Internet of Things (IOT)

Vulnerabilities

Ms. Mohini Arora

HOD, Computer Science

Air Force Golden Jubilee Institute

About Internet of Things(IOT)?

- Networking of computing devices, vehicles, buildings connected to the Internet for exchange of data
- Functioning is controlled by digital devices, mostly by apps installed on smartphones
- Without or with minimum human intervention
- Leads to convenient, faster and timely output.

https://live.staticflickr.com/454/19716415899_ce89d4a149.jpg

About Internet of Things(IOT)?

- Everywhere around us – More than 20 billion devices are connected through IOT

- Possibilities of what can be done with IOT are endless.

- Is impossible to avoid since it impacts the way we live and work today

https://live.staticflickr.com/650/22370983740_408a434ef1.jpg

Popular Devices on IOT

- ❑ Smart Devices - Smart phones, Watches , Smart TV
- ❑ Laptops / Desktops
- ❑ Routers and Wireless Printers
- ❑ Microphones and Speakers
- ❑ Home Appliances – Refrigerators, Air Conditioners, Washing Machines

SAMSUNG SmartThings
Log Out
Routines
Cameras
Explore SmartThings
Smart Home. Intelligent Living.
See It In Action
SmartThings lets you easily monitor, control, and secure your home—from your TV or anywhere
How it Works
Uses
Products

https://live.staticflickr.com/565/31839836964_5748a738b1_b.jpg

Popular Devices on IOT

- ❑ Automated locks and connected doors
- ❑ Keycard readers / Smart Cards
- ❑ Surveillance devices like camer
- ❑ Intercom Systems
- ❑ Health bands

ttps://live.staticflickr.com/1711/24035319766_8b7e766dd3_b.jpg

https://n1.sdlcdn.com/imgs/i/f/l/M2-Waterproof-Heart-Monitoring-Fitness-SDL409770152-1-7ad71.jpg

Some Known Facts….

- An app or device is available for most actions and tasks that you can think of.
- Amazon's Alexa and Apple's Siri
  - Help you read and respond to texts without you having to pick up your phone.
  - Simple things like switching on lights, fans or any home appliance , can now be automated to when you enter and leave the room.
- Even devices like toothbrushes and children's toys have become a lot smarter and boast of internet-related services.

IOT and Education Sector

Teachers

Students

Parents

Administrators /Policy Makers

How is IOT beneficial for students?

- Individualization and Personal Learning
- More opportunities to learn at any time and from anywhere around the world
- Increased Level of Engagement
- Availability of digital books
- Collaborative Learning among students from across the globe

How is IOT beneficial for teachers?

- Advanced tools for teaching learning process
  - ✓ Digital Pens and Boards
  - ✓ Videos, illustrations and Simulations
- Automatic attendance
- Flexibility in teaching
- Easy communication
- Availability of Digital books and QR codes for study materials

How is IOT beneficial for Administrators?

- Can make use of IoT for school management
- Automatic monitoring of building, ventilation systems, heating systems using special devices and sensors;
- The security level can be increased significantly
- Saves a lot of time by automating the tasks which are otherwise very time-consuming.
- Can provide automated personal assistants who can alarm on your everyday plans.
- Easy mode to connect with students and staff

Are you **only** getting better experience?

and

Are you **NOT** giving away your information?

?

https://economictimes.indiatimes.com/tech/internet/beware-smart-gadgets-may-be-a-risk-to-your-privacy/videoshow/60994197.cms

IOT Vulnerabilities

Internet of Things (IoT) vulnerabilities stem from the tendencies of the devices to have low computational power and hardware limitations that don’t allow for built-in security features.

When does a cyber criminal attack?

- **Right opportunity for a cyber attack arises because :**
  - Many device manufacturers don’t care **to provide built-in security** while designing, deploying or running the IoT devices.
  - Owners of IOT devices usually don’t have the knowledge to keep these devices secure.
  - Sometimes the user may not even know that the device is or can be connected to the internet to begin with!

Why is IOT a matter of concern?

❑ *Control of life*

- Our lives are being completely handled by technology and are increasingly becoming dependent on it.
- The younger generation is already addicted to technology for every little thing and going towards a lazy environment.

❑ *Health Issues*

- Many IoT devices involve screens that expose users to blue light.
- Excessive exposure can be unhealthy and should never fully substitute for physical learning activities

❑ *Cost*

- Buying technology regularly can be prohibitively expensive.

Why is IOT a matter of concern?

❑ ***Initial learning***

- Huge diversity of devices and applications
- Challenge for teachers struggling to adapt to new gadgets and then use them with tech-savvy students

❑ ***Ongoing learning***

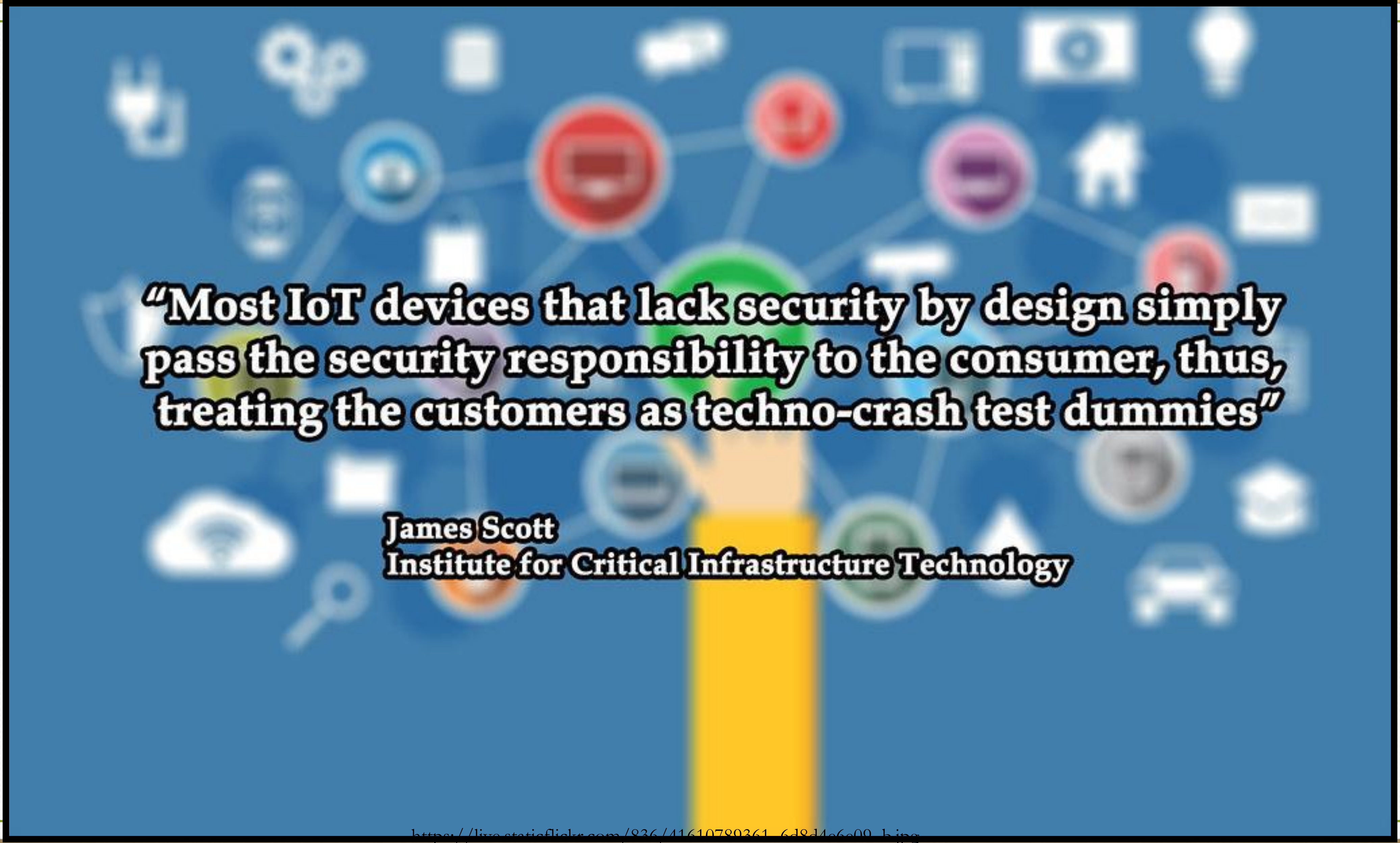
Maintaining an IoT initiative in the classroom, involves

- regularly updating technology
- taking new cybersecurity measures
- Attending mandatory workshops to keep oneself up to date.

Why is IOT a matter of concern?

❑ ***Privacy and Security Issues***

- No proper security in place
- Devices are vulnerable to sensitive data leakage as there are numerous untapped opportunities for cyber criminals to hack into your IOT devices.
- Cyber criminals who have gained access to your smart devices could spy on you and later use it for malicious purposes.



"Most IoT devices that lack security by design simply pass the security responsibility to the consumer, thus, treating the customers as techno-crash test dummies"

James Scott
Institute for Critical Infrastructure Technology

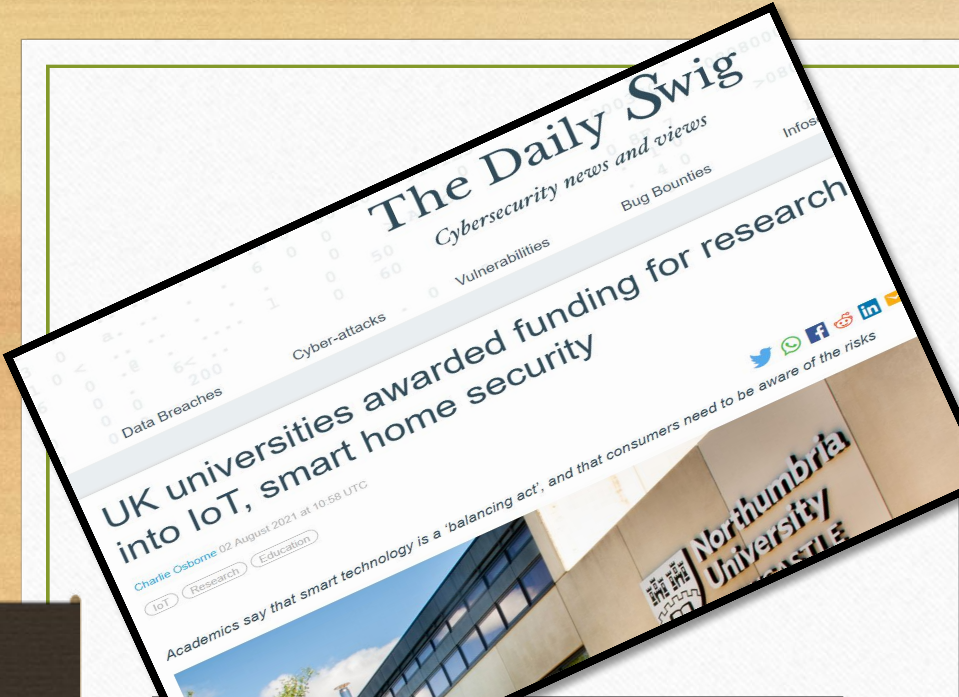
https://live.staticflickr.com/836/41610789361_6d8d4e6e09_b.jpg

IOT Vulnerabilities and Education Sector

Facts …

- ❑ Educational institutions are at significant risk today due to their adoption of IoT devices
- ❑ Threat trends show that cybercriminals are increasingly targeting these devices.
- ❑ One study conducted by HP found that 70% of the IoT devices tested contained security vulnerabilities.
- ❑ The Department of Homeland Security, USA has even created a Cybersecurity Education Training Assistance Program (CETAP), underscoring the ongoing concerns.

Facts ...

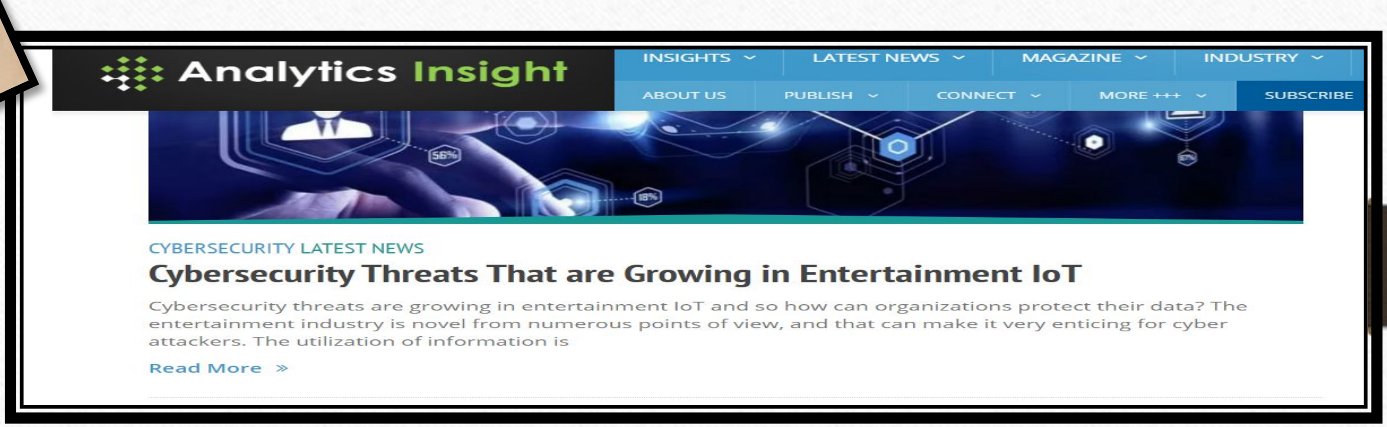


UK universities awarded funding for research into IoT, smart home security

Charlie Osborne 02 August 2021 at 10:58 UTC

IoT Research Education

Academics say that smart technology is a 'balancing act', and that consumers need to be aware of the risks

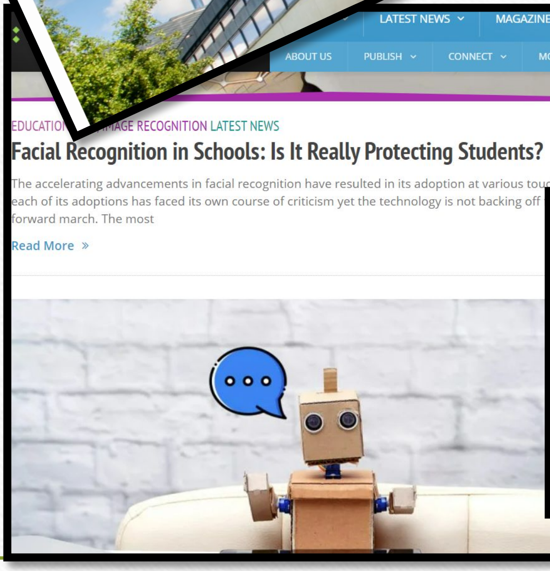


CYBERSECURITY LATEST NEWS

Cybersecurity Threats That are Growing in Entertainment IoT

Cybersecurity threats are growing in entertainment IoT and so how can organizations protect their data? The entertainment industry is novel from numerous points of view, and that can make it very enticing for cyber attackers. The utilization of information is

Read More »

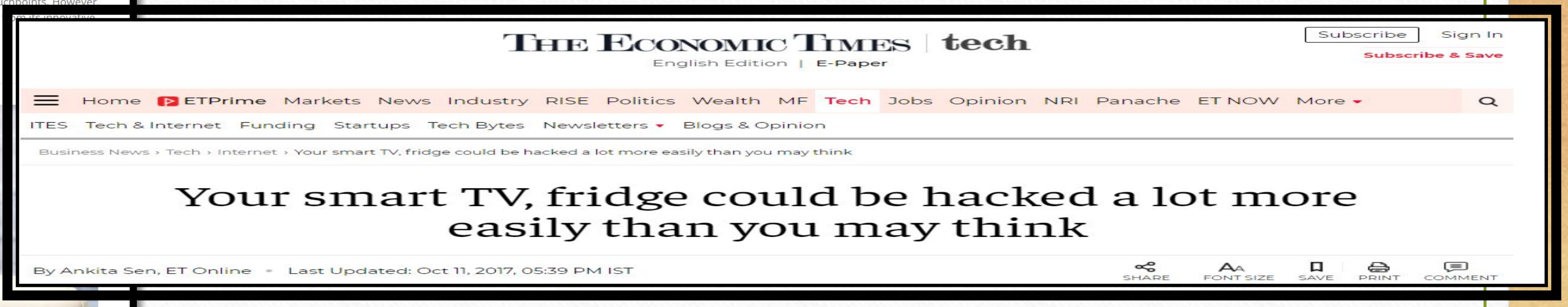


EDUCATIO IMAGE RECOGNITION LATEST NEWS

Facial Recognition in Schools: Is It Really Protecting Students?

The accelerating advancements in facial recognition have resulted in its adoption at various touchpoints. However, each of its adoptions has faced its own course of criticism yet the technology is not backing off from its innovative forward march. The most

Read More »



Business News › Tech › Internet › Your smart TV, fridge could be hacked a lot more easily than you may think

Your smart TV, fridge could be hacked a lot more easily than you may think

By Ankita Sen, ET Online • Last Updated: Oct 11, 2017, 05:39 PM IST

Facts …

- In Florida, there was a cybersecurity data breach through the security system of a virtual K-12 school that jeopardized the safety of the sensitive student and parent personal data.
- It included
  - names and birth dates of students
  - email addresses of the parents
  - Social Security numbers of the teachers.

The Reality …

As schools and universities continue to embrace connected devices, they must also stay up to date on threat intelligence and implement tools and policies to minimize connected device risks.

Top threats …

Mobile malware

- Students and teachers are using mobile phones / tabs for teaching learning process.
- Almost all such devices are having apps for
  - mobile banking /e-wallets/ UPI
  - social networking (WhatsApp , LinkedIn, Facebook, Telegram, Instagram etc.)
  - Health related apps
  - Maps / Cab services
- **26 percent** of detected malware specifically targeted mobile devices.

Top threats …

IoT Devices Exploits

- The devices that are commonly used for day to day work by teachers and students:
    - Printers
    - Routers
    - Web cameras
    - Microphones and Speakers
- Malware found targeting these devices to get personal and sensitive data.

Top threats ...

Crypto jacking

- Refers to cybercriminals using compromised devices to mine for cryptocurrency.
- Can harm performance and weaken security measures.
- Actively disable network security measures such as antivirus.

Top threats …

IoT botnets:

- Botnets are networks of remotely controlled devices, affected by malware, which can be manipulated by hackers.
- Can consist of hundreds and thousands of computers.
- Help hackers take over your home network devices and use them to perform illegal activities.
- Many IoT botnets are resilient and spread quickly.

Biggest hurdle in ensuring cyber safety for IOT devices

The **USERS** themselves

Devices such as laptops, smart home accessories and tablets often lack security or are not updated on a regular basis, making it vital for teachers to prioritize security when incorporating IoT devices into the classroom.

TOP IOT Vulnerabilities

According to OWASP (Open Web Application Security Project)

- ❑ Weak and guessable passwords
- ❑ Insecure networks and services
- ❑ Lack of secure update mechanisms
- ❑ Insecure or outdated components / hardware
- ❑ Insufficient privacy protection
- ❑ Insecure data transfer and storage
- ❑ Insecure default settings
- ❑ Lack of device management – No maintenance

Attackers take advantage of IOT Vulnerabilities (Examples)

- **Mirai Malware**
  - creates a botnet largely consisting of IoT devices.
  - Infects a device **through known default credentials** that allow access to the device.
  - Once inside, it forces the device to scan the internet for other vulnerable IOT devices
  - Once a sufficiently large botnet is made, they are typically used to launch a distributed denial of service (DDoS) attack on the organization.
- **St. Jude Medical's Merlin@home cardiac devices**
  - These devices included pacemakers and defibrillators.
  - Had the transmitters' vulnerability been exploited.
  - The battery could be drained rapidly, or the device could send shocks in the incorrect pace.

Tools and strategies to be considered by any educational institution

- Use Threat Intelligence and be aware of the types of attacks being used by cyber criminals

- Schools should leverage both local threat intelligence, based on what is going on in their networks, and worldwide threat intelligence.

Tools and strategies to be considered by any educational institution

- Take a "learn, segment and protect" approach to security.
  - To learn, schools must know about each device and their level of risk, connected to their network using a network access control tool.
  - IT teams can segment devices based on their risk and level of required access.
  - Once segmented, IT teams can protect by securely linking their new network segments together to maintain visibility of each device.

Tools and strategies to be considered by any educational institution

- To combat IoT botnets and crypto jacking, IT teams should try to locate, limit and interrupt communications between devices that allow botnets to thrive.

- For mobile malware, IT teams have to implement their own protective measures such as deploying mobile application security tools (OWASP ZAP, Drozer, QARK etc.)

Tools and strategies to be considered by any educational institution

- Regularly hold workshops for their staff, students and their parents to keep them updated on IOT threats and security measures.
- Go for regular maintenance of all digital devices and related software installed in the school.

Security Measures
(for individuals and educational institutions)

- Research the vendors of IoT devices
  - ensure they are reputable (may have to compromise on cost)
  - have a commitment to security with documentation.
- <u>Change default credentials</u>, using unique passwords:
  - IoT devices often require passwords for users to access services or control the device.
  - The default credentials of the devices can be weak, easy to guess, or hardcoded
    - embedded in the source code, unencrypted
    - to simplify setting up devices at scale, despite the significant risk to the device's security.
  - May use password managers

Security Measures
(for individuals and educational institutions)

- Use Two-factor authentication
  - creating new usernames and passwords, along with using an additional form of credential that an attacker is less likely to have access to.
  - increases the strength of credentials even further.
  - Especially helpful when it comes to malware like Mirai that uses known default credentials to quickly gain access to IoT devices.
- Keep the device's software up to date and install a comprehensive antivirus software
- Encrypt stored and transmitted data
  - Right click on folder->Properties -> Advanced-> Select Compress and Encrypt (Windows)
  - Use encryption tools (LastPass, BitLocker, VeraCrypt etc.)

Security Measures
(for individuals and educational institutions)

- Securing backend
  - The devices used to connect to a larger network ecosystem (for eg. – 5 G networks) can be compromised.
  - If not secure, no filtering of traffic coming in or going out from the device.
  - Use strong passwords and proper authentication / monitoring methods for your routers.
- Customize operating system (OS) platforms. Ensure account logins and proper privacy settings.
- Avoid use of third-party software and hardware that come from a compromised supply chain.

Security Measures
(for individuals and educational institutions)

- Do NOT use pirated software, especially movies, videos and games
- Store data on a secure device and in secure environment.
- Do not fall for offers and promotions and give your personal data– Remember Nothing Comes for free
- Switch off the smart devices when not in use

Security Measures
(for individuals and educational institutions)

- While teaching online:
  - Teachers should make sure that all financial / social networking or other personal apps are closed.
  - Regularly update your device and apps
  - Take care not to divulge any personal information to the students
  - Teachers and students should share their experiences with various IOT devices

To sum up…..

1. IoT devices are **vulnerable because they do not have the computational power to run security functions** and vendors may sacrifice security in the rush to market.
2. Organizations and individuals should **research the vendors** they buy from to ensure they are reputable and security-minded.
3. The best practice to secure a device is to **make new login credentials and use two-factor authentication** to access and control IoT devices.

THANK YOU