Future of Connected Devices

Featuring Guest Speaker: Dr. Mohamed Chouikha

In 2003 President Bush declared “The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace.” That same year a national strategic plan to secure cyberspace was published. In this talk, the presenter will discuss the relevance and the impact of cybersecurity since then. Illustrative example will be given to emphasis the importance of the creation of a unified view of cybersecurity based on existing and new tools. The presenter will also describe how PVAMU can be involved in this endeavor.

Join Us This Week, 10/26 - 10/30, for:

Tech Tuesday Tip on
Facebook & Twitter & Instagram

Special Guest Speaker - Dr. Mohamed Chouikha
Wednesday 10/28 at 11 am
Zoom meeting, check your PV Email

Cyber Security Capstone
Thursday, 10/29 at 1 pm
Zoom meeting, check your PV Email

Where we are headed:

Word wide spending on cyber security is expected to reach $133 billion in 2022.

Due to COVID-19 some employers are having to allow employees to use their personal devices for work and as a result organizations will focus on securing those devices.

Cyber-attacks are continuing to evolve due to hackers leveraging human behavior and Artificial Intelligence to improve attacks.

Mobile network providers are preparing for the transition from lte to 5G. The expanded capacity of 5G also means an influx of devices and breach points.

What can you do?

1. Install an antivirus solution on all your devices.
2. Use a VPN to stop strangers from accessing your data without permission & spying on your online activity.
3. Always be aware of what apps you are installing as many require access to your phones storage. If you notice unusual apps on your smart device or computer, uninstall them & monitor if they come back.
4. Trust but verify – Look for unusual data activity from your smart device, computer, etc.
5. Secure your network at home and work securely at work, this include paying attention to phishing emails.
6. Update the default back end passwords on all your IoT devices. Follow your device’s instructions on updating the “admin/password” style credentials of your gadgets. To find this information, consult with your manufacture’s tech manuals or contact them directly.

CITE
CENTER FOR INFORMATION TECHNOLOGY EXCELLENCE

Cyber Security Awareness Month

Each poster, post, email and session will have QR Codes to answer questions about Cyber Security as part of a month long scavenger hunt to win prizes!