University of Dayton
Center for Cybersecurity and Data Intelligence

Cyber Flyers 2025-2026

Annual Report



CYBER FLYERS

University of Dayton

Cyber Flyers

Cyber Flyers is a joint effort between the Center for Cybersecurity and Data Intelligence and UDit as a high impact experiential learning opportunity for students. The Cyber Flyers are a student-led team, composed of a diverse set of majors, and are advised by the CCDI. The primary mission of the team is to provide cybersecurity education, training, and outreach to the student community on campus.

The team has a partnership with the TxCR (Texas Cyber Range at Texas A&M), another student-led cybersecurity focused group. The teams currently share the results of their initiatives, and TxCr hosts a blog for our team (cf.therangerpost.com).

We are organized around project teams, each with a director, and an executive director providing strategic direction:

- **Campus Marketing and Communication (CMAC):** Develop and execute social media content strategies targeting students. Plan and coordinate campus events such as speaker series, tabling, giveaways, and collaborative programming with student organizations (e.g., SGA, Greek councils, Flyer News, Flyer Enterprises) and university departments (e.g., Communication, Criminal Justice, Computer Science, MIS, Athletics, Dining Services). Track engagement KPIs including post frequency, follower count, event attendance, and post-event satisfaction surveys.
- **Phishing Simulation & Training (PSAT):** Assist in designing, building, and maintaining a library of phishing email templates and landing pages. Planning and running phishing simulation campaigns using open-source tools such as GoPhish. Support research into cybermindfulness principles, training effectiveness, and decay of training over time. Contribute to documentation of campaign processes and technical procedures for university IT partners.
- **Cyber Threats & Mitigation Research (CTMR):** Research current cybersecurity threats, vulnerabilities, and mitigation strategies. Produce written deliverables (articles, briefs, or whitepaper-style reports) that may inform campus outreach content and could be suitable for publication. Collaborate with institutional resources to ensure research is timely and relevant.

Technical Infrastructure, Consulting & Special Projects: Contribute to emerging initiatives such as cyber range architecture and operations (hypervisors, identity and access management, networking, remote access) or community-facing cybersecurity clinic services (security assessments, policy review, risk analysis for nonprofits and small businesses). Engage with industry frameworks (NIST, CIS) and standard security tools as applicable. Support project planning, documentation, and client communication. Our Team also created cybersecurity training for UDit for student training.

Letter from the Executive Director



Allison Shelly, MIS & BAN '26

When I first started with Cyber Flyers, we were a small group of students with majors in the MIS and IT fields. We communicated through a Discord server, had no sub-teams, and tackled every task collaboratively. We worked with a UD art student to design our logo, created vlogs interviewing students around campus, and piggybacked our posts off the CCDI's social media platforms. We worked hard, but our small team still struggled to gain the reach we wanted. Through it all, we stayed united by the same goal: to teach our peers about cybersecurity and keep our campus community safe.

Fast forward several semesters, and we now have a much bigger team. We've organized into three sub-teams, each targeting a different, equally important way to spread our message. We have successfully tabled at Up the Orgs and in KU, run phishing simulations to train students, and published blog articles about hot cyber topics. We've also hosted guest speakers, partnered with the Hanley Sustainability Institute for a podcast on the real implications of AI, and created cybersecurity training modules that show new students where to get help on campus.

I would like to thank all of our partners and mentors who have supported us over the years. A special thank you to John Wolfe and Grant Neeley from the CCDI who have been pivotal in bringing Cyber Flyers to life. Thank you to Carl Rodgers from UDit, the students from Texas A&M University Cyber Range (TxCR) for their collaboration, as well as our past guest speakers – Blaze Baker, Dean Halter, Brian Lakatos, and Joe Tinney – for taking the time to share their messages with us. We are proud of how far we have come, but this is just the beginning for Cyber Flyers!

Allison Shelly '26
Executive Director, Cyber Flyers

Letter from Staff Advisor

The Cyber Flyers were founded in Fall 2024 in the Center for Cybersecurity and Data Intelligence by Dr. Grant Neeley and myself. Our intention was to provide a place where students interested in cybersecurity could provide peer to peer education about cybersecurity to increase the overall security posture of the university while allowing our students to learn. We started with a small team of 6 students, that laid the groundwork in our first year for partnerships with university departments, UDit, City of Dayton leaders, and private sector technology professionals. Our initial student group really took the initiative to set a clear direction for the group for this year and turn the team into a meaningful experiential learning opportunity.

The team grew this academic year from 6 students to 14 students, with almost all the prior team continuing. This year our students were divided into teams, each led by a director, that specialized in an area that furthered the team's mission. The students that we have on the team come from a variety of majors (Criminal Justice, Computer Science, Management Information Systems, Communication, Marketing, Accounting) which allows our team to bring together differing approaches to cybersecurity for the benefit of campus. Cyber Flyers is a primarily student led and operated group. Grant and I provide ongoing guidance and project assistance. Our team wildly exceeded our expectations this academic year and produced some amazing work for their peers on campus, while also engaging with the greater Dayton community. Our Executive Director and the individual team directors did a great job steering the direction of the team and deserve recognition for their fantastic efforts and outcomes this academic year.

John Wolfe '18, MA, MBA
Cyber Flyers Advisor
Senior Academic Support Engineer
UDit | Center for Cybersecurity and Data Intelligence

Cyber Flyers Team

- **Allison Shelly, *MIS & BAN '26* – Executive Director, Cyber Flyers**
  - **Camryn McKenzie, *CMM '27* – Director, Campus Marketing and Communication**
    - Saija Cleveland, *CJS '26*
    - Lauren Turner, *MGT '26*
    - Elise Krier, *MIS '27*
    - Yoni Mendez-Antonio, *MKT '28*
  - **Tidiane Dia, *CIS '26* – Director, Cyber Threats and Mitigation Research**
    - Drew Hall, *CJS '26*
    - Alan Torres, *CPS '28*
  - **Charlie Tucker *MIS* '26 – Director, Phishing Simulation and Training**
    - Austin Bohlman, *MIS '26*
    - Jameir Jackson, *GEN '27*
    - Alex Haag, *CPS '28*
    - Ethan Lally, *CPS '29*

Campus Marketing and Communication (CMAC)

Director: Camryn McKenzie, *CMM '27*



Mission: Sharing our message by hosting events and posting to social media to keep students and the community informed on cybersecurity.

University *of* Dayton
Center for Cybersecurity and Data Intelligence

University *of* Dayton

CYBER FLYERS

Campus Marketing and Communication (CMAC)

Key Responsibilities

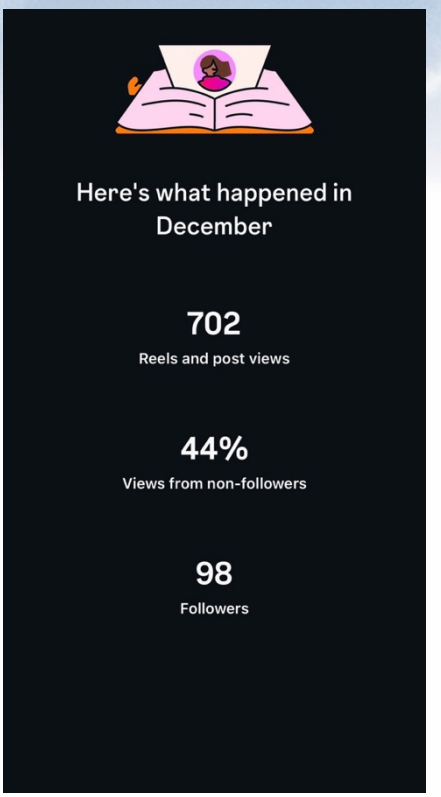
- Weekly Instagram posts that summarize blog posts (by research team) that are intriguing for our target audience.
- TikTok videos that showcase tabling events to promote campus engagement with Cyber Flyers.
- LinkedIn posts highlighting Cyber Flyers accomplishments or important topics.
- Hosted tabling events and guest lectures open to the public to spread awareness on cyber security.

Major Initiatives & Accomplishments

Initiative Name: Interactive Tabling Events

- **Objective**: Increase student engagement with Cyber Flyers.
- **Description**: Set up in student union with donuts and signs to educate students on cyber security, promote blog subscription and social media channels. We typically set up interactive games so students can get a better understanding of our mission at Cyber Flyers.
- **Outcome/Impact**: Students leave feeling more knowledgeable about cyber safety, and we always ensure that they follow our social media accounts.

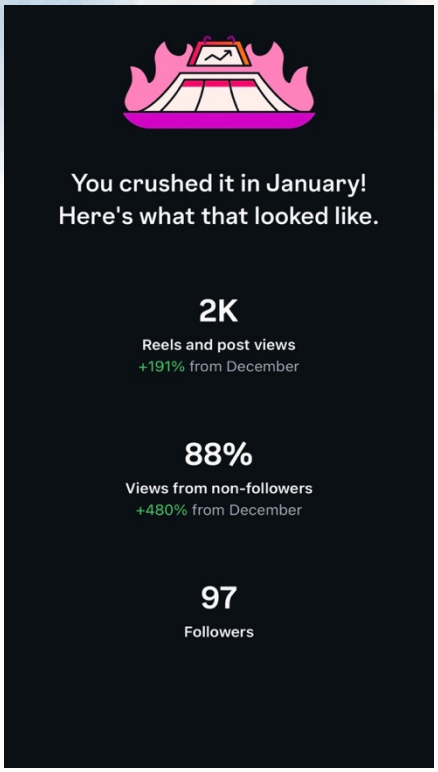
Metrics, Impact, Visuals & Links:



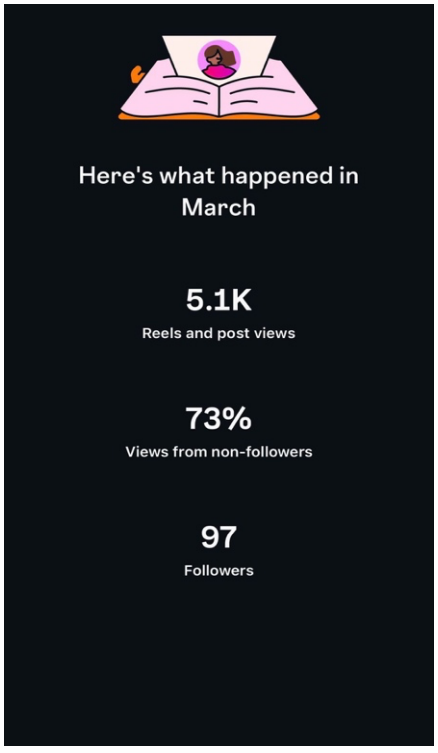
[LinkedIn]

[Instagram]

[TikTok]







University of Dayton
Center for Cybersecurity and Data Intelligence

University of Dayton

CYBER FLYERS

Looking Ahead...

Challenges & Lessons Learned

- **Key challenges faced**: Growing our followers count on Instagram. We have lots of views, but not enough people are following us.
- **How they were addressed**: Using tabling events to promote our blog and socials in person so we get followers in real time.
- **Lessons learned for the future**: Incorporate a giveaway to promote sharing posts, increase followers, and overall, more clicks on our pages.
- Full cooperation from all team members was low at times.

Goals for Next Year

- More guest lecture events, more tabling events, introduce giveaways.
- Look to collaborate with other groups on campus.
- See more growth on social media pages.

Closing Summary

Our Campus Marketing and Communications team plays a critical role in bringing Cyber Flyers' mission to life by making cyber safety accessible, engaging, and visible across campus. Through consistent social media content, interactive tabling events, and public guest lectures, we act as the bridge between research and real student awareness. Our efforts not only increase knowledge around cyber security but also build a recognizable presence that encourages ongoing engagement with Cyber Flyers. With additional funding, we can expand our outreach through larger events, creative campaigns like giveaways, and more strategic collaborations, ultimately reaching a wider audience and making an even greater impact on student safety and digital awareness.

Cyber Threats and Mitigation Research (CTMR)

Director:
Tidiane Dia,
CIS '26



Mission: Educate and empower students by breaking down real-world cyber threats; while providing clear, actionable mitigation strategies.

University *of* Dayton
Center for Cybersecurity and Data Intelligence

University *of* Dayton

CYBER FLYERS

Cyber Threats and Mitigation Research (CTMR)

Key Responsibilities

- Research emerging cybersecurity threats and attack techniques
- Publish educational articles for student awareness
- Develop themed campaigns to improve engagement and understanding
- Translate technical cybersecurity concepts into student-friendly content
- Support Cyber Flyers' mission through awareness and education initiatives

Major Initiatives & Accomplishments

Initiative Name: *AI Campaign*

- *Objective: Educate students on the risks and impact of AI in cybersecurity*
- *Description: Created a multi-article campaign exploring AI threats, security concerns, and real-world implications*
- *Outcome/Impact: Increased engagement and contributed to a ~70% open rate in recent articles*

Initiative Name: *How Attacks Happen Campaign*

- *Objective: Help students understand real-world attack methods*
- *Description: Published a series of articles breaking down how common cyber attacks occur*
- *Outcome/Impact: Improved content cohesion and significantly increased student engagement*

Initiative Name: *Podcast Initiative*

- *Objective: Expand content delivery beyond written articles*
- *Description: Filmed a podcast focused on sustainability in AI and data centers*
- *Outcome/Impact: Introduced a new engagement format and expanded audience reach*
- *Link:https://mediaspace.udayton.edu/media/HSI%20ON%20AIR%3A%20Impact%20of%20AI/1_106qtrh0/392333883*

Initiative Name: *Activism Security*

- *Objective: Educate students on the risks and long-term consequences of online activity, especially related to social media and activism*
- *Description: Developed a campaign consisting of multiple articles and potential video content, covering digital footprints, consequences of political activity online, guidance for students involved in activism, and safety considerations during protests*

- *Outcome/Impact: Expanded the scope of cybersecurity awareness beyond technical threats, helping students understand real-world personal and professional risks associated with online behavior*

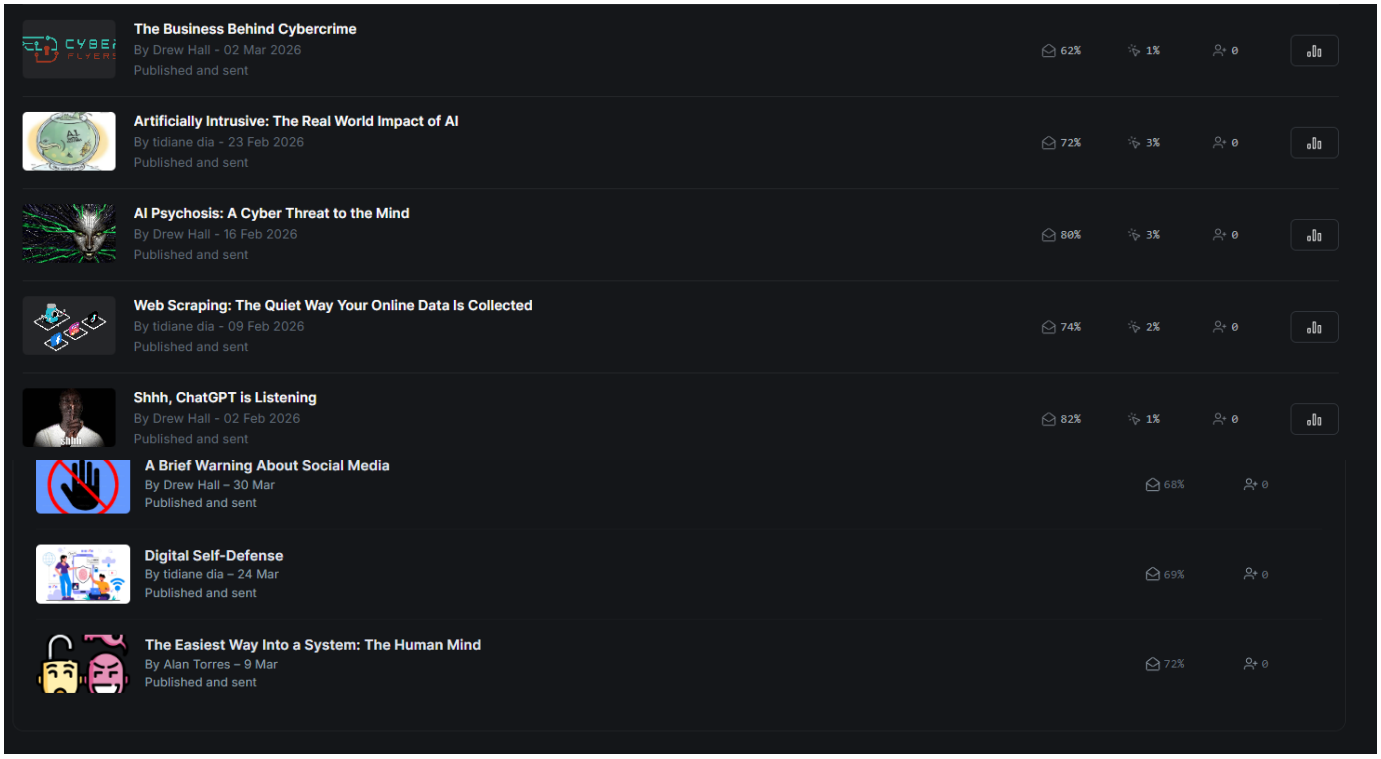
Initiative Name: *Backdoors & Breaches Event*



- *Objective: Provide hands-on cybersecurity learning experience*
- *Description: Hosted an interactive cybersecurity game event with Joe Tinney from Secure Cyber*
- *Outcome/Impact: Increased student engagement through experiential learning*

Metrics & Impact

- Newsletter growth: 4 → 159 members
- 16 articles published across multiple campaigns
- Email engagement increased from ~40–45% to consistently 60–80% open rates
- Top-performing content reached up to 80%+ engagement
- 1 podcast produced expanding beyond written content
- 1 interactive cybersecurity event hosted



University *of* Dayton
Center for Cybersecurity and Data Intelligence

University *of* Dayton

CYBER FLYERS

Looking Ahead...

Challenges & Lessons Learned

- **Key challenges faced:** Early low engagement and lack of content cohesion
- **How they were addressed:** Shifted to campaign-based content strategy
- **Lessons learned:** Structured, themed content significantly improves engagement and retention

Goals for Next Year

- Expand campaigns into more cybersecurity topics
- Increase multimedia content (podcasts, videos, interactive content)
- Continue improving engagement and reach across the student body

Closing Summary

The Cyber Threats & Mitigation Research Team plays a critical role in advancing Cyber Flyers' mission by translating complex cybersecurity concepts into accessible, engaging content for students. Through measurable growth in membership and engagement, the team has demonstrated its ability to educate and impact the university community, making it a valuable initiative worthy of continued investment and support.

Blog Hosted in partnership with TxCr at Texas A&M:
https://cf.therangerpost.com

Phishing Simulation and Training (PSAT)

Director: Charlie Tucker, *MIS '26*



Mission: Educating the University of Dayton on cybersecurity, particularly the student population, by creating targeted training, and designing & running phishing simulations.

University *of* Dayton
Center for Cybersecurity and Data Intelligence

University *of* Dayton

CYBER FLYERS

Phishing Simulation and Training (PSAT)

Key Responsibilities

- Phishing email campaigns created with scaling difficulty based on the NIST Phish Scale.
- Creation of training pages customized to each phishing campaign to inform those who clicked on best practices and what to look out for next time.
- Compilation of phishing campaign results, including the number of opens and clicks.

Major Initiatives & Accomplishments

Initiative Name: Getting Started

- **Objective:** Develop research questions and create an environment to train students.
- **Description:** In the Fall semester, under the leadership of former Team Director Alex Haag, the PSAT worked hard to ask real research questions. The goal was to create a study that accomplished two things. One, to train students on phishing awareness and protect them from future scams. Two, to gather compelling data, in order to make a case to the University of Dayton to expand our efforts to the whole student body.
- **Outcome/Impact:** We were greatly successful in getting started with this project. We developed a plan over the course of the first few weeks, we got our environment set up, and began the initial research on what makes an effective phish. We took some sample phishes as well as our research questions to the University of Dayton Center for Cybersecurity and Data Intelligence where we presented our plan and gathered support. The project was approved to move forward in the Spring semester.

Initiative Name: The Test Group

- **Objective:** The goal with our test group was to gather initial data on clickrates of certain phishes to see the effectiveness of our training over time.
- **Description:** We hit the ground running at the start of the Spring semester. Immediately we developed four phishes of varying difficulties and complexities, and we also created landing pages where one would be redirected to should they fall for the phish. These landing pages were insightful, pointing out the red flags in the emails and providing general information about phishing and cyber-hygeine. Once we produced the phishes and landing pages, we got the final approval and promptly began sending them out.

Outcome/Impact:

- 4 total email phishes sent out to 156 people each (Not including a phish sent to a Cyber Essentials for Criminal Justice class).
- An average of 123 emails opened per phish, out of the 156 sent to.
- 33 total links clicked on within all four phishes.
    - 4 Phish examples sent below for quantitative metric outcome

Visuals & Highlights: **Phishing Results 2026**



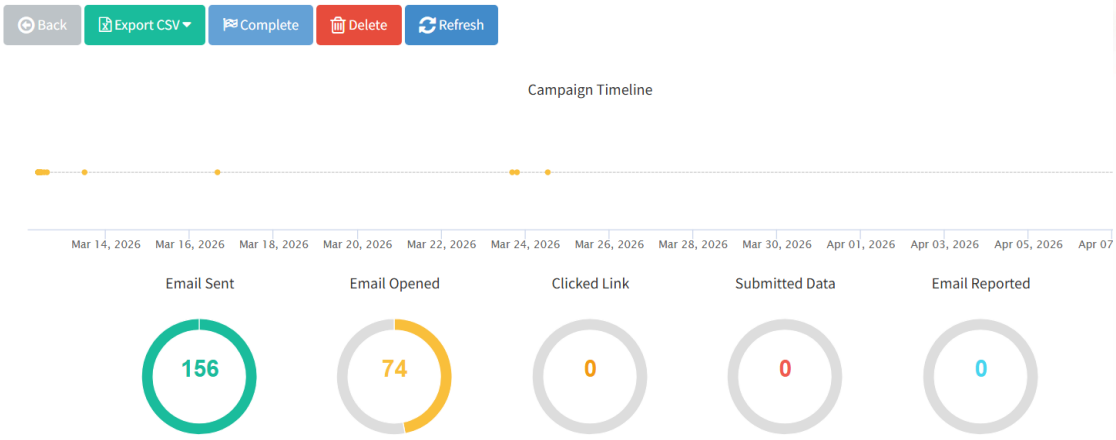


University of Dayton
Center for Cybersecurity and Data Intelligence

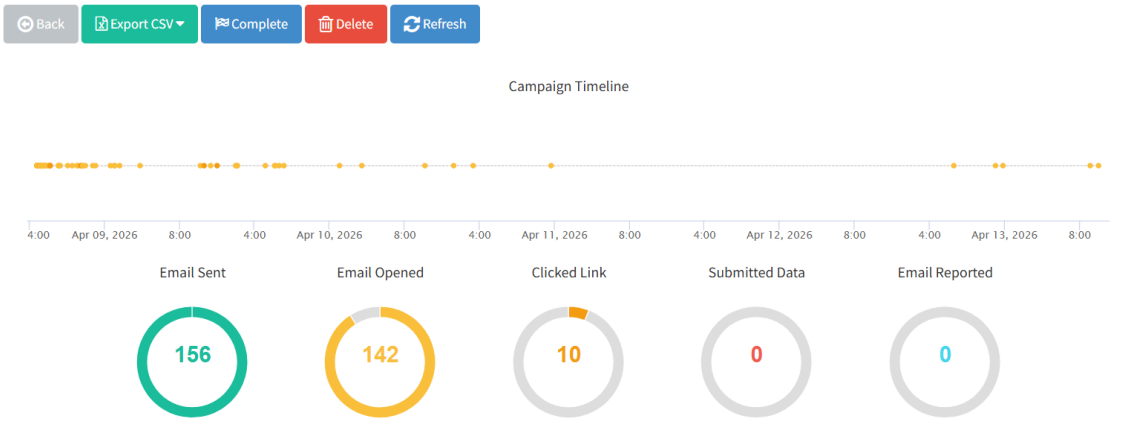
University of Dayton

CYBER FLYERS

Results for FAKE UDIT PHISHING EMAIL



Results for Fake Job Phish



University of Dayton
Center for Cybersecurity and Data Intelligence

University of Dayton

CYBER FLYERS

Looking Ahead...

Challenges & Lessons Learned

Key Challenges Faced:

- **Administrative Authorization Protocols:** Navigating the approval process with university administration required extensive negotiation to ensure simulation parameters aligned with compliance and standards.
- **Scripting and HTML Execution Errors:** Technical anomalies within the HTML source code resulted in non-functional hyperlinks for specific deployments. This technical failure led to a **0%** click-through rate for one campaign, as the intended link explaining the phish was inaccessible to recipients.
- **Automated Defensive Filters:** Phish's being sent out got flagged as spam, preventing the delivery of emails to the student body.
- **Participant Acquisition & Scalability:** Securing a significant sample size of students who would voluntarily opt-in to a long-term cybersecurity phish study.

How They Were Addressed:

- **Strategic Advocacy:** The team presented and held meetings for research-backed justifications to the necessary stakeholders
- **Integrated Recruitment Events:** To overcome low engagement, the team transitioned to an **active recruitment model**, hosting in-person events to explain the mission. This resulted in a database of participants who explicitly agreed to receive future simulations.
- **Quality Assurance (QA) Iterations:** Following the HTML link failure, the team implemented a mandatory phish test to a small group within the cyber flyers organization to see if the phish ended up in all or some spam boxes.

Lessons Learned for the Future:

- **Direct Outreach Efficacy:** Physical presence and campus partnerships are more effective for building a participant database than passive digital requests.
- **Technical Redundancy:** A testing of all HTML scripts within GoPhish must be reviewed and tests must be sent out to the cyber flyers organization first to prevent a phish failure.
- **Collaboration:** Building strong partnerships across the university was key. By collaborating with established departments, we gained the administrative support and credibility needed to scale our efforts, moving from small test groups toward our goal of educating the entire student population.

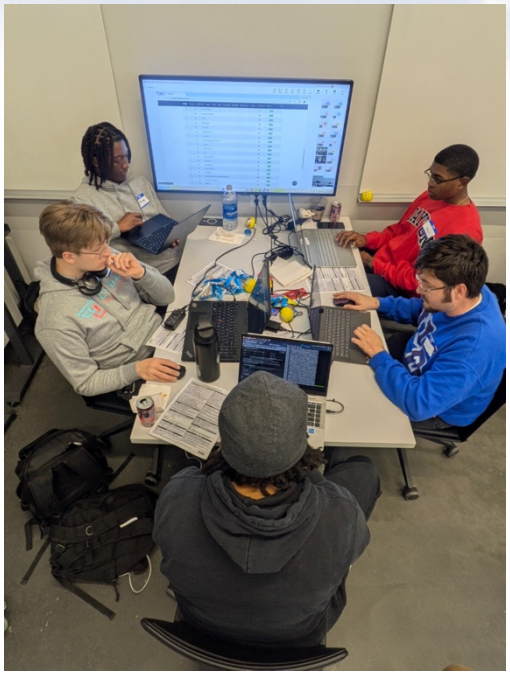
Goals for Next Year

- **Expand Test Groups:** Secure permission from university leadership to increase/ gain access to student emails for more accurate data.
- **New Student Training:** Roll out our completed phishing modules to all incoming first-year students to build a foundation of security awareness from day 1.
- **Update Simulation Tactics:** Create more realistic phishing examples that mimic the latest scams currently targeting the campus community consistently
- **Measure Progress:** Use the results from our larger testing groups to show university administration the clear impact and necessity of our training program for students

Closing Summary

Information alone is rarely enough to change behavior; true learning happens when students can make mistakes in a risk-free environment. This year, our simulations reached 156 students per campaign, revealing an average open rate of 79% and identifying 33 critical vulnerabilities where students would have compromised their data in a real-world attack. By providing these "safe failures," we turn potential security breaches into hands-on educational moments. Your support allows us to scale these simulations university-wide, moving beyond small test groups to ensure every Flyer has the practical experience needed to defend themselves and the University against evolving cyber threats.

We want to give a final honorable mention to a few of the events our team attended over the past year.



Several of our members traveled to the University of Cincinnati for a Capture the Flag (CTF) event hosted by the Ohio Cyber Range Institute (OCRI). In the cyber world, a CTF is a computer-based competition where teams race to solve technical puzzles and find hidden vulnerabilities. We spent a Saturday competing against other teams, meeting objectives, and flexing our Linux skills! The Cyber Flyers would love to host a similar event one day.

We also attended the Ohio Information Security Conference (OISC) hosted by Technology First at Sinclair Community College. We made connections with cyber professionals from across the state, learning about hacking, penetration testing, AI, and more as we explored their booths. As an added bonus, our members got to watch individuals from UD, including John Wolfe, present their research on leveraging AI in phishing scams!



Finally, Cyber Flyers were asked to create cybersecurity awareness training for all students by UDit's IT Security team. We are planning to deliver that to UDit by the end of the academic year, for release in Fall 2026.