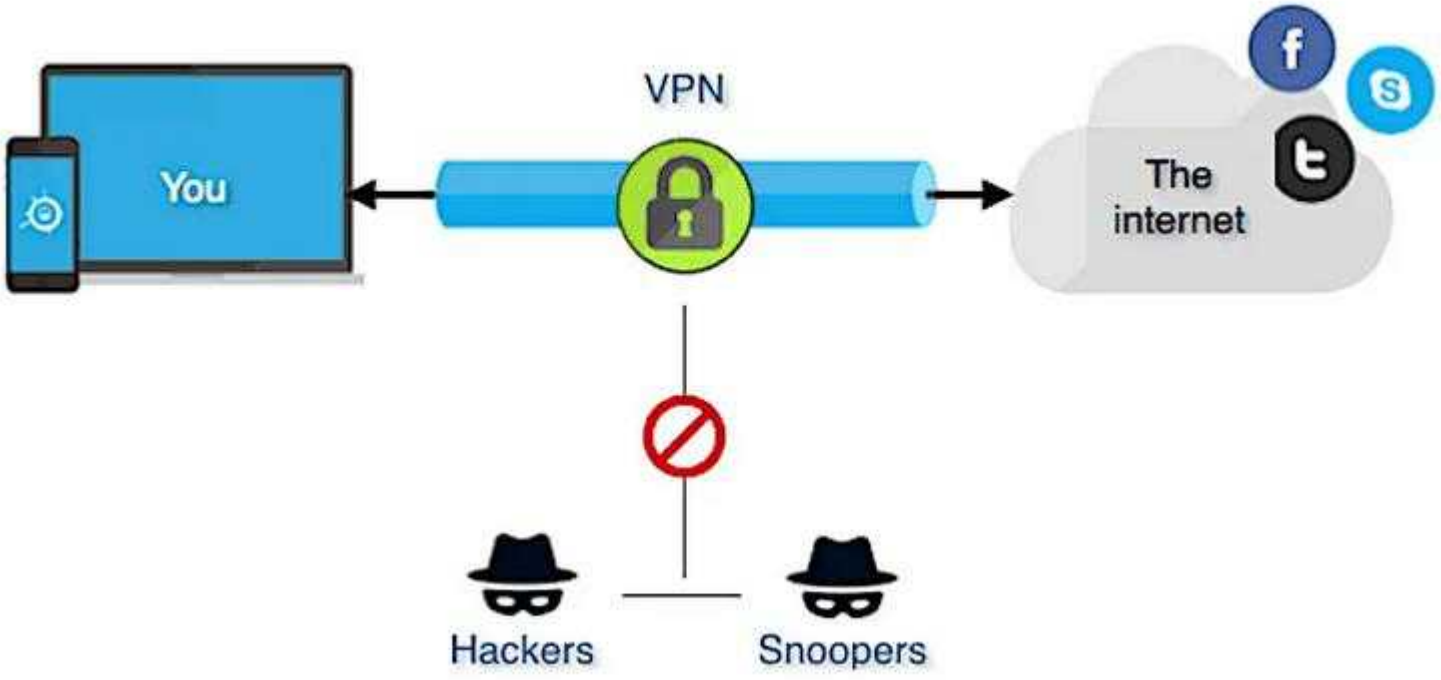
- **Part-time employee**
- **People from our own circle**
- **Steal info if no proper access control in place**

Digital Resources for Librarians

- **Security Tools**
  - Remote Access (VPN)
  - Authentication (OpenAthens)
  - Password Manager (LastPass, iCloud Keychain)
- **Electronic Resources**
  - PubMed
  - Web of Science
  - ClinicalKey
  - AccessMedicine

Virtual Private Networks (VPN)

- **A secure tunnel will be created using VPN over the unsafe communication channels**



https://networkencyclopedia.com/virtual-private-network-vpn/

Virtual Private Networks (VPN)

- **Access University resources from home in a secure way**
- **Make sure the home computer is secure**
  - Security updates
  - Security software installed and configured properly

OpenAthens

- **Access Management Platform**

https://twitter.com/openathens/status/885080014580064257/photo/1

OpenAthens

- **Access Management Platform**
- **Single Sign-on**
  - Access e-resources across library databases and publisher websites with just one login
  - Use University/organization credentials (won't be transmitted to different publisher sites)
  - Secure protocols used (SAML 2.0, AES-256, etc.)
  - Based on Google Cloud Platform (GCP)

Password Manager

- **Useful for manage (a lot of) passwords for online presence**
- **LastPass vs. iCloud Keychain**
  - LastPass: richer features, more secure, fee-based
  - iCloud Keychain: free, mostly on Apple devices

Handling Cyber Incidents

- **Identify attack**
- **Mitigate the attack (unplug the devices from network)**
- **Investigate the attack**
- **Decision making not always easy**
  - Judgement call
  - A biomed device was attacked, however it's being used to treat patients

Raising Security Awareness

- **Trust cautiously**
  - A person, an organization, a device, a web site, an email, a post, an application, an update ……
- **Manage your devices**
  - Keep an inventory of own devices
  - Apply patches regularly
  - Use appropriate security defenses, firewall, IDS, encryption
  - Wipe data before getting rid of any device
- **Manage your accounts**
  - Password
  - Two-factor authentication/multi-factor authentication

Protect Your Cyber Self

- **You**
  - Be mindful about what you share
  - Think twice before clicking links & install applications
  - Don't accept unknown connections or friend requests
- **Your Accounts**
  - Check privacy settings
  - Practice password hygiene
  - Secure with two/multi-factor authentication
- **Your Devices**
  - Lock it
  - Antivirus
  - Keep OS & Software updated

Demos

- **Phishing attack**
  - Amazon
  - Facebook
- **Password checking**
- **Ransomware attack**

Conclusions

- **Cyber threats on a rapid rise including those against library systems**
- **Solutions to the cyber challenges**
  - Cyber awareness needed
  - Cyber hygiene for our librarians important
  - Cybersecurity skills need to be equipped for librarians

Thanks and Questions?