SAINT LUCIA CONNECTED DIGITAL SKILLS YOUTH INTERNSHIP
Digital Skills Training

Workshop Title: Understanding and Addressing Cybersecurity for Teens

Prerequisites:

1. Good communication skills.
2. The willingness to take on a new challenge
3. The ability to work with a team.

Description

This 12-hour workshop aims to introduce cybersecurity basics to young persons with limited prerequisite skills and knowledge. Covering essential aspects of cybersecurity in the context of personal and school-based digital tool use, the workshop employs a hands-on, interactive approach to ensure students grasp and apply the concepts effectively. The workshop will provide students a glimpse into various cybersecurity careers, engage them in fun, challenging activities, and highlight the importance of cybersecurity in the digital age.

Learning Outcomes:

In this workshop participants will:

1. Discuss the importance of cybersecurity and implications in their personal and professional activities.
2. Identify common cybersecurity threats, risks, and vulnerabilities associated with the use of digital tools and online platforms.
3. Apply basic strategies to protect digital devices and data, including secure password creation, data backup, and understanding of phishing attacks.
4. Identify the security features and potential vulnerabilities of different Operating Systems.
5. Discuss various cybersecurity roles and career paths.
6. Develop a proactive approach and personal responsibility in maintaining safe practices online.

Session	Learning Outcomes	Suggested Activities
	Discuss the importance of cybersecurity and implications in their personal and professional activities.	**Introduction to Cybersecurity (15 minutes)** Start the session with a brief discussion on what cybersecurity is, why it is important, and the consequences of not taking cybersecurity seriously. This will set the stage for the rest of the activities. **Cybersecurity Mythbusters (30 minutes)** In this interactive activity, you will debunk some common myths about cybersecurity. Create a quiz using a platform like Kahoot or Quizlet, where participants have to identify whether a statement about cybersecurity is a myth or fact. This activity aims to clarify misconceptions about cybersecurity and enhance their knowledge in a fun and engaging way. Myths vs Facts: Cybersecurity in a Digital World **Password Puzzles (30 minutes)** This activity will highlight the importance of using strong passwords. First, provide a brief overview of the criteria for creating strong passwords. Then, divide participants into teams and challenge them to create the strongest password. The teams will present their password (without revealing the actual password, but explaining their strategy), and the rest of the group votes on which one they think is the strongest based on the presented criteria. **Phishing Detective (30 minutes)** Create a set of fictitious emails, some of which are examples of phishing attempts. Ask the participants to identify which emails are phishing and

Session	Learning Outcomes	Suggested Activities
		discuss why. This exercise helps the students learn how to spot phishing emails and avoid becoming victims of such scams. **Cybersecurity Game (15 minutes)** Conclude the session with an online game that tests the participants' knowledge of cybersecurity. For example, the "Football Fever: Secure the Win" game allows participants to lead a football team to victory by making informed cybersecurity decisions. This fun activity reinforces the lessons learned in a fun and engaging way. **Wrap Up and Discussion (15 minutes)** Conclude the session with a wrap-up of what was learned and an open discussion about the activities. Reinforce the importance of being cyber smart in both their personal and professional lives. Encourage them to share their newfound knowledge with their friends and family members to spread the importance of cybersecurity. Resources: ● Why should you teach cybersecurity to your kids? ● What teenagers need to know about cybersecurity ● Digital safety and security tips for college students and teens ● Cybersecurity Awareness: What It Is And How To Start
	Identify common cybersecurity threats, risks, and vulnerabilities associated with the use of digital tools and online platforms.	**Cybersecurity True or False (15 minutes)** Start with an engaging ice-breaker game to familiarize participants with cybersecurity terms and concepts. Prepare a series of statements about cybersecurity (using information from resources below), and ask the students to guess if they're true or false.

Session	Learning Outcomes	Suggested Activities
		Introduction to Cybersecurity (20 minutes) Give a brief introduction to cybersecurity, threats, risks, and vulnerabilities using the information from Security 101: Vulnerabilities, Threats & Risk Explained. Use simple language to explain these concepts and make sure to relate them to students' daily use of the internet and social media. **Cyber Threat Theater (30 minutes)** Split the group into smaller teams and assign each a common cyber threat (like phishing, malware, cyberbullying, online scams). Ask them to prepare a short skit demonstrating the assigned threat and how it can be mitigated. They can use the information provided in the following resources: ● Digital safety and security tips for college students and teens ● What teenagers need to know about cybersecurity **Hands-On: Cybersecurity Survivor (30 minutes)** For this activity, prepare scenario cards featuring various cybersecurity threats. students must work in their teams to identify the threat, discuss the risk and vulnerability, and propose ways to mitigate it. They can use their devices to research and find solutions, which will also help them in understanding how to find reliable cybersecurity resources online. The team that solves the most scenarios correctly wins the "Cybersecurity Survivor" title. ● Best Cybersecurity Lessons and Activities for K-12 Education **Discuss and Reflect (15 minutes)** Discuss the scenarios and solutions provided by the students. Reflect on why certain solutions are effective and how others could be improved.

Session	Learning Outcomes	Suggested Activities
		Highlight the importance of being aware of threats and risks while using the internet and social media. Use the following resource: Healthy Lifestyle: Tween and teen health. **Real-world Applications and Further Learning (15 minutes)** Discuss the opportunities for further learning, like cybersecurity competitions, workshops, and online courses [6]. Finally, ask students to make a personal commitment to apply at least one learned cybersecurity principle in their daily digital activities. Resources: ● Healthy Lifestyle: Tween and teen health ● Why should you teach cybersecurity to your kids? ● What teenagers need to know about cybersecurity ● Digital safety and security tips for college students and teens ● Cybersecurity Awareness: What It Is And How To Start ● Security 101: Vulnerabilities, Threats & Risk Explained ● Learning Cybersecurity: Competitions and Workshops for Teens
	Apply basic strategies to protect digital devices and data, including secure password creation, data backup, and understanding of phishing attacks.	**Digital Safety Basics (20 minutes)** Begin the activity with a review of the importance of digital safety. Highlight the various risks that are present in the digital world, such as malware, phishing, cyberstalking, and social engineering, referencing information from the provided sources: ● Digital safety and security tips for college students and teens ● What You and Your Teen Need to Know About Cyberstalking ● Phishing Attacks: A Recent Comprehensive Study and a New Anatomy ● Spoofing and Phishing

Session	Learning Outcomes	Suggested Activities
		Password Creation Game (20 minutes): Have the students participate in a fun game to understand the importance of password creation. The students can be divided into teams and are given the challenge to create a complex password. The facilitator can use the tips from the following resource to guide them and later score their passwords based on complexity, uniqueness, and strength. ● Password Safety: Top Ten Tips for Teens **Data Backup Interactive Session (30 minutes)** Show a short video or animation on the importance and methods of data backup. Then, encourage them to share their current practices of backing up data, and discuss different ways to do it effectively. Encourage them to set up automatic backups on their devices if they have not done so already. ● Video: What Is Data Backup? Why Do We Need Data Backup? **Phishing Attack Role-play (40 minutes)** Create a role-play scenario involving phishing attacks, incorporating knowledge from [3], [4], [6], and [9]. The students can be divided into groups with some acting as phishers and others as potential victims. The phishers must plan a phishing attack (without actually implementing it), and the potential victims must recognize and prevent the attack. After the role-play, discuss the tactics used and how to avoid them. **Phishing Attack Role-play (40 minutes)** Create a role-play scenario involving phishing attacks, incorporating knowledge from the resources listed. The students can be divided into groups with some acting as phishers and others as potential victims. The

Session	Learning Outcomes	Suggested Activities
		phishers must plan a phishing attack (without actually implementing it), and the potential victims must recognize and prevent the attack. After the role-play, discuss the tactics used and how to avoid them. • Phishing Attacks: A Recent Comprehensive Study and a New Anatomy • Spoofing and Phishing • How to Recognize and Avoid Phishing Scams • Phishing Attacks: 18 Examples and How to Avoid Them **Wrap up - Open Discussion (10 minutes)** End the session by allowing students to share their thoughts, experiences, and learning. Discuss online behavior, the potential consequences of social media misuse, and the importance of awareness, referencing the guide Social Media - Teen Use and Abuse. Also, stress the importance of seeking help when needed, and provide them with resources and contacts to report any digital threats they might encounter.
	Identify the security features and potential vulnerabilities of different Operating Systems.	*For this session students will need access to devices with different operating systems installed: Windows, macOS, Linux, Android.* **Introduction (10 minutes)** 1. Welcome the participants and provide a brief overview of the importance of understanding operating system security. 2. Explain the objectives and expected outcomes of the workshop. Operating System Overview (20 minutes) Present a high-level introduction to different operating systems, such as Windows, macOS, Linux, and Android.

Session	Learning Outcomes	Suggested Activities
		Discuss the unique features, market share, and common usage scenarios of each operating system. Highlight the importance of security in operating systems and its impact on personal privacy and data protection. **Security Features Exploration (30 minutes)** 1. Divide participants into small groups (3-4 members per group). 2. Assign each group a specific operating system to focus on. 3. Provide access to computers or laptops with the assigned operating systems. 4. Instruct the groups to explore and identify the built-in security features of their assigned operating system. 5. Encourage them to make a list of the features and discuss their purposes and benefits. **Vulnerability Analysis (45 minutes)** 1. Introduce the concept of vulnerabilities in operating systems and their potential risks. 2. Explain common types of vulnerabilities (e.g., misconfigurations, outdated software, weak passwords) using information provided from the following source: 7 Most Common Types of Cyber Vulnerabilities - CrowdStrike. 3. Guide the groups to conduct online research to identify specific vulnerabilities associated with their assigned operating system. 4. Instruct them to create a presentation or a poster that highlights the vulnerabilities, potential risks, and suggested mitigation strategies. **Group Presentations (30 minutes)** 1. Ask each group to present their findings on the security features and vulnerabilities of their assigned operating system.

Session	Learning Outcomes	Suggested Activities
		2. Encourage them to engage the audience by explaining their research and answering questions. 3. Facilitate discussions among the groups and allow for knowledge sharing and cross-learning. **Wrap-up and Conclusion (5 minutes)** 1. Summarize the key takeaways from the activity. 2. Highlight the importance of maintaining a strong security posture and staying updated with the latest security practices. 3. Provide additional resources or references for further exploration. Resources: ● What Is Operational Security? OPSEC Explained | Fortinet ● Mobile Security: Threats and Best Practices ● How to Identify and Prepare for Network Security Threats and Vulnerabilities ● 7 Most Common Types of Cyber Vulnerabilities - CrowdStrike ● Security Awareness Training: 6 Important Training Practices
	Discuss various cybersecurity roles and career paths.	
	Develop a proactive approach and personal responsibility in maintaining safe practices online.	