Services & Cyber Security

TARIQ AHMED SHEIKH

Important Shared Infrastructure

- General Purpose Labs
- Anti-Malware
- Wi-Fi
- Network Printing
- Internet
- Office365
- Zambeel
- LMS
- SAP
- Games
- SharePoint
- HPCC

Software

- SPSS Statistics
- Stata
- Palisade
- MatLab
- EViews
- Refinitiv
- NVivo
- SPSS AMOS
- AspenTech
- ArcGIS
- Adobe Suite

Cyber Security?

- Confidentiality
- Integrity
- Availability

Awareness?

- Human is the weakest link
- Password construction

Type of Threats	Real-World Example
Ransomware	RYUK
Fileless Malware	Astaroth
Spyware	DarkHotel
Adware	Fireball
Trojans	Emotet
Worms	Stuxnet
Rootkits	Zacinlo
Keyloggers	Olympic Vision
Bots	Echobot
Mobile Malware	Triada

Top 10 Cyber Threats in 2022

https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/

1 Social Engineering

Any network is hackable if an employee can be duped into sharing access.

2 Third-Party Exposure

Vendors, clients, and app integrations with poor security can provide access to an otherwise well-protected network.

3 Configuration Mistakes

Even the most cutting-edge security software only works if it's installed correctly.

4 Poor Cyber Hygiene

Employee training is essential to ensure those with network access maintain safe cyber practices.

5 Cloud Vulnerabilities

Online data storage and transfer provides increased opportunities for a potential hack.

6 Ransomware

Hackers can capture sensitive data or take down networks and demand payment for restored access.

7 Mobile Device Vulnerabilities

Devices that connect to multiple networks are exposed to more potential security threats.

8 Internet of Things

Smart technology users may not realize that any IoT device can be hacked to obtain network access.

9 Poor Data Management

When massive amounts of unnecessary data are kept, it's easier to lose and expose essential information.

10 Inadequate Post-Attack Procedures

Security patches must be as strong as the rest of your cybersecurity protections.

Password

- Keep passwords confidential;
- All user passwords must be at least 8 characters in length (10 Characters are recommended)
- Passwords must contain characters from at least 3 of the following 4 categories
  1. Upper-case alphabets (A-Z)
  2. Lower-case alphabets (a-z)
  3. Base 10 digits (0-9)
  4. Special characters (e.g. !, @, #, $, ^, &, etc.)

Password Construction

- **Don't** choose a password that is a dictionary word (English or foreign)
- **Don't** choose a password that is the name of a family member, pet or friend
- **Don't** choose keyboard, word or number sequences as passwords (e.g. 12345678, qwerty, asdfg, aaaaa, etc.)
- **Don't** choose passwords that are hybrids of the above
- **Don't** choose passwords that are any of the above spelled backwards
- **Don't** choose passwords that are any of the above followed or preceded by a digit (e.g. 1password, password1, etc.)

DOs

- Do change your password regularly for every system you are using
- Do enable your Screen Saver Password or lock your workstation
- Do backup your data at least once a week
- Do lock away all confidential documents, files and USB's at the end of each work day
- Do use LUMS VPN to remote connect, when needed
- Do keep your screen clear in case of a visitor, space sharing, student

Don'ts

- Do not share your password with anyone including staff
- Do not write your password on any paper, whiteboard or post it pad
- Do not insert password in your emails
- Do not visit inappropriate web sites e.g. hacker web sites
- Do not download unlawful or unlicensed software from the Internet
- Do not install unlicensed software onto your computer
- Do not give your mobile phone to untrusted resource
- Do not leave your computing device or phone unattended

Email Use

- Staff should not use the email system for the following reasons
  - Chain letters
  - Non company sponsored charitable solicitations
  - Political campaign materials
  - Harassment
  - And any other non-business use
    - Staff are allowed to use the email for personal use but within reason

Release of Information to Third Parties

- Confidential information should not be released to third parties unless there is a need to know and a Non Disclosure Agreement has been signed. It is the responsibility of all staff to safeguard the company's information.

Always remember……

- Keep information confidential
- Protect your password
- Always report suspicious activity
  - infosec@lums.edu.pk, helpdesk@lums.edu.pk

What is KnowBe4?

- https://training.knowbe4.com/ui/login?logout=true