**Material Development**

**1. Topic Information**

* **Title**: Mobile and IoT Security
* **Description**: Security of mobile devices, applications, and other IoT devices such as sensors and appliances.

**2. Learning Objectives**

* **Primary Objectives**:
  + Device Security Settings: Optimal configurations for security.
  + Secure IoT Configuration: Best practices for IoT device security.
  + Threats to Mobile Devices: Common threats and protection strategies.
  + Secure Mobile Payments: Ensuring safe mobile financial transactions.
  + Device Safety: Keeping devices secure with passwords and proper handling.
  + App Smarts: Choosing safe apps and understanding app permissions.
  + Downloading Apps: How to safely download and install apps from trusted sources.
  + App Permissions: Understanding and managing app permissions ensures they don’t overreach and compromise personal data.
* **Secondary Objectives**:
  + How to tell if an app or website is safe to use and download
  + Becoming more aware of where our data is stored and used by other companies, what is dangerous, and what is okay

**3. Target Audience**

* **Age Group**: This group is for all ages, but it can be focused more on teens through older adults, anyone who uses mobile devices and other IoT devices to download apps, manage finances, and use different data.
* **Skill Level**: Beginner, Intermediate, Advanced.
* **Specific Needs**: Uses mobile devices and IoT devices every day for a variety of purposes

**4. Material Types and Formats**

* **Main Format**: PowerPoint Presentation
* **Supplementary Materials**: Scenarios, questions, additional reading links, diagrams
* **Accessibility Features**: None applied, screen reader possible.

**5. Instructor Guide**

* **Synopsis**: There is a main interactive PowerPoint with information, examples, and activities.
* **Key Points**:
  + What are IoT and mobile devices, and how do we keep them safe?
  + How to bank safely online
  + Understanding safe apps and app permissions
* **FAQs**: Anticipated questions and their answers to prepare instructors.
  + How do IoT devices communicate with each other and the cloud?
    - Communication protocols like Wi-Fi, Bluetooth, Zigbee, and MQTT.
  + What are the key differences between edge computing and cloud computing in IoT?
    - Processing data locally (edge) versus centrally (cloud).
  + Can you give examples of industries other than smart homes where IoT is significantly used?
    - Examples include healthcare (remote patient monitoring), agriculture (smart farming), and manufacturing (predictive maintenance).
  + What are some real-world examples of DDoS attacks affecting IoT devices?\*\*
    - Mirai Botnet was a massive security breach caused by a malware worm that used a list of default usernames and passwords to hack into various devices and networks.
  + How can we secure an IoT device if the manufacturer does not update regular firmware?
    - Network segmentation, using third-party security solutions, or choosing different products.
  + What is the role of encryption in preventing data breaches?
    - Encryption is crucial in preventing data breaches by transforming readable data into an unreadable format that can only be deciphered with the correct decryption key.
  + How does 2FA work, and what are some common methods?
    - 2FA requires a second form of verification when a password is entered to verify the user’s identity. Some methods are SMS codes, authentication apps, and biometric verification.
  + What is the difference between TLS and SSL?
    - SSL is older and has more vulnerabilities. TLS was designed to remove those vulnerabilities and have stronger security.
  + What are the implications of a data breach for consumers and companies?
    - Effects on consumer trust, financial losses, and legal consequences for companies.
  + What should users look for in a secure financial app?
    - Features like encryption, secure coding practices, and strong user authentication.
  + What are the latest trends in mobile payment security?
    - Innovations like biometric verification, tokenization, and blockchain technology.
  + What are the risks of granting excessive permissions to mobile apps?
    - Potential for data leakage, privacy invasion, and misuse of personal information.
  + How can users stay informed about security vulnerabilities in the apps they use?
    - Following security news, enabling automatic updates, and checking developer advisories.
  + What should users do if they suspect an app is malicious after installation?
    - Multiple steps include uninstalling the app, running a security scan, and reporting it to the app store.

**6. Activities and Engagement Strategies**

* **Interactive Activities**: A PowerPoint presentation with questions and scenarios can be used to test knowledge or start discussions.
* **Engagement Tips**: There are some activities in the main PowerPoint presentation.

**7. Assessment**

* **Evaluation Method**: Quiz to test knowledge.
* **Success Criteria**: Be able to complete the activities in the leading PowerPoint, the quiz, and the scenarios correctly.

**8. Sources and References**

* **Primary Sources**:

[Icons Used in PowerPoint](https://creativemarket.com/eucalyp)

[Pictures Used in PowerPoint](https://creativemarket.com/eucalyp)

Websites Used for Research:

[What Is IoT Architecture? Guide And Examples | MongoDB](https://www.mongodb.com/resources/basics/cloud-explained/iot-architecture)

[23 IoT Devices Connecting the World | Built In](https://builtin.com/articles/iot-devices)

[What Is IoT Cybersecurity | CompTIA](https://www.comptia.org/content/articles/what-is-iot-cybersecurity)

[What Is a DDoS Attack and How Does It Work | Cybersecurity | CompTIA](https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works)

[What Is Malware - How to Prevent and Remove It | Cybersecurity | CompTIA](https://www.comptia.org/content/articles/what-is-malware)

[How to Protect Connected Home Devices and Appliances from Cyber Attacks - IoT Security Foundation](https://iotsecurityfoundation.org/how-to-protect-connected-home-devices-and-appliances-from-cyber-attacks/#:~:text=Utilization%20of%20security%20protocols%20like,configuration%2C%20or%20other%20sensitive%20information).

[A Guide to the 12 Most Common IoT Protocols & Standards](https://www.datamation.com/applications/iot-protocols-and-standards/)

[The Risks of Mobile Banking Apps: Keep Your Money Safe](https://www.identityguard.com/news/risks-of-using-mobile-banking-apps)

[How To Spot Fake Apps: App Size, Permissions, Source](https://www.aura.com/learn/how-to-spot-fake-apps)

[What are fake apps? How to identify and avoid fake apps](https://www.comparitech.com/blog/information-security/what-are-fake-apps/)

[Understand app privacy & security practices with Google Play's Data safety section - Android](https://support.google.com/googleplay/answer/11416267?hl=en&co=GENIE.Platform%3DAndroid#zippy=)

* **Suggested Further Reading**: Any websites used are good for further reading and go more in-depth than PowerPoint.

**9. Legal and Compliance Checks**

* **Copyright Compliance**: Ensuring all used materials are correctly licensed or credited. All pictures or icons not taken by me have been credited with the website below. All images used are free to use and only have to be credited.
* **Privacy Considerations**: Ensuring content complies with privacy laws, especially if the personal data of learners might be involved. Personal data of learners is not required to be used.

**10. Technology Requirements**

* **Needed Software or Hardware**: Computer or device with access to Google Slides.
* **Technical Support Resources**: If slides are broken or misplaced, my email is [Kaylee Maczek](mailto:kaylee53@iastate.edu). Other technical support depends on the device being used.

**11. Feedback Mechanism**

* **For Learners**: kaylee53@iastate.edu
* **For Instructors**: kaylee53@iastate.edu

**12. Review and Update Schedule**

* **Review Frequency**: Most content here should be good for a few years. However, technology is ever-changing, so it is suggested that the material be checked once or twice a year.
* **Update Protocols**: Edit the slides to update information.

**13. Delivery Modalities**

* **Online**: Through multiple shared Google Slides, the content can be accessed.
* **In-Person**: Presenting the Google Slides is a good way to use them in person.
* **Hybrid**: Slides can be shared from the instructor's screen on an online call or presented for in-person meetings. Slides can also be given to the learners for their use as well.

Blooms taxonomy: <https://www.celt.iastate.edu/instructional-strategies/effective-teaching-practices/revised-blooms-taxonomy/>