



## Ohio Cyber Collaboration Committee (OC3)

Ohio's cyber community working together to help Ohio's citizens and organizations achieve world class cyber security

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



## Ohio Cyber Collaboration Committee (OC3)

Ohio must posture itself with an enterprise-wide approach that allows for a statewide cyber governance structure. More importantly, Ohio must develop and implement the appropriate authority to provide the capability to respond to and prevent cyber-attacks.

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



## Ohio Cyber Collaboration Committee (OC3)

### The Threat

- Cyber crime is projected to cost the global economy \$9.2 trillion by 2024, more than 10 times the cost since 2015. Average per attack is 9.48 million.
- There were over 4,100 recorded data breaches and those breaches exposed 22 billion records in 2023
- The cyber-insurance industry is already estimated to be worth well over \$10.33 billion growing to 27.8 billion by 2026.
- Multiple firms project that by 2023, 30 billion devices will be connected to the "Internet of things," a huge growth in the number of devices that connect ever more of daily life to the Web.
- Prevention is cheaper than remediation.

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

#### Threat Actors

- Nation State actors
- Criminal enterprises
- Intellectual property theft/industrial espionage
- “Hacktivists”/terrorists
- Personal/political attacks/insiders
- Malicious Acts/Vandalism
- Rogue Malware

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

#### Types of Attacks

- Phishing – emails over 90% of attacks, Vishing, Smishing, Spear Fishing, whaling  
<https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf>
- Block (SPF DKIM DMARC), Educate, Report, Protect (segment, least privilege, updates)
- Ransomware – Every 14 seconds – New threat - Blackmail
- DOS/DDOS Attacks - (distributed denial-of-service) attempts to disrupt normal web traffic and take a site offline by overwhelming a system, server or network with more access requests than it can handle.
- “Man in the middle” – Public wi-fi or weak link on your own network
- Social Engineering
- Insider attacks/physical security/vendor 3<sup>rd</sup> party corruption
- Password attacks/hacks/brute force
- “Typo squatting” fake login pages, clickjacking
- Viruses/other Malware

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

#### Common Vectors of Attack

- Emails and email attachments
- Unpatched vulnerabilities – OS, Apps
- Compromised/weak credentials (username/password)
- Infected downloads (Trojan horse)
- Compromised thumb drives/CDS/DVDs/SD cards
- Malicious links/advertising/QR codes, Domain Shadowing
- Drive by downloads (infected websites)
- Man in the middle, Open Wi-Fi or weak link on your own network
- Windows Macros
- Deception/social engineering
- Unsecured vendors/support programs

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---

### TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	200k years
14	3 mins	4 years	64k years	750k years	15m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

---

---

---

---

---


---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3) Password Strategies

- Never reuse or duplicate passwords
- use long complex passwords – 12 minimum with numbers, upper- and lower-case letters, and symbols - longer is better (74 characters per slot)
- Avoid words in the dictionary, part of your name, where you work, your school, the current year, DOB, anniversaries, pets' names, etc.
- Use embeds
- Use the first letters of phrases i.e. The Beatles The Long and Winding Road – \$TlAwRtLydWnDistRb76 21 characters, all 4 options, no dictionary words - (trillions of years to brute force attack!)
- Use a password manager (does have some risks)
- Add multi factor authentication (something you know with something you have) i.e. password plus cell phone and pin number
- Set maximum number of tries, then lock out or freeze account
- Change password any time something bad happens

<https://www.oc3.ohio.gov/>

---

---

---

---

---

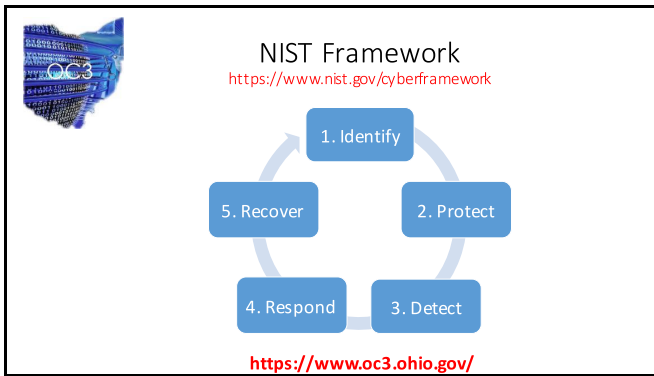
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---



**Ohio Cyber Collaboration Committee (OC3)**  
**Simple Solutions**

- Update OS and Programs, Delete old or unused programs (Windows 10, Big Sur)
- Change default usernames and passwords on hardware/systems (Mirai malware)
- Use strong passwords and Use Multi Factor Authentication (MFA)
- Use/turn on firewall and antivirus programs
- Inventory your network, block unknown devices
- Isolate internet of things/wireless devices from computers (segmentation)
- Have a separate guest network accounts for visitors/IOT/kid's accounts/old tech
- Don't click links in emails or on web pages – look it up, type it in
- Treat outside/unknown thumb drives/CDs/DVDs as highly risky
- Treat outside attachments as risky
- Don't go to sketchy web sites
- Beware of free stuff
- Don't trust something just because you think you know someone
- Backup your data everyday – Use encryption on sensitive data, airgap backup(3-2-1)
- Don't forget physical security, screen locks etc. – “windows L” - don't lend your phone
- Be careful on social media, don't give up your PII - GPS in pictures

---

---

---

---

---

---

---

---



**Ohio Cyber Collaboration Committee (OC3)**  
**Steps to get better**

- Train - users, managers, IT staffs, executives
- Complete Cyber inventory – hardware, software, data, policies
- Audit/implement best practices – NIST standards (OhCR)
- Develop Cyber Response/Recovery Plan
- Develop Continuity of Operations Plan
- Develop and Conduct Tabletop Exercise (CISA)
- Practice all in a red on blue Cyber Range Exercise
- AARs and improve, Audits/Pen tests - not a “one and done” project – “Persistent Cyber Improvement” (PCI) is the key



<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



**Ohio Cyber Collaboration Committee (OC3)**

**Our Mission:** To provide an environment for collaboration between key stakeholders, including education, business and local government to strengthen cyber security for all in the State of Ohio and to develop a stronger cyber security infrastructure.

**Our Goals/Committees:** OC3 has established four subcommittees to help it achieve its primary goals: Education/Workforce Development, Cyber Range, Cyber Protection and Preparedness, and Governance and Public Awareness. The committees are composed of Ohioans with a wide range of cyber and educational expertise dedicated to making Ohio a leader in how to integrate public-private partnerships into solving the cyber security problem.

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

#### Education/Workforce Development Subcommittee:

Grow the workforce and improve the training and education of users and students in cyber security by:

- a. Encouraging individuals of all ages to consider cyber security as a career, help individuals to further develop their cyber security skills at the K-12 and higher education level or as adult learning.
- b. Identifying critically needed skills and developing training and educational paths to meet the growing need for skilled workers in the cyber security field. Giving students the hands-on experience needed to be ready to work on day one.
- c. Training users/students at all levels in good, age appropriate, cyber hygiene and best cyber security practices.
- d. Provide educators the skills and tools needed to support this growing workforce.

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

#### Ohio Cyber Range/OCRI:

Provide a secure cyber security test and training environment, known as a cyber range, to:

- a. Support the education of students at the K-12 and University level.
- b. Conduct cyber security exercises and competitions to hone cross organizational incident response capabilities and develop future cyber security professionals.
- c. Research and test industry-standard best practices, evaluate and test innovative technologies and processes.
- d. Enable a training environment for the current and future cyber security workforce, including National Guard personnel, state and local government personnel, faculty and students in the education community, and private sector entities.
- e. Provide a Cyber Portfolio for learners, and support internships.
- f. Will be able to connect from any location with OARnet access.

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



## OCRI Impact | 2018 - 2024

#### 18 RPCs / 26 Institutions:

- Bowling Green State University
- Cedarville University
- Cinday Cyber at SOCH
- Cleveland State/Case Western IoT Collaborative
- Cuyahoga Community College
- Eastern Gateway Community College
- Lorain County Community College
- Ohio State University
- Ohio University
- Owens Community College
- PAST Foundation
- Rio Grande Community College
- Stowess State University
- Stark State College
- Tiffin University & Findlay Partners
- University of Akron
- University of Cincinnati
- University of Dayton



<https://www.ohiocyberrangeinstitute.org/>

---

---

---

---

---

---

---

---

## OCRI Education Module Library

- A collection of learning materials
  - Instructional materials
  - Assessment materials
  - Hands-on component
- Geared towards K-12, Higher Ed, and/or Workforce Development
- Developed to be shared
  - Choose parts to develop your own courses
  - Build upon what others have created
  - Contribute and collaborate



---

---

---

---

---

---

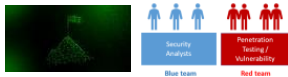
---

---

## OpFor v Blue Pilot Exercise:

Capture the Flag (CTF)

Red Team vs. Blue Team



<https://www.ohiocyberinstitute.org/>

---

---

---

---

---

---

---

---

## OC3 Cyber Protection Subcommittee

### Deliverables

- Ohio Cybersecurity Strategic Plan
- K-12 Cyber Challenge – IN PROGRESS
- OC3 Website Development
- Cyber TTX Exercises – IN PROGRESS
- Cyber Toolkit / User's Guidebook of Best Practices – IN PROGRESS
- Mock Cyber Incident
- Cyber Risk Assessment
- Cyber Symposium / Annual Conference
- Ransomware Awareness Campaign

<https://www.oc3.ohio.gov/>



---

---

---

---

---

---

---

---



## Ohio Cyber Collaboration Committee (OC3)

### Governance and Public Awareness Subcommittee:

Identify and share best practices, policies and technologies for all Ohioans by:

- a. Providing a collaborative research and development environment for the development and testing of innovative technologies and processes.
- b. Ensuring cyber threats are part of emergency planning at all levels both public and private.
- c. Using public awareness tools to educate and inform key decision makers of good cyber security practices and the latest information.
- d. Educating the general public on the importance of cyber security for the "Internet of Things."
- e. Sharing threat intelligence between both public and private sector entities, facilitated through the Ohio Homeland Security State Fusion Center.

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



## The Ohio Cyber Reserve

Bringing Cyber Talent to the Fight




---

---

---

---

---

---

---

---



## The Ohio Cyber Reserve

### The Need for a Cyber Reserve

1. Ohio's cyber experts are understaffed and over missioned
  - DAS
  - ONG
2. Small governmental entities do not have the resources or expertise to deal with cyber threats
  - Entities need help with assessments and best practices, as well as assistance when a cyber event occurs
    - Townships, villages, small cities, and smaller counties, eligible nonprofits
    - First responders, city services and utilities, Boards of Elections, public data
3. Critical infrastructure needs more protection, especially smaller utilities and emergency services
4. K-12 educators are typically not cyber security experts
  - They need help setting up cyber programs and cyber clubs within Ohio's high schools and junior high schools
  - Students need mentors who can inspire them and show them the pathways to a cyber career
5. Ohio needed a way to tap into the wealth of cyber talent that exists throughout the state and connect that talent to the needs of Ohio, but in a way that is sustainable from a budget perspective




---

---

---

---

---

---

---

---



## The Ohio Cyber Reserve



### The Ohio Plan

1. Created a volunteer firefighter style Cyber Reserve made up of trained civilians nested under the Adjutant General's Department
2. Legislatively modeled after the Ohio Military Reserve ORC Chapter 5920
3. The Adjutant General's Department has developed appropriate policies to support and regulate the teams
  - Members are volunteer civilians subject to state call up in a cyber emergency to support the Ohio National Guard's cyber response efforts
  - While in training status, volunteers are not paid, but when activated will be paid as state civilian employees
  - Volunteers are vetted with appropriate background checks, training requirements
  - Volunteers are organized into regionally based teams
  - The teams are provided training, equipment and IDs and work out of ONG armories
  - When fully trained and certified will be available for call up to assist in cyber response
  - Volunteers who are not fully trained, but who have been vetted can be used to support student mentoring efforts under the Ohio Cyber Collaboration Committee (OC3)

---

---

---

---

---

---

---

---



## The Ohio Cyber Reserve



### OhCR Mission Set

1. **Assist** - While in a volunteer status, the Cyber Response Teams will provide outreach, training, education, and security assessments to eligible governmental entities and critical infrastructure to reduce cyber vulnerability and increase resiliency.
2. **Educate** - While in a volunteer status, the Cyber Response Teams will assist K-12 educational efforts supporting cyber clubs and mentoring students in support of the Ohio Cyber Collaboration Committee's (OC3) Education and Workforce Development efforts.
3. **Respond** - When called to paid state active duty status, the Cyber Response Teams, under the direction of the Adjutant General's Department will be available to respond to cyber incidents at eligible governmental entities and critical infrastructure.

---

---

---

---

---

---

---

---



## The Ohio Cyber Reserve



### Want to be a member?

1. To join the OhCR or request assistance, email us at [OhioCyberReserve@ucmail.uc.edu](mailto:OhioCyberReserve@ucmail.uc.edu)
2. For more information contact:

Craig Baker  
 Program Administrator,  
 Ohio Cyber Reserve (OhCR)  
 2825 W Dublin Granville Road  
 Columbus Ohio 43232-2789  
 O: 614-336-7992  
[Craig.w.baker2.nfg@army.mil](mailto:Craig.w.baker2.nfg@army.mil)

---

---

---

---

---

---

---

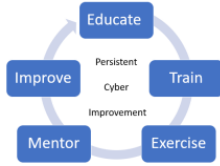
---





# Scalability of OC3 Efforts Ohio Persistent Cyber Improvement (O-PCI)

## Senior Leaders Brief



OHIO CYBER RANGE INSTITUTE  
UNLOCKING POTENTIAL. SECURING THE FUTURE.




---

---

---

---

---

---

---

---



## Gateways

	Gateway 1 (Core)			Gateway 2 (Proficiency)			Gateway 3 (Advanced)		
	Classes	Products/actions	End Point	Classes	Products/actions	End Point	Classes	Products/actions	End Point
All Users	Cyber Awareness		Annual Cert	Cyber Awareness		Annual Cert	Cyber Awareness		Annual Cert
IT Professionals	Cyber 101	Cyber Inventory Best practices/NIST Internal Auditor	OHCR visit and review AAR	Cyber 102	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Usable Plans TTX AAR	Cyber 103	Red on Blue X plan	Complete Red on Blue AAR
Managers	Cyber 101	Cyber Inventory Best practices/NIST Internal Auditor	OHCR visit and review AAR	Cyber 102	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Usable Plans TTX AAR	Cyber 103	Red on Blue X plan	Complete Red on Blue AAR
C-Suite	Cyber 101, Legal/Risk management	Internal Auditor Review Provide resources	Org. Badge	Cyber 102, Legal/Risk management	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Org. Badge	Cyber 103, Legal/Risk management	Red on Blue X plan	Org. Badge

---

---

---

---

---

---

---

---



## Ohio Cyber Collaboration Committee (OC3)

### Other Pending Programs:

- State aggregate purchasing program
- .GOV migration
- Cyber Fusion Center

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

#### Resources you can use

- OC3 – <https://www.oc3.ohio.gov>
- Ohio Cyber Range – <https://ohiocyberrangeinstitute.org>
- Ohio Cyber Reserve/ONG – Use email process (assist/educate - [OhioCyberReserve@ucmail.uc.edu](mailto:OhioCyberReserve@ucmail.uc.edu))
- Ohio Homeland Security/CISA – <https://www.cisa.gov>
- FBI/Department of Public Safety/Secret Service/NSA
- NIST – <https://www.nist.gov>
- NICE - <https://niccs.cisa.gov/workforce-development/nice-framework>
- Trusted vendors
- OARnet – Survey - <https://oar.net/securitysurvey>

---

---

---

---

---

---

---

---



### Ohio Cyber Collaboration Committee (OC3)

OC3 is supported by a “whole of government” approach to ensure its success. Primary sponsors are the Adjutant General's Department/Ohio National Guard, the Department of Higher Education, The Department of Education, The Department of Administrative Services, The Department of Public Safety, and The Department of Transportation.

OC3 has over 120 organizations who are active members who support the OC3 mission and objectives

<https://www.oc3.ohio.gov/>

---

---

---

---

---

---

---

---



### OHIO CYBER COLLABORATION COMMITTEE (OC3)

Ohio's cyber community working together to help Ohio's citizens and organizations achieve world class cyber security

#### Points of Contact

##### Primary

Mark Bell  
 Cyber Security Outreach Coordinator  
 2825 W Dublin Granville Road  
 Columbus Ohio 43232-2789  
 Phone 614-336-4903  
 Mobile 614-256-2391  
 Mark.a.bell16.nfg@army.mil



##### Alternate

Craig Baker  
 Program Administrator,  
 Ohio Cyber Reserve (OHCOR)  
 2825 W Dublin Granville Road  
 Columbus Ohio 43232-2789  
 O: 614-336-7992  
 Craig.w.baker2.nfg@army.mil




---

---

---

---

---

---

---

---