**About the Assignment**

In this assignment, you will design a cybersecurity awareness campaign for your own company or organization.

* Research the common cyberattacks that affect your industry or sector and their consequences, and then create a presentation that teaches your colleagues about the importance of cybersecurity and how to protect themselves and their company or organization from cyber threats.
* You may include some tips and best practices for reducing the attack surface and enhancing the CIA triad. Please share some resources or links for further learning in cybersecurity.
* Additional information and tips:
  1. Consider the use of tools such as PowerPoint, Prezi, Canva, Animoto, etc. to make your campaign more engaging and appealing.
  2. For the research part, make use of online resources, such as the Verizon Data Breach Investigations Report, the CrowdStrike Global Threat Report, the MITRE ATT&CK Group's page, etc., to find out what types of attacks are most prevalent and impactful in your domain. You could also use some examples or case studies of real incidents or breaches that illustrate the severity and cost of cyberattacks.
  3. When teaching your colleagues about protecting themselves from cyberattacks, be sure to include tips and best practices for employees from websites such as Cybersecurity Ventures, CyberSeek, etc.

**Notes for Submitting Your Assignment**

Please upload your work below once you have finished.

While you can make your own decision on which format to use, please make sure that it does not exceed ten pages/slides.

Please note: this is individual work.

Rubric

**Assignment A3.1 Rubric**

| Assignment A3.1 Rubric | | |
| --- | --- | --- |
| **Criteria** | **Ratings** | **Pts** |
| This criterion is linked to a learning outcomeResearch on cyberattacks | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Comprehensive research on prevalent attacks in the industry. Used multiple reputable sources. | **4 Pts**  **Proficient**  Adequate research on most prevalent attacks. Used a few reputable sources. | **3 Pts**  **Basic**  Limited research with missing key attacks. Relied on few sources. | **2 Pts**  **Needs improvement**  Minimal or no research. Relied on one or no reputable sources. | | 5 pts |
| This criterion is linked to a learning outcomePresentation quality | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Engaging, clear, and professionally presented. Effective use of visuals and narration. | **4 Pts**  **Proficient**  Organized and mostly clear. Good use of visuals and narration. | **3 Pts**  **Basic**  Some organization but lacks clarity in places. Limited use of visuals. | **2 Pts**  **Needs improvement**  Disorganized, unclear, or lacking in visuals and narration. | | 5 pts |
| This criterion is linked to a learning outcomeEducational content | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Comprehensive coverage of cybersecurity importance, protection methods, and best practices. Demonstrated deep understanding. | **4 Pts**  **Proficient**  Adequate coverage of most aspects. Demonstrated understanding. | **3 Pts**  **Basic**  Limited coverage with some gaps in content. Some understanding shown. | **2 Pts**  **Needs improvement**  Minimal or no coverage. Lack of understanding evident. | | 5 pts |
| This criterion is linked to a learning outcomeUse of tools | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Effective and creative use of tools like PowerPoint, Prezi, Canva, etc. has ehanced the campaign's appeal. | **4 Pts**  **Proficient**  Adequate use of tools to support the campaign. | **3 Pts**  **Basic**  Limited use of tools, with missed opportunities to enhance appeal. | **2 Pts**  **Needs improvement**  Minimal or no use of tools. Campaign lacks appeal. | | 5 pts |
| This criterion is linked to a learning outcomeReal-life examples/case studies | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Incorporated multiple relevant examples/case studies to illustrate severity and cost of attacks. | **4 Pts**  **Proficient**  Incorporated some relevant examples/case studies. | **3 Pts**  **Basic**  Limited use of examples/case studies or not entirely relevant. | **2 Pts**  **Needs improvement**  No use of examples/case studies. | | 5 pts |
| This criterion is linked to a learning outcomeTips and best practices | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Comprehensive, well-reasoned tips and best practices based on reputable sources. Demonstrated deep understanding. | **4 Pts**  **Proficient**  Adequate tips and best practices based on some reputable sources. Demonstrated understanding. | **3 Pts**  **Basic**  Limited tips and best practices with some gaps in reasoning. | **2 Pts**  **Needs improvement**  Minimal or no tips and best practices. | | 5 pts |
| This criterion is linked to a learning outcomeResources for further learning | |  |  |  |  | | --- | --- | --- | --- | | **5 Pts**  **Full points**  Provided multiple relevant resources/links for further learning in cybersecurity. | **4 Pts**  **Proficient**  Provided some relevant resources/links. | **3 Pts**  **Basic**  Limited resources/links provided or not entirely relevant. | **2 Pts**  **Needs improvement**  No resources/links provided. | | 5 pts |
| Total points: 35 | | |