



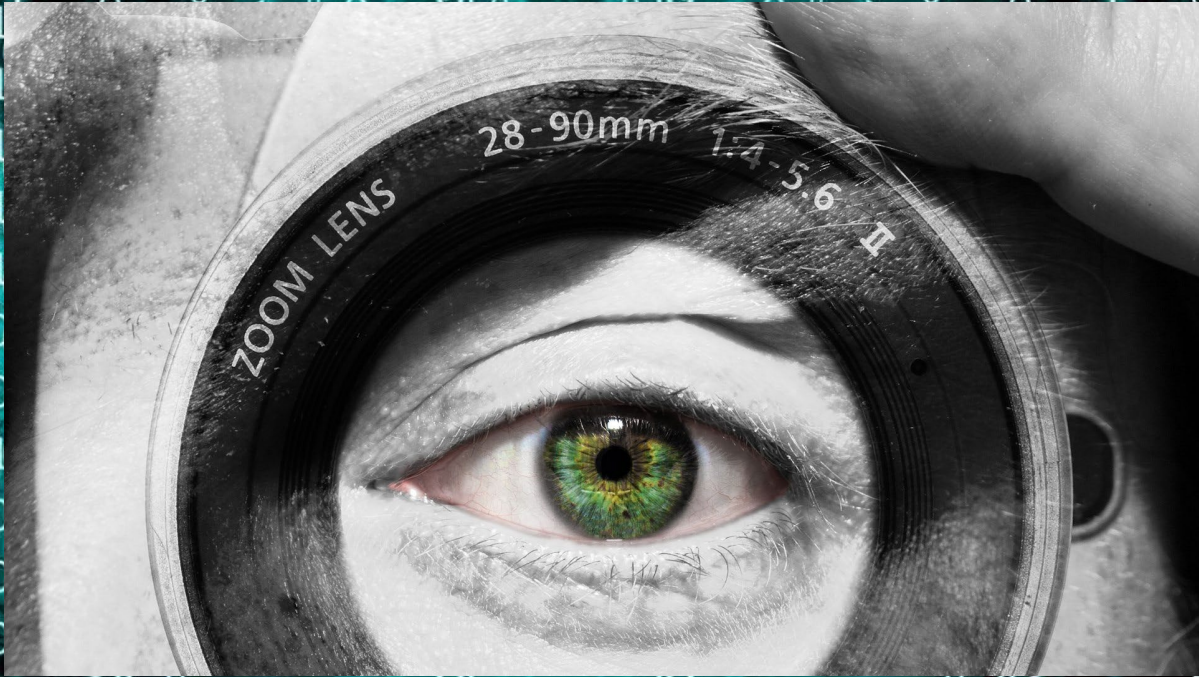
SCHOOL SAFETY SUMMIT

JUNE 15, 2023



RAISING CANE'S RIVER CENTER | BATON ROUGE, LA

Examining School Safety Through the Lens of Cybersecurity: A Different Approach



Objectives

1. Attendees will become familiar with CYBER.ORG's grant funded (CTE) curricula and Cyber Range.
2. Attendees will understand what the Cyber Range is and its purpose.
3. Attendees will learn how a Cyber Range creates real-world experiences for students in the classroom.
4. Attendees will understand the connection between Cybersecurity and School Safety.

Agenda

- LET'S GO!!!! Credential Harvesting Lab
- Cybersecurity and School Safety
- Who are we?
- What do we offer?
- Explore the Cybersecurity Course
- What is the CYBER.ORG Cyber Range?
- Closure

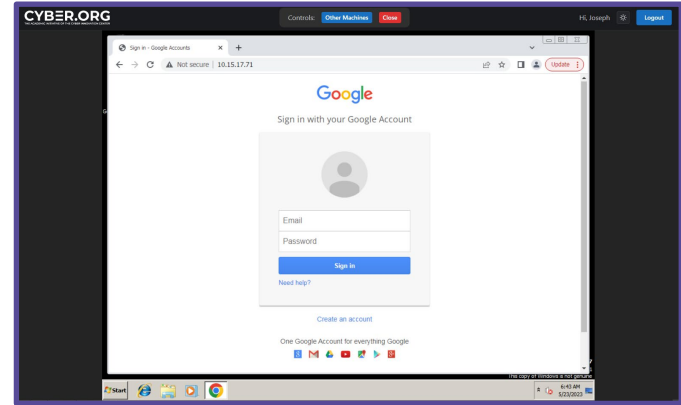
CYBER.ORG Cyber Range Credential Harvesting Lab

The screenshot displays the web interface for the CYBER.ORG app at the URL `apps.cyber.org/classrooms`. The header includes the CYBER.ORG logo with the tagline "THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER", the user name "Hi, Joseph", a settings icon, and a "Logout" button. A left-hand "Admin Panel" sidebar lists navigation options: "Your Dashboard", "Applications", "Users", "Classrooms", "Instance Types", and "Instances". The main content area is titled "Classrooms" and features a breadcrumb "Home / Classrooms" and an "Add a Classroom" button. Below this, three classroom cards are visible: "Joe Class", "Class 2", and "Test Classroom".



What is Credential Harvesting?

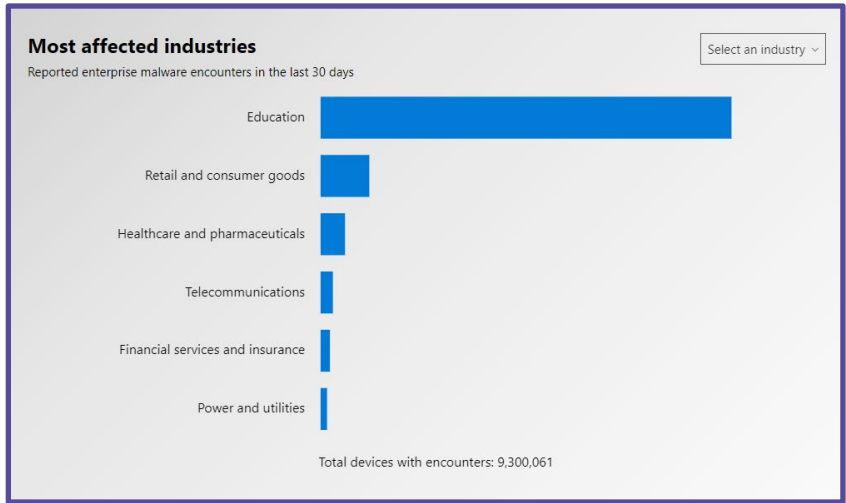
- A malicious actor attempting to obtain log-in credentials from victims
 - Create a fake website
 - Clone of a real website
 - Get the victim to visit the website
 - Victim enters their username/password
 - Does not actually authenticate
 - Malicious actor sees their username/password



Partnering to Safeguard K-12 Organizations from Cybersecurity Threats

Cybersecurity and Infrastructure Security Agency (CISA) - January 2023

There is no more important institution to the future prosperity and strength of the United States than our nation's K-12 education system. K-12 schools and school districts have adopted advanced networking technologies that facilitate learning and make schools more efficient and effective. This technological gain, however, has introduced heightened risks. Malicious cyber actors are targeting K-12 education organizations across the country, with potentially catastrophic impacts on students, their families, teachers, and administrators.



From: Microsoft (May 2023)



Cybersecurity and School Safety...

- There has been a 300% increase in cybercrimes since the beginning of COVID-19, according to the U.S. FBI.
- 62% of nearly 5.8 million malware cases reported came from the education sector (Microsoft Security Intelligence, 2023).
- The number of K-12 students taking online courses is now approximately 4.5 million, a radical number given that online enrollment in 2000 was fewer than 50,000 students (OnlineSchools.org, 2023).



Cybersecurity and School Safety...

- As well as the threats all users face when going online, such as computer viruses and email scams, students are at risk from the following:
 - Cyberbullying
 - Inappropriate Content
 - Sexting
 - Sextortion/Ransomware
 - Oversharing
 - Online Predation
- [Cyberthreats, viruses, and malware - Microsoft Security Intelligence](#)

Who is CYBER.ORG?

- Who is CYBER.ORG?
 - Funded by CISA (CETAP)
 - Help close the workforce shortage
 - National security problem
- Who am I?
 - Willie Henderson, M.Ed.
Cyber Education Specialist
Louisiana CYBER.ORG Range Specialist

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER





The nation has a critical cybersecurity workforce shortage.
Efforts to close the cyber workforce gap **MUST** begin in K-12 classrooms.

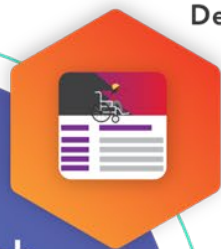
Our Impact
as of March 2022

- **25,000+** teachers enrolled in CYBER.ORG content from 50 states and 4 US territories
- **3.4 million** students currently impacted by CYBER.ORG content
- ▶ **19,000+** teachers trained to teach cybersecurity both through in-person and virtual professional development

Cultivate State Partnerships



Develop Classroom Resources



Our Approach

Supporting K-12 educators and students to build foundational cybersecurity awareness, cyber career awareness, and technical cybersecurity skills.

Support Student & Community Events



Lead Professional Development



Our Goal:
Cyber Education for All Students
By ensuring that all students receive a cybersecurity education, we build a steady stream of cyber-literate students who are prepared for the workforce after school.

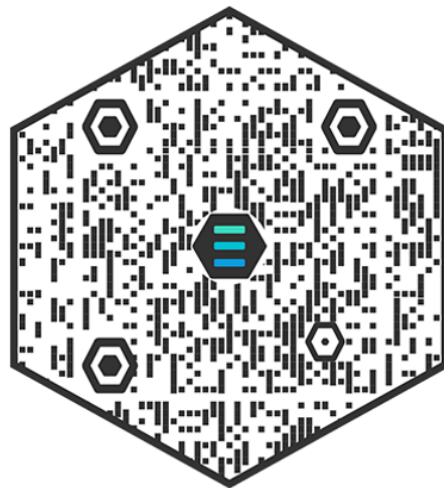


CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

NO-COST CYBERSECURITY CLASSROOM RESOURCES

CLASSROOM CONTENT
PROFESSIONAL DEVELOPMENT
CAREER AWARENESS



Cybersecurity Courses

Introductory Technology Courses

Integrated Cybersecurity Courses

Cybersecurity



Cybersecurity Basics



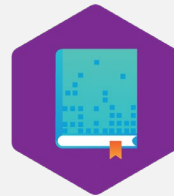
IT Fundamentals



Coding Fundamentals



Cyber Literacy



Robotics in the Classroom



Cyber Society



Science +



Computational Thinking



STEM EDA



What is the Cybersecurity Course?

- Lays a foundation of understanding all the essential knowledge and skills needed to begin a future in the cyber workforce.
- Part of LDOE's Cyber Security Jump Start Pathway
- Prepares students for Industry Based Certifications: CompTIA Security+



The screenshot shows a website for a Cybersecurity course. The header features the title "Cybersecurity" and a subtitle "Understanding the interconnectedness of devices and how to protect them". A navigation bar includes "Home" and "Course Information". Below this is a "Support Materials" section with a table listing resources. A "Supplemental Materials" section follows with another table of links.

Lesson Name	Teacher Notes	Resources
Course Teaching Guide	Teaching Guide Suggested Order	Lab Descriptions Case Study Descriptions Cybersecurity Syllabus - Example Case Study - Cybersecurity Salaries
Student Acceptable Use Policy		Acceptable Use Policy
CompTIA Security+ Information		SYO-601 Objectives

Lesson Name	Teacher Notes	Lessons	Resources
Linux Materials			Linux Cheat Sheet Lab - Fun with Linux



Security+ Objectives

- Aligned to CompTIA's SY0-601 Objectives
 - Exam will be updated in 2025
- Covers threats, attacks, vulnerabilities, risk management, cryptography, PKI, access management, etc.
- Experience is recommended
 - **Two years of experience in IT administration with a security focus**
- \$392 per exam (Vouchers available: District CTE Funds)
- Certificate is good for 3 years
- Pros and Cons: Looks amazing on a resume and less content than A+; difficult for some students





CYBER.ORG

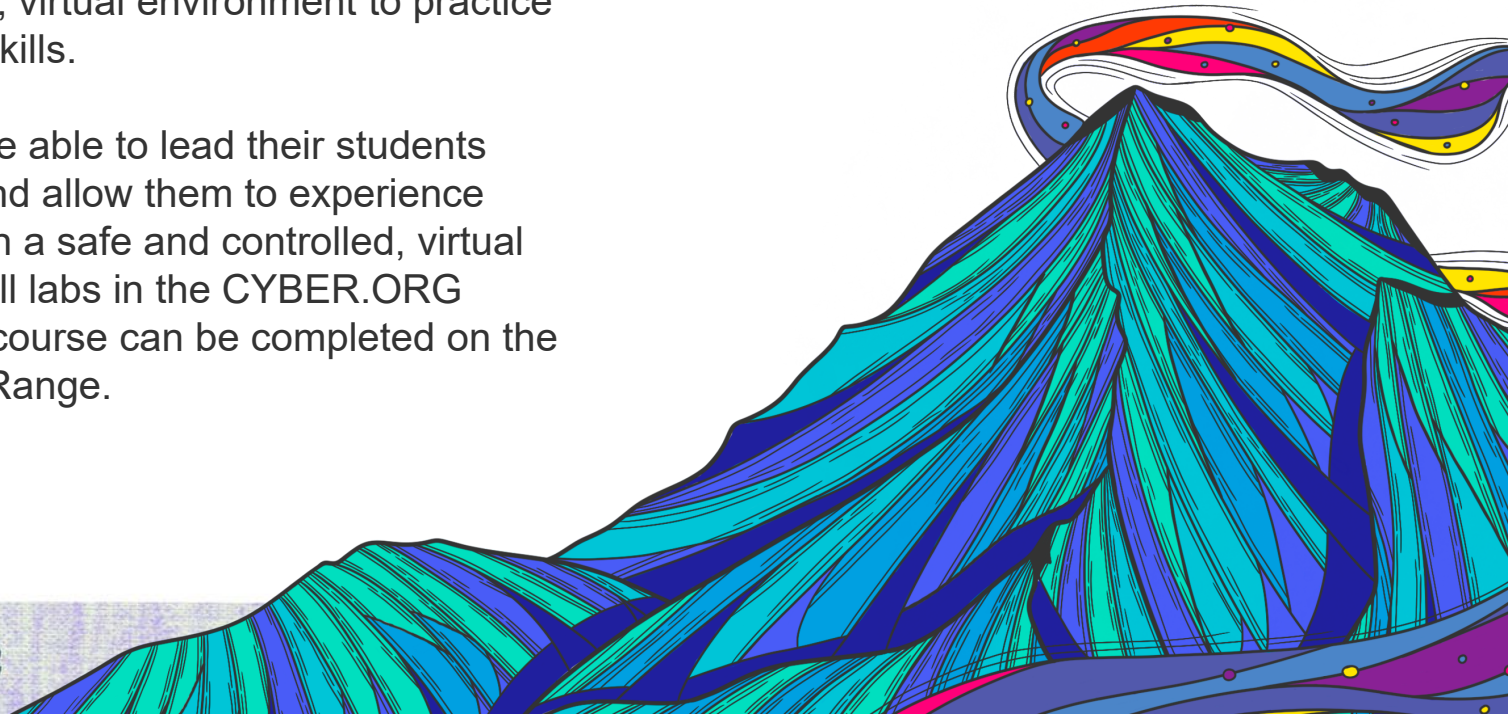
RANGE

A no-cost, safe, virtual environment to practice cybersecurity skills.

Teachers will be able to lead their students through labs and allow them to experience cyber-attacks in a safe and controlled, virtual environment. All labs in the CYBER.ORG Cybersecurity course can be completed on the CYBER.ORG Range.



 Believes



The CYBER.ORG Range

- Cloud hosted
- Browser based
- No software to install
- Scalable
- Engaging
- Interactive
- **No-Cost** to all US K-12 Educators

The screenshot displays the CYBER.ORG user interface. At the top, it says 'CYBER.ORG THE EDUCATIONAL INITIATIVE OF THE CYBER INNOVATION CENTER' and includes a 'Logout' button. Below this is a 'Current VMs' section with two entries: 'Kali' (IP: 10.15.88.76) and 'Windows 7' (IP: 10.15.110.106). Each entry has 'Connect' and 'Terminate' buttons and an 'Expires At: 23:59' indicator. A third section, 'Available to Launch', is partially visible. In the foreground, a terminal window shows a Netmap scan of the Kali VM. The terminal output includes: 'global options: <code>ncmd</code>', 'got answer:', '==>HEADER<<- opcode: QUERY, status: NXRROR, id: 28731', 'flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1', 'OPT PSEUDOSECTION:', 'EDNS: version: 0, flags: 0, udp: 4096', 'QUESTION SECTION:', 'cyber.org. IN A', 'ANSWER SECTION:', 'cyber.org. 300 IN A 23.185.0.2'. Below this, a 'Query 1' section shows 'Host is up (0.000095s latency). Not shown: 998 closed ports. PORT STATE SERVICE 22/tcp open ssh 3389/tcp open vnc-1'. The scan is completed in 0.08 seconds. In the background, a browser window shows the CYBER.ORG website with a 'Browse Free Cyber Curricula' pop-up.



 Believes

Using the Range for Experience

- “Example” Labs - Fuzzing Lab
 - Learn what fuzzing is
 - Learn how to use fuzzing
 - Also use OWASP-ZAP
 - And SQL Injection

Size	Resp. Body	State	Payload
4,298 bytes		Reflected	1 uni/*
4,332 bytes		Reflected	1;(load
4,519 bytes		Reflected	' ' 6
4,549 bytes		Reflected	' or '1'='1
4,549 bytes		Reflected	' or 1=1--
4,549 bytes		Reflected	' or '1'='1
4,549 bytes		Reflected	' or 'a'='a
4,554 bytes		Reflected	1' or '1'='1
4,579 bytes		Reflected	' or '7659'='7659
4,579 bytes		Reflected	' or '7659'='7659
4,589 bytes		Reflected	anything' or 'x'='x

View the GET Request

- Navigate back to OWASP-ZAP application
- Click on History
- Double click on the last GET under the Method column
 - You should see the “SQLCOMMANDS” show up in the GET request

History

Double click the last GET under the Method column

Verify “SQLCOMMANDS” appears in the GET request

CYBER.ORG



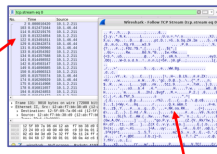
Believes

Using the Range for Experience

- “Tool” Labs - Wireshark Lab
 - Learn how to capture packets, view packets, and understand packets
 - Understand the risks of using the internet “in a café”

Follow TCP Stream

- Find a Packet
 - Find a TCP Protocol packet if possible
- Right-Click on the packet
- Go to the “follow” option
- Select the “TCP Stream” option
- The window shows all the data from this stream
 - Stream = multiple packets that make up an exchange of data
- The main Wireshark window is displaying all the packets in this stream
- What are you seeing?
 - This is a webserver communicating with a browser
 - Each website you visit carries out a similar exchange



All the packet's data

Seeing a Capture

- In Wireshark, search for the following in the display filter up top

```
ip.addr == <IP Address>
```

- Use the IP Address of device you pinged

No.	Time	Source	Destination	Protocol	Length	Info
13349	12.138877916	10.1.44.4	10.1.44.6	ICMP	98	Echo (ping) request [eth0/0.0.0.0] seq=1725
13350	12.138877916	10.1.44.6	10.1.44.4	ICMP	98	Echo (ping) reply [eth0/0.0.0.0] seq=1725
14602	13.146607518	10.1.44.4	10.1.44.6	ICMP	98	Echo (ping) request [eth0/0.0.0.0] seq=2761
14603	13.146607519	10.1.44.6	10.1.44.4	ICMP	98	Echo (ping) reply [eth0/0.0.0.0] seq=2761
15816	14.164852181	10.1.44.4	10.1.44.6	ICMP	98	Echo (ping) request [eth0/0.0.0.0] seq=5776
15817	14.164852189	10.1.44.6	10.1.44.4	ICMP	98	Echo (ping) reply [eth0/0.0.0.0] seq=5776
16660	15.187998582	10.1.44.4	10.1.44.6	ICMP	98	Echo (ping) request [eth0/0.0.0.0] seq=6718
16661	15.187998584	10.1.44.6	10.1.44.4	ICMP	98	Echo (ping) reply [eth0/0.0.0.0] seq=6718
17222	16.212642993	10.1.44.4	10.1.44.6	ICMP	98	Echo (ping) request [eth0/0.0.0.0] seq=9712
17223	16.212642998	10.1.44.6	10.1.44.4	ICMP	98	Echo (ping) reply [eth0/0.0.0.0] seq=9712



CYBER.ORG

CYBER.ORG



Believes

Using the Range for Experience

- “Attack” Labs - Ransomware Lab
 - Use the actual WannaCry payload
 - Understand how a ransomware attack works
 - Understand how to defend against a ransomware attack

Get the Ransomware File

- Navigate into theZoo directory
 - `cd theZoo`
 - Use ls to see the contents of theZoo directory
 - Open theZoo Repository
 - `python theZoo.py`
 - Type “YES” when prompted
 - You should see the `mdb #>` prompt
 - You are in theZoo Repository

```
student@kali:~$ cd theZoo/
student@kali:~/theZoo$ ls
LICENSE.md  README.md  theZoo.py
student@kali:~/theZoo$ python theZoo.py
Type YES in capital letters to accept
> YES
In t
mdb #>
```



Believes

Sign-up for our curricula
[Curricula Sign Up | Cyber.org](https://www.cyber.org/curricula-sign-up)

Click the sign-up button in the
top right corner

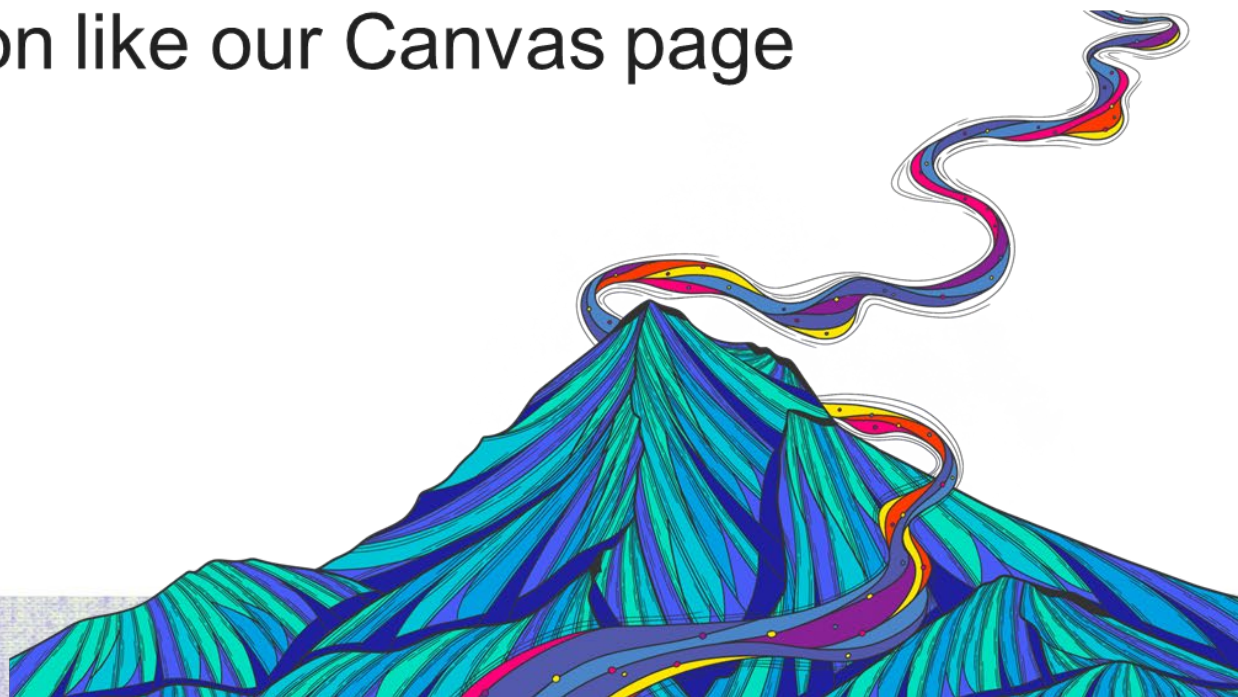


Sign up for the CYBER.ORG Range

- <https://apps.cyber.org/login>
- Human verification like our Canvas page



 Believes



Contact Me

- **Willie Henderson**
- Cyber Education Specialist
- LA CYBER.ORG Range Specialist
- willie.henderson@cyber.org





**Thank you for attending,
“Create a GREAT day!”**