

// MONTHLY CYBERSECURITY AWARENESS

CyberShield

BULLETIN

⚡ **SECURE YOUR WORLD — ONE CLICK AT A TIME**

🎉 **CONGRATULATIONS, CLASS OF 2026!**

// CECIL COLLEGE · COMMENCEMENT 2026

Here's to the **Class of 2026** — Go Forth and Secure the World!

June marks a milestone at Cecil College as students from across every program cross the stage and carry their knowledge, skills, and determination into the next chapter of their lives. To every graduate: your hard work, resilience, and curiosity have brought you here. The world you are entering needs people who care about doing things right — and that is exactly who you are.

The Cybersecurity Club is immensely proud of every member who graduates this year. You have not just earned a degree — you have built a foundation for a career at the forefront of one of the most critical fields in the modern world.

🎓 **Class of 2026**

✓ **Cecil College**

✚ **Go Seahawks!**

🛡️ **Cyber Ready**

★ **GRADUATE SPOTLIGHT**

// CS-CYBERSECURITY CLUB · CLUB PRESIDENT · CECIL COLLEGE CLASS OF 2026

Elijah Smith

CLUB PRESIDENT · COMPUTER SCIENCE - CYBERSECURITY

It is with enormous pride and deep admiration that the Cecil College CS-Cybersecurity Club congratulates our outgoing President, **Elijah Smith**, on his graduation from Cecil College.

Elijah has been the heartbeat of this club — a natural leader, tireless organizer, and genuine champion for cybersecurity education across our entire campus community.

Under Elijah's leadership, the club has grown in impact, visibility, and achievement. He led the team to a **2nd place finish at the UMBC Maryland Cyber Cup** in March 2026, helped launch the **CyberShield Bulletin** newsletter — now in its fourth issue — and created a welcoming environment where students of all backgrounds and skill levels felt they belonged.

Elijah brought energy to every meeting, wisdom to every challenge, and heart to every interaction. He understood early on that cybersecurity is ultimately about people — protecting them, educating them, and empowering them. He carried that belief into everything he did.

 **Maryland Cyber Cup — 2nd Place**

 **Co-Founded CyberShield Bulletin**

 **Club President — CS-Cybersecurity Club**

 **CAE-CD Designated Institution Alumni**

 **Cecil College Class of 2026**

// FROM THE FACULTY ADVISORS

"Elijah has exemplified what it means to be a servant-leader. He never sought the spotlight for himself — he always shone it on his teammates and the mission of the club. We are incredibly proud of everything he has accomplished and absolutely certain that the cybersecurity community is gaining an exceptional professional. We will miss his leadership dearly, but we know his best work is still ahead of him."

— **Professor Jacqueline Wilson & Dr. James Morgan, Faculty Advisors**

Congratulations, Elijah! 🎉👏

From everyone in the Cecil College CS-Cybersecurity Club — we are proud of you and grateful for everything you gave to this community.

EDITOR'S WELCOME

FROM THE FACULTY ADVISORS & THE CS-CYBERSECURITY CLUB

Welcome to **Volume 1, Issue 4** of the CyberShield Bulletin — our summer edition, and the final issue before our fall semester return. June is a month of transitions: graduations, travel, internships beginning, and a well-earned change of pace. It is also, unfortunately, a prime season for cybercriminals who know that our guards are often down when we are relaxed and on the move.

This month we cover one of the most underestimated security risks that most people encounter every single summer: **public Wi-Fi**. Airport lounges, hotel lobbies, coffee shops, and vacation rental networks are hunting grounds for attackers. We will walk you through exactly what the risks are and — more importantly — how to enjoy your summer without becoming a statistic.

We also have the joy this issue of celebrating our graduates, and especially our remarkable outgoing Club President, **Elijah Smith**. On behalf of the entire club family, thank you for reading, stay safe out there, and have a wonderful summer.

// JUNE 2026 FEATURED THREAT

Public Wi-Fi: The Invisible Danger at Your Favorite Summer Spots

 **Risk Level: HIGH** — Over 25% of public Wi-Fi hotspots worldwide use no encryption at all. Connecting to them is the digital equivalent of having a conversation in the middle of a crowded room — anyone nearby can listen in.

Why Public Wi-Fi Is Dangerous

When you connect to a public Wi-Fi network — at an airport, coffee shop, hotel, or vacation rental — you are sharing that network with strangers. Unlike your home network, where you control who connects, a public hotspot may have dozens or hundreds of unknown users. Some of those users may be attackers actively monitoring traffic.

The fundamental problem is that unencrypted or weakly encrypted networks allow attackers to intercept data traveling between your device and the internet. This is called a **Man-in-the-Middle (MitM) attack** — the attacker positions themselves silently between you and the websites you visit, reading everything that passes through.

The Most Common Public Wi-Fi Attacks

Man-in-the-Middle (MitM) Attack

The attacker intercepts communication between your device and the network. They can read your messages, capture login credentials, and even alter webpages you visit — silently and without your knowledge. You see nothing unusual while it happens.

Evil Twin Hotspot

An attacker sets up a rogue Wi-Fi network with a name nearly identical to a legitimate one — "Airport_Free_WiFi" next to the real "Airport_WiFi." When you connect to the fake network, all your traffic routes through the attacker's device. This is trivially easy to execute with a \$35 device and free software.

Unencrypted Traffic Sniffing

On unencrypted networks, a basic packet-sniffing tool — freely available and legal to own — can capture every byte of data your device sends. Any website you visit that uses HTTP (not HTTPS) exposes everything you type in plain text, including usernames, passwords, and form entries.

Session Hijacking

Even after you log into a website over a secure connection, your session may be tracked by a cookie. On an unencrypted network, an attacker can steal that session cookie and use it to access your account — without ever knowing your password. Your banking session, email, or

social media can be hijacked this way.

What About HTTPS? Am I Safe?

HTTPS encrypts the content of your communication, which is a significant protection. However, it does not hide *which* websites you visit (that metadata is still visible), and it does not protect you from Evil Twin attacks, DNS manipulation, or malware installed via the network. HTTPS is necessary but not sufficient on public Wi-Fi.

// IF YOUR DEVICE IS LOST OR STOLEN WHILE TRAVELING

Act immediately: remotely lock or wipe the device using Find My iPhone (Apple), Find My Device (Android/Google), or Find My Device (Windows). Change passwords for all accounts accessible on that device — starting with email and banking. Contact your carrier to suspend the SIM. File a police report if needed for insurance purposes.

TIP OF THE MONTH

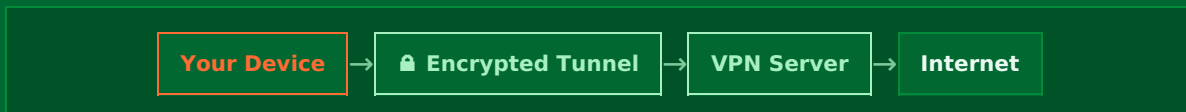
Use a VPN on Every Public Network — Here's How

A Virtual Private Network (VPN) is your single most effective defense on public Wi-Fi. It encrypts all your traffic before it leaves your device, making it unreadable to anyone on the same network — including your internet provider.

A VPN encrypts your traffic end-to-end, even on the most dangerous public networks.

Think of it as a private, armored tunnel from your device to the internet — no one can see inside.

How a VPN Works



Without a VPN, the attacker sits between "Your Device" and "Internet" and reads everything. With a VPN, all they see is encrypted noise.

Setting Up a VPN — Step by Step

- 1 Choose a reputable VPN service. **Recommended options:** ProtonVPN (free tier available, Swiss-based, no-logs policy), Mullvad (privacy-focused, accepts anonymous payment), or ExpressVPN / NordVPN (paid, widely trusted). **Avoid free VPNs that have no clear business model** — if it is free, your data may be the product.
- 2 Download the app on every device you travel with — phone, laptop, and tablet.
- 3 Enable the VPN *before* connecting to any public or unknown network. Make it a habit: open VPN app → connect → then open browser.
- 4 Choose a server in your home country for the best performance, unless you have reason to appear in another location.
- 5 Enable the **kill switch** feature if available — this disconnects your internet if the VPN drops, preventing accidental exposure.

Your Summer Travel Security Checklist

- ✓ Install and test your VPN *before* you leave home
- ✓ Enable full-disk encryption on your laptop (BitLocker on Windows, FileVault on Mac)
- ✓ Set a strong PIN/password and enable biometric lock on your phone
- ✓ Enable "Find My Device" and remote wipe on all devices before you travel
- ✓ Avoid accessing banking or sensitive accounts on public Wi-Fi — use mobile data instead
- ✓ Verify the exact Wi-Fi network name with hotel/café staff before connecting
- ✓ Log out of all accounts and clear saved passwords before crossing international borders
- ✓ Keep your OS and apps fully updated before departure — patches close known vulnerabilities

Pro tip for international travel: Border agents in some countries have legal authority to demand device access. Keep a travel device with minimal data if you are concerned, or use full-disk encryption and power off the device before crossing any border checkpoint.

CAREER CORNER

What Comes Next? Pathways for Our Graduates

For students graduating from Cecil College's cybersecurity program — including our own Elijah Smith — the transition into the workforce or continued education opens several exciting paths.

Transfer Pathways

Cecil College has transfer agreements with several Maryland four-year institutions. Cybersecurity graduates are particularly well-positioned for programs at **University of Maryland, UMBC, Towson University**, and **Capitol Technology University**. Cecil's CAE-CD designation is recognized and respected at all of these programs.

Entry-Level Roles to Target

SOC Analyst I

Help Desk / IT Support

Network Technician

Junior Penetration Tester

The **SOC (Security Operations Center) Analyst** role is the most in-demand entry point into cybersecurity careers. It involves monitoring networks for threats, triaging alerts, and responding to incidents. Starting salaries in the Maryland/DC region range from **\$55,000-\$75,000**, and the role provides rapid skill growth.

Certifications That Open Doors

If you have not already, prioritize earning **CompTIA Security+** before or shortly after graduation — it is a baseline requirement for many federal and private-sector positions in our region. Pair it with **CompTIA A+** or **Network+** if your background needs strengthening in IT fundamentals.

Stay connected: Club alumni are encouraged to stay in touch with Professor Wilson and Dr. Morgan. We actively support members with references, job leads, and mentorship long after graduation. [\[CONFIRM: Club alumni contact email\]](#)

25%

Of public Wi-Fi hotspots worldwide use no encryption whatsoever

SOURCE: Kaspersky Global Wi-Fi Report

1 in 4

Users have had information stolen while using public Wi-Fi

SOURCE: Norton Cyber Safety Insights Report

40%

Of people have connected to a Wi-Fi network they weren't sure was safe — including in airports and hotels

SOURCE: Symantec Wi-Fi Risk Report

\$35

Cost of equipment needed to set up a rogue Evil Twin Wi-Fi hotspot — accessible to anyone

SOURCE: DEF CON Security Research, 2025

Summer Security Tools

ProtonVPN

protonvpn.com

Free tier available. Swiss privacy laws, strict no-logs policy, and open-source apps. Excellent for students on a budget.

Mullvad VPN

mullvad.net

Privacy-first VPN with anonymous account creation. No email required to sign up. €5/month flat rate.

Apple Find My / Google Find My Device

apple.com/find-my / android.com/find

Enable before you travel. Allows remote location, lock, and wipe of lost or stolen devices.

HTTPS Everywhere (EFF)

eff.org/https-everywhere

Browser extension that forces encrypted HTTPS connections whenever available. Free from the Electronic Frontier Foundation.

Travel Safe — CISA Tips

cisa.gov/tips/st04-001

Official CISA guidance on cybersecurity while traveling — device security, border crossings, and public network safety.

Dates to Watch

JUN
TBD

Cecil College Commencement 2026

Congratulations to all graduates!

[CONFIRM: Ceremony date/location]

JUL-
AUG

Summer Internships Begin

Club members starting federal and private sector internships — reach out to share your experience!

AUG
15

Fall Semester Registration Deadline

Plan your fall schedule — CS and cybersecurity courses fill fast

SEP
2026

Club Resumes — Fall Kickoff

New leadership, new members welcome. Watch for announcement!

OCT
2026

National Cybersecurity Awareness Month

Special edition + major campus events. Our biggest issue yet!

CLASS OF 2026

Stay Connected After Graduation

Graduating does not mean leaving the community. Cecil College alumni are always welcome at club events, guest speaker sessions, and competition teams.

Alumni Network: Contact Professor Wilson or Dr. Morgan to stay on the club mailing list, receive job leads, or return as a guest speaker and mentor for current students. Your journey is an inspiration.

Cecil College's **CAE-CD designation** is a credential that follows you for life — list it proudly on your résumé and LinkedIn profile.

[CONFIRM: Alumni contact email]

CLUB CORNER

Leadership Transition & Fall 2026 Preview

With Elijah Smith graduating, the Cecil College CS-Cybersecurity Club will be welcoming new student leadership for the Fall 2026 semester. Officer elections and appointments will take place at our first fall meeting. If you are passionate about cybersecurity, leadership, and community — this is your moment.

Open Positions for Fall 2026

- ✦ **Club President** — Lead meetings, coordinate events, and represent the club across campus and at competitions.
- ✦ **Vice President** — Support the President, lead technical workshops, and coordinate CTF competition teams.
- ✦ **Newsletter Editor** — Take ownership of the CyberShield Bulletin, coordinate contributor

submissions, and work with faculty advisors on content.

✦ **Social Media / Outreach Coordinator** — Grow the club's visibility on campus and in the community.

Interested? Contact the club before September to express your interest.

[CONFIRM: Club contact email for officer interest]

Club Snapshot

Founded	2017
Faculty Advisors	Prof. Jacqueline Wilson & Dr. James Morgan
Outgoing President	Elijah Smith, Class of 2026 🌟
Meeting Frequency	Bi-Weekly (Fall)
Focus Areas	Scholarships, Internships, Ethical Hacking, Defense & Awareness
Open to	All Majors & All Levels

Thank you for a great inaugural year of CyberShield Bulletin! Vol. 1 wraps with this issue.
Vol. 2 returns in September 2026. Have a safe summer, Seahawks! 🦅

[CONFIRM: Club email]

📅 VOL. 2 PREVIEW — FALL 2026

SEPTEMBER 2026 • VOL. 2 ISSUE 1

Back to Campus: Securing Your Devices

Fall semester security checklist — securing laptops, cloud accounts, and safe use of campus and home networks as the academic year begins.

OCTOBER 2026 • VOL. 2 ISSUE 2

Cybersecurity Awareness Month — Special Edition

Our biggest issue yet — themed around National Cybersecurity Awareness Month with campus events, workshops, guest speakers, and a community security challenge.

NOVEMBER 2026 • VOL. 2 ISSUE 3

Holiday Scam Season: Staying Safe Online

Fake e-commerce sites, gift card fraud, charity scams, and travel booking fraud — the holiday threat landscape and how to shop safely.

DECEMBER 2026 • VOL. 2 ISSUE 4

Year in Review & 2027 Threat Forecast

A look back at the biggest cybersecurity stories of 2026 and a forward look at the emerging threats and trends our community should 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

The CyberShield Bulletin returns in September 2026 as Volume 2. Submissions for the September issue are due August 15.

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]