CECIL COLLEGE · COMPUTER SCIENCE - CYBERSECURITY CLUB
NORTH EAST, MARYLAND

VOL. 2 — ISSUE 3
SEPTEMBER 2026
BACK-TO-CAMPUS EDITION

// MONTHLY CYBERSECURITY AWARENESS

CyberShield BULLETIN

⚡ SECURE YOUR WORLD — ONE CLICK AT A TIME

WELCOME BACK, SEAHAWKS!

// CECIL COLLEGE · FALL SEMESTER 2026 · BACK-TO-CAMPUS SECURITY EDITION

The Fall Semester Is Here — Let's Hit the Ground Running

September at Cecil College means new classes, new faces, new opportunities — and, as your cybersecurity club is here to remind you, a whole new set of digital risks that come with being back on a shared academic network. Whether you are a returning student settling into a familiar routine or a first-semester Seahawk stepping onto campus for the very first time, this issue is your complete security orientation for the semester ahead.

This month we also officially launch the **2026–2027 CS-Cybersecurity Club year** — complete with new leadership, exciting programming, and some ambitious goals we are committed to achieving together as a community.

Fall 2026 Kickoff | Club Year Launch | Cloud Security Alert | New Leadership

EDITOR'S WELCOME

FROM THE FACULTY ADVISORS — PROFESSOR JACQUELINE WILSON & DR. JAMES MORGAN

Welcome to the **September 2026 Back-to-Campus Edition** — Volume 2, Issue 3 of the CyberShield Bulletin. Over the summer, this newsletter covered ransomware (July) and IoT device security (August). Now, as the semester begins and students flood back onto campus networks with laptops, phones, and a semester's worth of ambitions, we turn to a threat that

touches every one of you multiple times per day: **cloud account security**.

Google Drive, OneDrive, iCloud, Canvas, Dropbox — your academic life runs in the cloud. That is both a convenience and a vulnerability. This month we explain exactly what can go wrong with cloud accounts and how to make sure yours are locked down before the semester gets into full swing.

We are also thrilled to formally open the **2026–2027 club year**. New leadership will be elected at our kickoff meeting, and we have a full year of competitions, workshops, guest speakers, and community events planned. To every new student: you belong here. Come find us.

Professor Jacqueline Wilson & Dr. James Morgan, Faculty Advisors
Cecil College Computer Science – Cybersecurity Club

⚠ THREAT SPOTLIGHT

// SEPTEMBER 2026 FEATURED THREAT

Cloud Account Takeover: When Your Drive, Email & Canvas Aren't Yours Anymore

🚨 **Risk Level: HIGH** — Cloud account takeovers spiked 61% on college campuses in the 2025–2026 academic year. The beginning of each semester is peak season — attackers know that new students are setting up accounts, clicking orientation emails, and connecting to unfamiliar networks all at once.

What Is Cloud Account Takeover?

A cloud account takeover happens when an unauthorized person gains access to one of your online accounts — your college email, Google Drive, OneDrive, Dropbox, Canvas (your learning management system), or any cloud-based service. Once inside, they can read your files, steal your personal information, impersonate you in emails to professors or financial aid, lock you out of your own account, or silently monitor your activity for weeks.

What makes cloud accounts such high-value targets is **how much lives inside them**. Your academic records, course submissions, financial aid correspondence, personal documents, and communications with professors and advisors — all of it is potentially exposed when a single cloud account is compromised.

The Most Common Attack Vectors

🎣 Phishing & Credential Harvesting

The overwhelmingly most common method — a convincing fake login page for Canvas, Google, or your college portal captures your username and password when you click a link from a phishing email. Attackers send these out in bulk at the start of every semester, disguised as IT announcements, financial aid alerts, and registration reminders. Reviewed in depth in our March 2026 issue.

🔑 Password Reuse Attacks

If you used the same password for a service that was breached — and as we covered in April's

issue, 65% of people do — attackers test those stolen credentials against your college account, Google account, and any other platform automatically. This is called credential stuffing and it is fully automated. A breach at a gaming site becomes a compromise of your academic account in minutes.

📱 MFA Fatigue ("MFA Bombing")

Even accounts protected with Multi-Factor Authentication are not immune. In an MFA fatigue attack, the attacker — who already has your password — repeatedly sends you MFA push notifications hoping you will eventually approve one out of confusion or frustration. This technique successfully bypassed MFA at several major organizations in 2025. The defense: never approve an MFA request you did not initiate, and switch from push notifications to an authenticator app code where possible.

☁ Insecure Sharing Settings

Not all cloud threats come from outside attackers. Misconfigured sharing settings — documents set to "anyone with the link" when they should be private — expose sensitive information to anyone who finds or guesses the URL. This is especially common with course projects, internship applications, and personal resumes stored in Google Drive or OneDrive.

What Attackers Do Once Inside

Access to a college cloud account is a treasure trove. Attackers commonly: read financial aid and scholarship communications to craft follow-up scams; use your student email to send phishing messages to professors and other students (your name adds credibility); access stored personal documents like tax forms and ID scans; and pivot to other accounts by using "Forgot Password" links sent to your now-compromised email. A single cloud account breach has a cascading effect across your entire digital life.

> *"The start of fall semester is the single highest-risk period for student account compromises. Attackers exploit the chaos of orientation week — unfamiliar systems, hurried setups, and students clicking links they might otherwise scrutinize more carefully."*
>
> — EDUCAUSE Cybersecurity Report, Higher Education, 2025

How to Protect Your Cloud Accounts

Enable MFA on every cloud account — especially your Cecil College email and Canvas. We covered this in March's issue. If you have not done it yet, do it today. It is the single highest-impact action you can take.

Audit your sharing settings. Open Google Drive or OneDrive right now and search for files shared with "Anyone with the link." Change these to specific individuals or "Restricted" unless there is a specific reason for open sharing.

Check for suspicious account activity. Gmail, Outlook, and Google Drive all show recent sign-in activity and connected apps. Review these at the start of the semester and revoke access from any app you do not recognize.

Do not approve unexpected MFA prompts. If your phone buzzes with an MFA approval request you did not initiate, deny it immediately and change your password — someone has your credentials and is attempting to log in right now.

💡 TIP OF THE MONTH

Conduct Your Semester-Start Security Audit — In 20 Minutes

> *Think of this as your digital back-to-school checklist. Run through it once at the start of each semester and you will close the most common vulnerabilities before attackers have a chance to exploit them.*

⏱ 20 minutes now = a full semester of protection

Each step below directly addresses a threat we have covered this year. Your summer reading is paying off.

Your 20-Minute Semester Security Audit

1. **Update all devices (5 min).** Check for OS, browser, and app updates on your laptop, phone, and tablet. Run them now. August's issue covered why this matters for IoT devices; it applies equally to your main devices. Unpatched software is the most common entry point for malware.
2. **Audit your passwords (5 min).** Open your password manager (April's tip) and use its built-in health report to identify weak, reused, or breached passwords. Update any flagged accounts — starting with your Cecil College email, Canvas, and financial aid portal.
3. **Verify MFA is active (3 min).** Check that Multi-Factor Authentication is enabled on your Cecil College account, personal email, Google Drive or OneDrive, and financial accounts. Reference March's issue for setup steps if needed.
4. **Review cloud sharing settings (3 min).** Open Google Drive / OneDrive → click the search bar → filter by "Shared externally." Change any documents set to open sharing that should be private. This step alone prevents a significant category of data exposure.
5. **Check "Have I Been Pwned" (2 min).** Visit haveibeenpwned.com and enter your email address. If any new breaches appear since last semester, change those passwords immediately using your password manager.
6. **Verify your backup is running (2 min).** Open your cloud backup app (Backblaze, OneDrive, or iCloud) and confirm the last successful backup ran recently. July's issue covered the 3-2-1 backup rule — a semester of coursework is too valuable to leave unprotected.

Set a calendar reminder to repeat this audit at the start of every semester — January, May, and September. It takes 20 minutes and provides a semester's worth of protection. Share this checklist with a classmate who might need it.

🎓 CAREER CORNER

Cloud Security Engineer: The Career the Industry Can't Fill Fast Enough

Following this month's cloud security theme, we spotlight one of the hottest and fastest-growing specializations in all of technology — a field where qualified candidates are so scarce that entry-level roles regularly command six-figure salaries in the Mid-Atlantic market.

What They Do

Cloud Security Engineers design, implement, and maintain secure cloud environments on platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. They configure access controls, monitor for misconfigurations, automate security responses, ensure compliance with regulatory frameworks, and respond to cloud-native threats. As organizations migrate more of their infrastructure to the cloud every year, the demand for professionals who can secure it scales in lockstep.

It is a role that rewards people who are both technically deep and systematically minded — someone who can think like an attacker, configure like an engineer, and communicate risk like a business analyst.

Relevant Certifications

AWS Security Specialty | **AZ-500 (Azure Security)** | **CCSP (ISC²)** | **CompTIA Security+**

Starting salaries in Maryland and the DC metro region: **$80,000–$105,000** for entry-level cloud security roles, rising sharply with AWS or Azure certifications. The federal government, defense contractors, and financial services firms in our region are all actively recruiting.

Fall club workshop: We are planning a hands-on AWS Free Tier security lab this semester — learning to configure secure cloud environments using the same tools used in industry. No prior cloud experience needed. Watch for the announcement. `[CLUB TO CONFIRM: Workshop date]`

DID YOU KNOW?

61%

Spike in cloud account takeovers on college campuses in the 2025–2026 academic year

SOURCE: EDUCAUSE Security Report, 2025

#1

Cloud misconfiguration remains the leading cause of cloud data breaches for the fourth consecutive year

SOURCE: IBM X-Force Threat Intelligence Index, 2026

77%

Of cloud breaches involve compromised credentials — not sophisticated hacking techniques

SOURCE: CrowdStrike Global Threat Report, 2026

3.5M

Unfilled cybersecurity jobs globally in 2026 — cloud security is the fastest-growing specialty

SOURCE: Cybersecurity Ventures, 2026

RESOURCES

Cloud Security Tools

Google Account Security Checkup

`myaccount.google.com/security-checkup`

Review recent sign-in activity, connected apps, and security settings for your Google account. Takes two minutes — run it today.

Microsoft Account Security

`account.microsoft.com/security`

Audit sign-in activity, manage MFA, and review connected devices for your Microsoft / OneDrive account.

Have I Been Pwned

`haveibeenpwned.com`

Check whether your email has appeared in known data breaches. A semester-start essential — run it now.

Google Drive Audit Log

`drive.google.com → Settings → Activity`

View who has accessed, shared, or edited your Drive files. Spot unauthorized access immediately.

CISA — Secure Cloud Business Applications

`cisa.gov/scuba`

Federal guidance on securing cloud applications — especially relevant for M365 and Google Workspace users at academic institutions.

KEY DATES

Fall 2026 Calendar

SEP TBD — **Club Fall Kickoff Meeting**
First meeting of the 2026–2027 year. All welcome — new members especially!
`[CONFIRM: Date/Time/Room]`

SEP TBD — **Officer Elections**
President, VP, Newsletter Editor, Outreach Coordinator
`[CONFIRM: Date]`

SEP TBD — **Cloud Security Hands-On Lab**
AWS Free Tier security workshop — all levels welcome
`[CONFIRM: Date/Time]`

OCT 2026 — **Cybersecurity Awareness Month**
Special edition + campus-wide events — our biggest issue yet!

OCT TBD — **Maryland Cyber Cup Registration**
CTF competition team tryouts begin
`[CONFIRM: Registration deadline]`

NOV 2026 — **Guest Speaker Series**
Industry professional — topic TBD
`[CONFIRM: Details]`

NEW TO CECIL?

Join the Club This Semester

The CS-Cybersecurity Club is open to every student at Cecil College — any major, any experience level. Here is what membership looks like:

- ✓ Hands-on labs and real-world skill building
- ✓ CTF competition team — beginner to advanced
- ✓ Certification study groups (Security+, and more)
- ✓ Internship and scholarship guidance
- ✓ Faculty mentorship from Prof. Wilson & Dr. Morgan
- ✓ A community that grows careers

No experience needed. Show up to the kickoff meeting — that is all it takes to get started.

`[CONFIRM: Club email / social media]`

CS-CYBERSECURITY CLUB — 2026-2027 KICKOFF

// ACADEMIC YEAR 2026-2027 · CS-CYBERSECURITY CLUB OFFICIAL LAUNCH · CECIL COLLEGE

The 2026–2027 Club Year Is Officially Open

This is it. The new club year is live. With the summer behind us and the semester in full swing, the Cecil College CS-Cybersecurity Club enters 2026–2027 with a clear vision, measurable goals, and the drive to make this the most impactful year in our club's history. Here is exactly what we are building — and what we expect from every member who joins us.

What We Expect — From Leadership and From Every Member

Great clubs do not happen by accident. They are built by people who show up consistently, push each other to grow, and stay true to a shared mission. Here is what the 2026–2027 CS-Cybersecurity Club is committed to — and what we ask of every member who wears the Seahawk name.

Show Up

Attend meetings consistently. Every session builds on the last. Presence is the baseline of membership.

Keep Learning

Dedicate time each week to skill-building — TryHackMe, study groups, or personal projects. Growth is not passive.

Support Each Other

More experienced members mentor newer ones. We rise together. Cybersecurity is a team discipline, not a solo act.

Compete Hard

Represent Cecil with skill and integrity at every CTF and competition. We play to win — and we play fair.

Give Back

Participate in at least one community outreach or awareness event. What we know is only valuable if we share it.

Set Goals

Every member is encouraged to set a personal milestone — a certification, a CTF rank, an internship. Name it. Chase it.

Club Year 2026–2027 Measurable Goals

1 Top-3 Finish at Maryland Cyber Cup

We finished 2nd last year. We are hungry for more. Competition team formation begins at the kickoff meeting.

2 Publish 9 Issues of CyberShield Bulletin

September through May, with at least one student-authored article every issue. Our newsletter is now a community institution.

3 Support 5 Members in Earning Certifications

Structured study groups for Security+, CySA+, and others — free, peer-led, and faculty-supported.

4 Place 3 Members in Internships or Co-ops

Connecting members with federal programs (NSA Pathways, DHS, CISA) and regional private-sector employers.

5 Deliver 2 Community Outreach Events

Taking our cybersecurity awareness mission beyond campus — to local schools, libraries, and community organizations.

6 Grow to 15+ Active Members by October

Recruiting across all programs and class years. If you know someone who would thrive here, bring them to the next meeting.

2026–2027 Club Leadership

Officer elections are held at the fall kickoff meeting. All enrolled Cecil College students in good standing are eligible to run. Positions are open — step up and lead.

Club President	Lead meetings, set the strategic direction, represent the club externally.	ELECTIONS
Vice President	Lead technical workshops, coordinate CTF teams, support the president.	ELECTIONS
Newsletter Editor	Own the CyberShield Bulletin — editorial calendar, contributors, production.	ELECTIONS
Outreach Coordinator	Social media, community events, new member recruitment, campus partnerships.	ELECTIONS
Faculty Advisor	Professor Jacqueline Wilson — mentorship, institutional support, and program continuity.	CONFIRMED
Faculty Advisor	Dr. James Morgan — academic advising, competition coaching, and CAE-CD liaison.	CONFIRMED

Interested in running for office? Reach out before the kickoff meeting. Officer experience is a genuine career differentiator — especially for students targeting federal and defense sector cybersecurity roles. `[CONFIRM: Contact email for officer interest]`

Club Snapshot — Fall 2026

Founded	**2017**
Faculty Advisors	**Prof. Wilson & Dr. Morgan**
Meeting Frequency	**Bi-Weekly**
Focus Areas	**Scholarships, Internships, Ethical Hacking, Defense & Awareness**
Institution	**NSA/DHS CAE-CD ✓**
Open to	**All Majors · All Levels**

// CYBERSHIELD BULLETIN — VOLUME 2 PUBLICATION SCHEDULE

Vol.2 · Iss.1	July 2026 — Ransomware & 3-2-1 Backups	PUBLISHED
Vol.2 · Iss.2	August 2026 — IoT Security & Fall Preview	PUBLISHED
Vol.2 · Iss.3	September 2026 — Cloud Security & Club Kickoff	YOU ARE HERE
Vol.2 · Iss.4	October 2026 — Cybersecurity Awareness Month ⭐	SPECIAL EDITION
Vol.2 · Iss.5	November 2026 — Holiday Scam Season	UPCOMING
Vol.2 · Iss.6	December 2026 — Year in Review & 2027 Forecast	UPCOMING
Vol.2 · Iss.7	January 2027 — New Year, New Threats	UPCOMING
Vol.2 · Iss.8+	February–May 2027 — Semester Series	UPCOMING

October is our biggest issue of the year. National Cybersecurity Awareness Month content, campus events, and guest contributors — submissions due September 20.

`[CONFIRM: October submission deadline & email]`

CONTACT THE CLUB

📧 [CONFIRM: Club Email]

📍 Cecil College, North East, MD 21901

🌐 [CONFIRM: Club website or portal]

📱 [CONFIRM: Social media handles]

SUBMISSIONS & CONTRIBUTIONS

October (Cybersecurity Awareness Month) submissions due **September 20**. We welcome articles, tips, event announcements, and spotlights from all community members.

Send to: [CONFIRM: Submission email]

ABOUT THIS NEWSLETTER

The CyberShield Bulletin is published monthly during the academic year by the Cecil College Computer Science – Cybersecurity Club. Student-produced. For educational purposes only.

Campus IT emergencies: [CONFIRM: IT contact]