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

VOL. 2 — ISSUE 2
AUGUST 2026
PRE-SEMESTER EDITION

// MONTHLY CYBERSECURITY AWARENESS

CyberShield BULLETIN

⚡ SECURE YOUR WORLD — ONE CLICK AT A TIME

FALL SEMESTER IS ALMOST HERE!

// CECIL COLLEGE · FALL 2026 SEMESTER · PRE-SEMESTER COUNTDOWN

Fall Is Right Around the Corner — Are You Ready?

August means one thing at Cecil College: the new academic year is nearly here. New students are orienting, returning students are registering for final seats, and the campus is preparing to come alive again after the summer break. For the CS-Cybersecurity Club, it means something even more exciting — a brand-new year of competitions, learning, community, and leadership opportunities.

This edition is your complete pre-semester briefing: what to expect from the fall semester, what the club has planned, and — because we are a cybersecurity newsletter — the security threat you should know about before you plug any new device into a campus or home network this fall.

Fall Semester Incoming | Seahawks Cyber Club | IoT Security Alert

EDITOR'S WELCOME

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

Welcome to the **August 2026 Pre-Semester Edition** of the CyberShield Bulletin — Volume 2, Issue 2. If July was our summer bridge, August is the on-ramp. The pace picks up now: course schedules finalize, syllabi appear, and the familiar energy of a new academic year begins to build.

For the CS-Cybersecurity Club, August is a month of preparation and anticipation. New leadership will be stepping into place. New members will be discovering us for the first time. And the entire club — returning members, incoming freshmen, transfer students — will be

coming together around a shared commitment to learning, competing, and securing our digital world.

This month's threat topic hits particularly close to home as students move into dorms, set up home offices, and connect new devices to college and home networks: **IoT (Internet of Things) security**. Smart TVs, gaming consoles, printers, smart speakers, and networked devices of all kinds are a growing attack surface — one that most people give very little thought to. We will change that this month.

Welcome back, Seahawks. Let's make this a great year.

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

⚠ THREAT SPOTLIGHT

// AUGUST 2026 FEATURED THREAT

IoT Insecurity: Every Smart Device in Your Dorm Is a Potential Open Door

Risk Level: HIGH & RISING — The average home now contains 21 connected devices. College students returning to campus — with smart TVs, gaming consoles, printers, speakers, and streaming sticks — are bringing an enormous, largely unsecured attack surface into shared campus and home networks.

What Is the IoT — and Why Should You Care?

The **Internet of Things (IoT)** refers to any device that connects to the internet beyond traditional computers and phones: smart TVs, gaming consoles, wireless printers, smart speakers (Alexa, Google Home), robot vacuums, smart thermostats, network cameras, streaming sticks, and even modern appliances. These devices are everywhere — and most of them were designed with convenience and cost-efficiency as priorities, not security.

Many IoT devices ship with **default passwords that are publicly known** ("admin/admin," "1234," "password"), run outdated operating systems that are never patched, and transmit data over the network in unencrypted form. Attackers actively scan for these devices — automated tools identify vulnerable IoT hardware on public and campus networks within minutes of them connecting.

Common Vulnerable Devices Students Bring to Campus

📺 Smart TVs

Often run outdated Android or proprietary firmware. Rarely updated by users. Can be hijacked to spy on a room via microphone or camera, or used as a network pivot point.

🎮 Gaming Consoles

Less risky than other IoT but can expose your network credentials and personal data if compromised. Keep firmware updated and enable two-factor authentication on gaming accounts.

🖨 Wireless Printers

Among the most exploited IoT devices. Many printers have open web interfaces accessible on the network with no password. Can be used to steal documents or as a network entry point.

🔊 Smart Speakers

Always-on microphones connected to cloud servers. Voice recordings are stored and processed remotely. On shared campus networks, any device on the network can potentially communicate with them.

📺 Streaming Sticks

Roku, Fire Stick, Chromecast, and similar devices often run outdated software and broadcast network information. Keep auto-updates enabled and use strong Wi-Fi passwords.

📷 Smart Cameras

Arguably the highest-risk IoT device. Baby monitors, security cameras, and webcams with default passwords have been publicly streamed by attackers — a serious privacy violation.

How Attackers Use Compromised IoT Devices

A hacked IoT device is not just a personal problem — it becomes a weapon. Compromised devices are routinely recruited into **botnets**: networks of infected machines used to launch massive DDoS (Distributed Denial of Service) attacks, send spam, mine cryptocurrency, or serve as a launchpad for attacks on other devices on the same network. The 2016 Mirai botnet — which took down major websites including Twitter, Netflix, and Reddit — was built almost entirely from compromised IoT devices like DVRs and IP cameras.

Closer to home: on a shared campus or apartment network, a single compromised IoT device can give an attacker visibility into network traffic from every other device on that network — including your laptop, phone, and student portal login.

> *"We do not think about our smart TV the same way we think about our laptop — but attackers do. Every connected device is a potential entry point, and IoT devices are often the least defended ones on any network."*
>
> — CISA IoT Security Guidance, 2025

💡 TIP OF THE MONTH

Lock Down Your IoT Devices Before the Semester Starts

> *You do not need to be a network engineer to dramatically improve the security of your connected devices. These steps take under 30 minutes and significantly reduce your exposure before you plug in for the fall semester.*

🔐 Changing default passwords on your IoT devices is the single highest-impact security action you can take this month.

Your IoT Security Setup Checklist

1. **Inventory every connected device.** Walk through your room or home and list every device that connects to Wi-Fi or Ethernet — TV, printer, speaker, console, camera, thermostat. If it connects, it is on your list.
2. **Change every default password immediately.** Log into each device's admin interface (usually through a browser or its companion app) and change the default password to something unique and strong. Use your password manager (remember April's issue!) to generate and store these.

3. **Enable automatic updates on every device.** Most IoT devices have a setting for automatic firmware updates — turn it on. If your device cannot be updated, seriously consider replacing it.

4. **Disable features you do not use.** Many IoT devices have remote access, UPnP, and cloud connectivity enabled by default. If you do not use these features, disable them — each one is a potential attack surface.

5. **Isolate IoT devices on a separate network if possible.** If your home router supports a guest network, put your smart TV, printer, and speakers on it — separate from the network your laptop and phone use. This limits what an attacker can reach if a device is compromised. Campus networks typically handle this segmentation for you.

6. **Cover or disable cameras when not in use.** A physical webcam cover (under $5) is the most reliable privacy protection for any camera-equipped device.

> **Quick win for this week:** Right now, go change the admin password on your home Wi-Fi router. Most people never change this from the factory default — and attackers know every factory default password for every common router model. This one action protects every device on your network.

🎓 CAREER CORNER

The IoT Security Specialist: A Career Exploding in Demand

As billions of new IoT devices come online each year — in homes, hospitals, factories, and cities — the need for professionals who specialize in securing them is growing faster than almost any other cybersecurity specialty.

What the Role Involves

IoT Security Specialists assess, test, and harden connected devices and the networks they operate on. The work spans firmware analysis, network protocol security, penetration testing of embedded systems, and advising manufacturers on secure-by-design principles. It is a uniquely multidisciplinary role — combining hardware knowledge, network security, and software security in ways that most purely IT-focused roles do not.

Relevant Certifications & Skills

`CompTIA Security+` `CompTIA CySA+` `GICSP (ICS/OT)` `CEH (EC-Council)`

Starting salaries for IoT security roles in the Mid-Atlantic region range from **$70,000–$95,000**, rising quickly with experience. The federal government and defense contractors in the Maryland/DC corridor are actively recruiting for OT (Operational Technology) and IoT security positions — a natural fit for Cecil CAE-CD graduates.

> **Fall club opportunity:** We are planning an IoT security hands-on lab session this fall — capturing and analyzing network traffic from common consumer devices. No prior experience needed. Watch for the announcement at our kickoff meeting.
>
> `[CLUB TO CONFIRM: Lab session date]`

💡 DID YOU KNOW?

DID YOU KNOW?

21

Average number of connected devices per U.S. household in 2026 — up from 11 in 2021

SOURCE: Deloitte Connectivity Report, 2026

57%

Of IoT devices are vulnerable to medium- or high-severity attacks due to unpatched firmware

SOURCE: Palo Alto Networks IoT Threat Report

98%

Of IoT device traffic is unencrypted, exposing data and credentials on the network

SOURCE: Palo Alto Networks, Unit 42

5 min

Average time before a new, unprotected IoT device is discovered and probed by automated scanners after connecting to the internet

SOURCE: SANS Internet Storm Center

RESOURCES

IoT Security Tools & Guides

CISA — IoT Security Guide

cisa.gov/iot

Official federal guidance on securing smart home and office devices. Plain-language tips for consumers and students.

Shodan.io

shodan.io

The "search engine for IoT devices." Ethically use it to see what your public-facing devices reveal to the internet — educational and eye-opening.

RouterSecurity.org

routersecurity.org

Comprehensive, plain-language guide to securing home routers — the most important device on your home network.

NIST IoT Cybersecurity

nvlpubs.nist.gov (SP 800-213)

The federal standard for IoT security. Valuable reading for students interested in policy, compliance, or federal contracting roles.

Fing — Network Scanner

fing.com

Free mobile app that shows every device on your network. Run it to audit your home or dorm network and identify unknown devices.

KEY DATES

August & Fall Calendar

AUG 15 — **September Newsletter Deadline**
Submit content for the back-to-campus issue

AUG TBD — **Fall Registration Closes**
Secure your cybersecurity course seats now
`[CONFIRM: Exact date]`

SEP TBD — ⚜ **Club Fall Kickoff Meeting**
All are welcome — new members especially!
`[CONFIRM: Date/Time/Room]`

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

SEP TBD — **IoT Security Hands-On Lab**
Club session — all skill levels welcome
`[CONFIRM: Date/Time]`

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

👋 NEW TO CECIL?

Welcome, Incoming Students!

If you are starting at Cecil College this fall, the CS-Cybersecurity Club is one of the best decisions you can make from day one. Here is what you get as a member:

- ✓ Hands-on labs and skill-building sessions
- ✓ CTF competition team membership
- ✓ Certification study groups (Security+, and more)
- ✓ Networking with industry professionals
- ✓ Internship & scholarship guidance
- ✓ A community that takes your growth seriously

No experience required. We were all beginners once. Come to the fall kickoff meeting and find out what we are all about. `[CONFIRM: Club email / social media]`

🍂 FALL 2026 — CECIL COLLEGE & CLUB PREVIEW

// FALL SEMESTER 2026 · CECIL COLLEGE · CS-CYBERSECURITY CLUB · ACADEMIC YEAR 2026-2027

The New Academic Year Is Here — Here Is Everything You Need to Know

Fall 2026 marks the beginning of a new chapter for Cecil College's cybersecurity community. With a fresh leadership team stepping up, an ambitious programme of events and competitions in place, and a newsletter now in its second volume, the Seahawks Cyber Club enters the year with momentum, purpose, and high expectations.

Cecil College Fall 2026 — What to Expect Academically

The fall semester brings the full return of Cecil's cybersecurity and computer science curriculum — hands-on lab sections, certification prep courses, and the program depth that makes our **NSA/DHS CAE-CD designation** meaningful. The CAE-CD designation is not ceremonial: it signals that Cecil's cybersecurity curriculum meets the rigorous knowledge-unit requirements set by the federal government for programs that produce cyber-ready graduates.

Back-to-Campus Security Checklist

Before you plug anything in or log on, run through these eight steps:

1 Update Everything

OS, browsers, apps, and firmware on all devices before connecting to any network. Patches close the doors attackers walk through.

2 Enable MFA on All Accounts

Especially your Cecil College portal, email, and financial aid accounts. Reviewed in detail in our March issue.

3 Audit Your Passwords

Use your password manager (April's tip) to identify and update any weak or reused passwords before the semester starts.

4 Secure Your IoT Devices

Change default passwords and enable auto-updates on every smart device before it touches the network. See this month's Tip of the Month.

5 Back Up Your Files

Semester projects, notes, and important documents. The 3-2-1 rule from July's issue — local backup plus cloud. Do it before the semester starts.

6 Know Campus IT Resources

Save the Cecil IT helpdesk number and email. Know how to report suspicious emails and who to contact if your account is compromised.

7 Use Campus VPN When Off-Site

Cecil provides VPN access for remote students. Use it when accessing college resources from public or shared networks. See June's issue for setup guidance.

8 Join the Cybersecurity Club

Show up to the fall kickoff meeting. Everything you need to build a cybersecurity career starts here.

`[CONFIRM: Date/Time/Room]`

CS-Cybersecurity Club — 2026-2027 Goals & Expectations

The incoming leadership team, guided by faculty advisors Professor Jacqueline Wilson and Dr. James Morgan, has set ambitious goals for the new club year. Here is what every member — new and returning — can look forward to and be held to:

Win a CTF

Target top-3 finish at Maryland Cyber Cup and participate in at least two additional competitions.

12 Issues

Publish the CyberShield Bulletin every month, September through May, with at least one student-authored feature per issue.

5 Certifications

Support at least five members in earning a new cybersecurity certification this academic year through study groups and exam guidance.

Grow Membership

Welcome at least 15 active members by October — expanding our reach across all programs and class years.

3 Internships

Help at least three members land cybersecurity internships or co-ops through the club's employer network and advising.

Community Reach

Deliver at least two community cybersecurity awareness workshops outside of campus — schools, libraries, or local businesses.

Open Officer Positions — Fill These at the Fall Kickoff

Club President	Lead the club, coordinate with advisors, represent Cecil at external events and competitions.	OPEN
Vice President	Lead technical programming, run workshops, and coordinate CTF team selection.	OPEN
Newsletter Editor	Own the CyberShield Bulletin — manage contributors, calendar, and monthly production.	OPEN
Outreach Coordinator	Social media, community events, recruitment, and partnerships with other campus organizations.	OPEN
Faculty Advisors	Prof. Jacqueline Wilson & Dr. James Morgan — institutional continuity, mentorship, and program support.	CONFIRMED

What we expect from every member: Show up with curiosity and a willingness to grow. Help each other. Represent Cecil College with integrity in every competition and community interaction. And remember — cybersecurity is a team sport.

`[CONFIRM: Officer interest contact email]`

CLUB SNAPSHOT

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

CyberShield Bulletin — Volume 2 Schedule

Vol. 2 Issue 1	**July 2026 ✓**
Vol. 2 Issue 2	**August 2026 ✓**
Vol. 2 Issue 3	**September 2026 — Back to Campus**
Vol. 2 Issue 4	**October 2026 — Awareness Month ★**
Vol. 2 Issue 5	**November 2026 — Holiday Scams**
Vol. 2 Issue 6	**December 2026 — Year in Review**

Submissions for the September issue are due August 15. Submit articles, tips, spotlights, or event announcements to `[CONFIRM: Submission email]`

CONTACT THE CLUB

📧 `[CONFIRM: Club Email]`

📍 Cecil College, North East, MD 21901

🌐 `[CONFIRM: Club website]`

📱 `[CONFIRM: Social media handles]`

SUBMISSIONS & CONTRIBUTIONS

September back-to-campus issue submissions due **August 15**. 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. Student-produced. Educational purposes only.

Campus IT emergencies: `[CONFIRM: IT contact]`
