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

VOL. 2 — ISSUE 1
JULY 2026
SUMMER BRIDGE EDITION

// MONTHLY CYBERSECURITY AWARENESS

CyberShield BULLETIN

⚡ SECURE YOUR WORLD — ONE CLICK AT A TIME

VOLUME 2 LAUNCH

// CYBERSHIELD BULLETIN · VOLUME 2 · ISSUE 1 · JULY 2026

Welcome to Volume 2 — A New Year, A New Chapter

When we published our first issue back in March 2026, we hoped to start a conversation about cybersecurity awareness at Cecil College. What we found instead was a community hungry for exactly this kind of practical, accessible security guidance — and a club ready to deliver it.

Volume 1 covered phishing, passwords, social engineering, and public Wi-Fi across four issues. We celebrated a 2nd place finish at the Maryland Cyber Cup, launched a newsletter that reached the entire Cecil College community, and said a proud farewell to our founding President, Elijah Smith. Now, with fall semester approaching and a new club year on the horizon, **Volume 2 is open for business.**

Vol. 2 · Issue 1 | New Club Year Ahead | Fall 2026 Preview

EDITOR'S WELCOME

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

Welcome to the **July 2026 Summer Bridge Edition** of the CyberShield Bulletin — and the opening issue of Volume 2. July is typically the quietest month on campus, but it is far from quiet in the world of cybersecurity. Summer is historically one of the most active periods for ransomware attacks against schools, hospitals, and government agencies — attackers know that IT staff are often reduced, students are away, and defenses are down.

This month we shine a light on ransomware — one of the most destructive and financially devastating cyber threats in the world — and give you practical steps to protect yourself, your

family, and your data. We also have an exciting preview of what is coming for the **CS-Cybersecurity Club in Fall 2026**, including new leadership opportunities, expanded programming, and some ambitious goals for the academic year ahead.

Summer goes fast. Fall semester arrives before you know it. We hope this issue keeps you sharp — and gets you excited about what is coming.

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

⚠ THREAT SPOTLIGHT

// JULY 2026 FEATURED THREAT

Ransomware: When Your Files Are Held Hostage

Risk Level: CRITICAL — Ransomware attacks on educational institutions increased 70% in 2025. Summer months — when IT staffing is reduced and systems go unmonitored — are peak attack season for schools and colleges.

What Is Ransomware?

Ransomware is a category of malware that infiltrates a computer or network, silently encrypts files — documents, photos, databases, entire drives — and then demands a ransom payment, often in cryptocurrency, in exchange for the decryption key. Without that key, your files are as good as gone. Paying the ransom is no guarantee of recovery, and it funds further attacks.

What makes ransomware so devastating is its speed and reach. Modern ransomware can encrypt tens of thousands of files in minutes and spread across an entire network — infecting every connected device — before anyone realizes something is wrong. By the time the ransom note appears on screen, the damage is already done.

How Does Ransomware Get In?

The most common entry points mirror what we have covered in earlier issues — and that is no coincidence. Ransomware almost always begins with a human decision:

ENTRY	FOOTHOLD	SPREAD	STRIKE
Phishing Email	**Install & Hide**	**Move Laterally**	**Encrypt & Demand**
Malicious attachment or link clicked by an employee or student	Malware installs silently, studies the network for days or weeks	Infects connected drives, servers, and networked devices	Files locked; ransom note displayed demanding crypto payment

Real-World Impact on Education

In 2025, a community college in the mid-Atlantic region suffered a ransomware attack during the summer break. The attack encrypted student records, financial aid databases, and the entire learning management system. With reduced IT staff on duty, the infection went undetected for four days before a faculty member noticed files were inaccessible. The college was forced to delay fall semester registration by two weeks, notify over 12,000 students of a potential data breach, and spend an estimated $1.2 million on remediation — none of which

was fully covered by insurance.

This is not a hypothetical scenario. It is the reality for dozens of educational institutions every year. And it starts with one click on one wrong email.

How to Protect Yourself and Your Data

Back up your files — regularly and correctly. This is the single most important defense against ransomware for individuals. If your files are backed up, a ransomware attack becomes a serious inconvenience rather than a catastrophe. See our Tip of the Month for the 3-2-1 backup rule.

Keep everything updated. Ransomware frequently exploits known vulnerabilities in operating systems and software. Enable automatic updates on your computer and phone. An unpatched system is an open door.

Do not click unexpected attachments. Review our March issue on phishing — this remains the #1 delivery mechanism for ransomware. If you did not expect an email with an attachment, do not open it without verification.

Use endpoint protection. Windows Defender (built into Windows 10/11) provides solid baseline ransomware protection. Enable "Controlled Folder Access" in Windows Security settings — it blocks unauthorized apps from modifying files in protected folders.

💡 TIP OF THE MONTH

The 3-2-1 Backup Rule: Your Ransomware Insurance Policy

> *If ransomware strikes and you have a current backup, you can restore your files and walk away without paying a cent. If you do not have a backup, you may lose everything. The 3-2-1 rule is the gold standard for personal and organizational data protection.*

🖥 3 copies · 2 different media · 1 offsite location

This simple formula has saved countless individuals and organizations from complete data loss.

What the 3-2-1 Rule Means

3	Total copies of your data, including the original
2	Different storage media types (e.g. external drive + cloud)
1	Copy stored offsite or in the cloud, away from your home network

Setting Up Your 3-2-1 Backup — Step by Step

1. **Identify what matters.** Documents, photos, schoolwork, financial records, creative projects. Make a mental inventory of what you cannot afford to lose.

2. **Set up cloud backup.** For Windows, enable **OneDrive** folder backup (built-in, free 5GB). For Mac, use **iCloud Drive**. For more storage, **Backblaze** backs up your entire computer for $99/year — the best value in personal cloud backup.
3. **Get an external hard drive** and connect it regularly for local backups. Windows Backup and macOS Time Machine automate this. A 1TB drive costs around $50–$60 and provides years of protection.
4. **Keep the external drive disconnected when not backing up.** A drive that is always connected can also be encrypted by ransomware. Plug it in, back up, then unplug and store it separately.
5. **Test your backups.** A backup you have never tested is a backup you cannot trust. Once a month, try restoring a single file from your backup to confirm it is working correctly.

> **Start this weekend:** Sign up for Backblaze or enable OneDrive/iCloud backup on your computer today. It takes under 10 minutes to set up and runs automatically from that point forward. Future-you will be very grateful.

CAREER CORNER

Spotlight: Incident Responder & Digital Forensics Analyst

Following our ransomware theme this month, we spotlight two of the most dynamic and in-demand roles in all of cybersecurity — the professionals who show up after an attack and take the system back.

What They Do

An **Incident Responder** is the cybersecurity equivalent of a first responder — called in when a breach, ransomware attack, or intrusion is detected. They contain the damage, eradicate the threat, recover systems, and document what happened. An **Digital Forensics Analyst** goes deeper — analyzing disk images, memory dumps, and logs to reconstruct exactly how an attack unfolded, who was responsible, and what data was accessed. Both roles require deep technical knowledge and the ability to perform under pressure.

Relevant Certifications

CompTIA Security+ | CompTIA CySA+ | EC-Council CHFI | GCFE (GIAC)

Average salaries in the Maryland/DC metro region: $85,000–$130,000 for experienced incident responders. Entry-level roles typically start around $60,000–$70,000. Demand is extremely high — especially for candidates with hands-on experience from CTF competitions and lab environments.

How Cecil College Prepares You

Cecil College's CAE-CD curriculum directly aligns with the knowledge units required for these roles — including network forensics, malware analysis, and security operations. Combine your coursework with TryHackMe labs and club CTF experience, and you will be competitive for these positions at graduation.

> **Summer challenge:** Work through TryHackMe's "SOC Level 1" and "Jr Penetration Tester"

learning paths over the summer. These free paths directly map to incident response and forensics skills employers want. Document your progress and add it to your résumé.

[CLUB TO CONFIRM: Club mentorship contact]

DID YOU KNOW?

70%

Increase in ransomware attacks on educational institutions in 2025 vs. 2024

SOURCE: Sophos State of Ransomware in Education Report

$1.4M

Average cost to remediate a ransomware attack on a school or college in 2025

SOURCE: Sophos / Coveware, 2025

21 days

Average downtime experienced by organizations hit with ransomware before systems are restored

SOURCE: Coveware Quarterly Ransomware Report

Only 8%

Of organizations that pay a ransom recover all of their data — paying does NOT guarantee recovery

SOURCE: Sophos Ransomware Report, 2025

RESOURCES

Ransomware Defense Tools

StopRansomware.gov

stopransomware.gov

Official U.S. government resource with current ransomware alerts, advisories, and recovery guidance. Jointly operated by CISA, FBI, and NSA.

No More Ransom Project

nomoreransom.org

Free decryption tools for hundreds of known ransomware variants. Before paying any ransom, check here — your files may already be recoverable.

Backblaze Personal Backup

backblaze.com

$99/year for unlimited computer backup. One of the best investments in data security for individuals and families.

Windows Controlled Folder Access

support.microsoft.com

Built-in ransomware protection for Windows 10/11. Blocks unauthorized apps from modifying files in protected folders. Free — just enable it.

ID Ransomware

id-ransomware.malwarehunterteam.com

Upload a ransom note or encrypted file sample to identify which ransomware variant hit you — helps find the right decryption tool.

KEY DATES

Summer & Fall Calendar

AUG 1 — **August Newsletter Deadline**
Submit content for the back-to-campus September issue

AUG TBD — **Fall Registration Deadline**
Register for fall cybersecurity courses before they fill

[CONFIRM: Date]

SEP TBD — **Club Kickoff Meeting — Fall 2026**
New members, new leadership, new year! All welcome.

[CONFIRM: Date/Time/Room]

SEP TBD — **Officer Elections**
Club President, VP, Newsletter Editor, Outreach Coordinator

[CONFIRM: Date]

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

SUMMER READING

Keep Sharp This Summer

Three things you can do right now to stay sharp before fall semester:

🎮 TryHackMe.com

Complete 1 room per week. Free tier. Tracks your progress and builds real skills through hands-on challenges.

🎙 Darknet Diaries Podcast

True stories from the dark side of the internet. Fascinating, educational, and completely free. Excellent while commuting or exercising.

📖 "Sandworm" by Andy Greenberg

The definitive account of the world's most dangerous nation-state hackers. Required reading for anyone serious about cybersecurity as a career.

FALL 2026 — CECIL COLLEGE & CLUB PREVIEW

// FALL SEMESTER 2026 · CECIL COLLEGE · CS-CYBERSECURITY CLUB

Fall Semester Is Coming — Here Is What

to Expect

The Cecil College fall 2026 semester is just around the corner, and the CS-Cybersecurity Club is planning its most ambitious year yet. Whether you are returning for another semester, enrolling at Cecil for the first time, or joining the club fresh, here is everything you need to know about what is ahead.

Cecil College Fall 2026 — Academic Highlights

The fall semester brings the full return of Cecil College's cybersecurity curriculum, including hands-on labs, certification prep courses, and the advanced coursework that sets our program apart. Cecil's **NSA/DHS Center of Academic Excellence in Cyber Defense (CAE-CD)** designation means your courses are aligned with the most rigorous federal cybersecurity standards — the same standards used to train federal agency professionals.

New and returning students are encouraged to explore the Computer Science and Cybersecurity course offerings early — enrollment fills quickly, particularly for lab-based sections. Speak with your academic advisor about the right sequence for your goals, whether you are heading toward a transfer, a certification, or direct entry into the workforce.

Key programs to explore for Fall 2026:

📌 Computer Science – Cybersecurity track
📌 CompTIA certification prep courses (A+, Network+, Security+)
📌 Digital Forensics coursework
📌 Networking fundamentals and advanced tracks

`[CONFIRM: Specific fall course schedule / registration link]`

New to Cecil College? The CS-Cybersecurity Club is one of the most active student organizations on campus and a fantastic way to build skills, friendships, and career connections from your very first semester. No experience required — just curiosity and a willingness to learn. Come to our fall kickoff meeting and see for yourself.

Club Year 2026–2027 — What to Expect

With our founding president Elijah Smith having graduated in June, the club enters a new chapter — building on an outstanding foundation and reaching even higher. Here is what the incoming leadership team has planned for the 2026–2027 academic year:

🏆

CTF Competitions

Returning to the Maryland Cyber Cup and expanding to regional and national competitions. Team formation begins at the first fall meeting.

CyberShield Bulletin

Monthly through the full academic year — September through May. Student contributors welcome every issue.

Guest Speaker Series

Industry professionals, federal agency representatives, and alumni returning to share real-world experience and career advice.

Certification Study Groups

Structured, peer-led study sessions for CompTIA Security+, CySA+, and other certifications — free and open to all members.

Internship & Job Pipeline

Connecting members with internship opportunities, federal programs, and local employers actively seeking Cecil graduates.

Community Outreach

Expanding our cybersecurity awareness programs beyond campus — to K-12 schools, local businesses, and the broader community.

// OPEN OFFICER POSITIONS — FALL 2026

Club President	Lead bi-weekly meetings, represent the club at college events, coordinate with faculty advisors, and set the strategic direction for the year.	OPEN
Vice President	Support the president, lead technical workshops, organize CTF team formation, and step in when the president is unavailable.	OPEN
Newsletter Editor	Own the CyberShield Bulletin — coordinate contributors, manage the editorial calendar, and work with advisors on final content each month.	OPEN
Outreach Coordinator	Manage club social media, coordinate community awareness events, and build relationships with other student organizations and local partners.	OPEN
Faculty Advisors	Professor Jacqueline Wilson & Dr. James Morgan — providing guidance, academic support, and institutional continuity across all club activities.	CONFIRMED

Interested in running for office? Reach out before the fall kickoff meeting to express your interest. Officer positions are open to any currently enrolled Cecil College student in good academic standing. Leadership experience in the club is a genuine résumé differentiator — especially for cybersecurity and technology roles.

`[CONFIRM: Contact email for officer interest]`

VOL. 2 EDITORIAL CALENDAR — FALL 2026

SEPTEMBER 2026 · VOL. 2 ISSUE 2

Back to Campus: Securing Your Devices

Fall semester checklist — securing laptops, cloud accounts, and campus network connections. New student security orientation guide.

OCTOBER 2026 · VOL. 2 ISSUE 3

Cybersecurity Awareness Month — Special Edition

Our biggest issue of the year. Campus events, workshops, a community security challenge, and guest contributors from across the Cecil community.

NOVEMBER 2026 · VOL. 2 ISSUE 4

Holiday Scam Season: Staying Safe Online

Fake e-commerce sites, gift card fraud, charity scams, and travel booking fraud — everything you need to know before the holiday shopping rush.

DECEMBER 2026 · VOL. 2 ISSUE 5

Year in Review & 2027 Threat Forecast

The biggest cybersecurity stories of 2026, our club's year in review, and a forward look at the threats and trends to watch for in 2027.

CONTACT THE CLUB

📧 [CONFIRM: Club Email Address]

📍 Cecil College, North East, MD 21901

🌐 [CONFIRM: Club website or portal link]

📱 [CONFIRM: Social media handles]

SUBMISSIONS & CONTRIBUTIONS

Submissions for the September back-to-campus issue are due August 1. We welcome articles, tips, spotlights, and announcements from students, faculty, staff, and 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. It is a student-produced publication for educational purposes only.

Campus IT emergencies: [CONFIRM: IT Department contact]