

// MONTHLY CYBERSECURITY AWARENESS

CyberShield

BULLETIN

⚡ SECURE YOUR WORLD — ONE CLICK AT A TIME

EDITOR'S WELCOME

FROM THE CLUB PRESIDENT & FACULTY ADVISOR

Welcome to the very first issue of the **CyberShield Bulletin** — your monthly guide to navigating the digital world safely. We are the Cecil College Computer Science - Cybersecurity Club, and we are thrilled to launch this newsletter for our entire community: faculty, staff, students, and neighbors.

Cybersecurity is no longer just a concern for IT departments or tech professionals. Every one of us — whether checking email, shopping online, or using campus Wi-Fi — is a potential target. The threats are real, evolving, and increasingly sophisticated. But the good news? **Awareness is your most powerful defense.**

Each month, we will bring you the latest threat intelligence, practical tips you can use immediately, campus resources, career insights, and a window into the exciting work our club is doing. No jargon overload — just clear, actionable information designed for every member of our community.

Thank you for joining us. Stay curious, stay cautious, and stay secure.

Elijah Smith, President — CS Cybersecurity Club
Professor Jacqueline Wilson & Dr. James Morgan, Faculty Advisors

▲ THREAT SPOTLIGHT

// MARCH 2026 FEATURED THREAT

AI-Powered Phishing: The New Face of a Familiar Attack

 **Risk Level: HIGH** — Colleges and universities are among the top targets for phishing campaigns due to their open networks, high email volume, and diverse user populations.

What Is It?

Phishing is not new — it is the practice of sending deceptive emails or messages designed to trick you into revealing passwords, financial information, or clicking malicious links. But in 2026, attackers are using **artificial intelligence (AI)** to craft phishing messages that are alarmingly convincing. Gone are the days of obvious spelling errors and awkward phrasing. Today's AI-generated phishing emails can perfectly mimic your professor, your bank, or even Cecil College's IT department.

How Does It Work?

Attackers use AI tools to scrape publicly available information — your LinkedIn profile, social media, or college directory — to personalize attacks. This technique is called **spear phishing**: targeted attacks crafted specifically for you. An email might reference your actual course schedule, greet you by name, and appear to come from a professor asking you to "review an attached document" — which is actually malware.

A newer variant uses **deepfake audio or video**. Imagine receiving a voicemail that sounds exactly like your department head asking you to wire money or share your login credentials urgently. These synthetic voices are now generated in seconds using freely available AI tools.

Who Does It Target?

Everyone. But students are particularly vulnerable during high-stress periods like financial aid deadlines, registration, and exam season — when a fake email about a "tuition payment issue" feels urgent and real. Faculty and staff are targeted for access to institutional systems, research data, and payroll.

How to Protect Yourself

Think before you click. Regardless of how legitimate an email looks, verify unexpected requests through a separate channel — call the person directly using a known number, not one provided in the suspicious email.

Look for these red flags: unexpected urgency or fear-based language, requests for login credentials or payment, email addresses that look almost-but-not-quite right (e.g., *cecilcollege.edu.org*), and links that don't match the display text (hover your cursor over links to preview the real URL).

When in doubt, report it. Cecil College's IT department

[CLUB TO CONFIRM: IT reporting email/portal] can evaluate suspicious emails quickly. One report could protect the entire campus.

TIP OF THE MONTH

Enable Multi-Factor Authentication (MFA) — Right Now

This month's tip is simple, free, and one of the most powerful things you can do to protect your accounts. Experts agree: MFA stops over 99% of automated account attacks.

 **MFA blocks 99.9% of account compromise attacks.**

What Is MFA?

Multi-Factor Authentication (MFA) — also called Two-Factor Authentication (2FA) — adds a second verification step when you log in. Even if someone steals your password, they still cannot access your account without this second factor.

How to Set It Up — Step by Step

- 1 Go to the account you want to secure (email, banking, social media, Cecil College portal).
- 2 Navigate to **Settings** → **Security** (or "Privacy & Security").
- 3 Look for **"Two-Factor Authentication," "Multi-Factor Authentication," or "Login Verification"** and enable it.
- 4 Choose your second factor: an **authenticator app** (like Google Authenticator or Microsoft Authenticator) is most secure. SMS text codes are also better than nothing.
- 5 Save your backup codes in a safe place — these allow access if you lose your device.

Priority accounts to protect first: Your Cecil College student/faculty email, financial aid portal, bank accounts, and any account that stores personal information or payment details.

CAREER CORNER

Breaking Into Cybersecurity: Start with CompTIA Security+

Cybersecurity is one of the fastest-growing career fields in the world, with the U.S. Bureau of Labor Statistics projecting 33% job growth through 2033 — far exceeding the national average. And you don't need a four-year degree to get started.

Spotlight Certification

CompTIA Security+

CompTIA A+

Google Cybersecurity Certificate

CompTIA Security+ is the industry's most widely recognized entry-level cybersecurity certification. It validates foundational skills in threat detection, risk management, cryptography, and network security. Most employers in government and private sector accept it as a baseline credential.

Cost: Approximately \$392 (exam vouchers; study materials vary). **Cecil College students** should check with Financial Aid and the CS department for potential voucher programs.

[CLUB TO CONFIRM: Any campus discount programs]

Study time: Most candidates prepare in 2–3 months with consistent study of 1–2 hours per day. Free resources include Professor Messer's CompTIA Security+ course on YouTube and practice exams at ExamCompass.com.

DID YOU KNOW?

3.4B

Phishing emails sent every single day worldwide

SOURCE: AAG IT Services, 2025

74%

Of data breaches involve human error — clicking a bad link or using a weak password

SOURCE: Verizon DBIR, 2025

\$9.9M

Average cost of a data breach in the U.S. — highest in the world

SOURCE: IBM Cost of a Data Breach Report, 2025

61%

Of college students reuse passwords across multiple accounts

SOURCE: Security.org Annual Survey



RESOURCES

Free Cybersecurity Tools

Have I Been Pwned?

haveibeenpwned.com

Check if your email or phone number has appeared in a known data breach. Free and instant.

CISA — Stop. Think. Connect.

cisa.gov/stopthinkconnect

Official U.S. government cybersecurity awareness resources, guides, and toolkits for all ages.

Google Safety Check

myaccount.google.com/security-checkup

Quickly audit your Google account security: passwords, 2FA, and connected apps.

StopRansomware.gov

stopransomware.gov

Federal guidance and alerts on ransomware. Essential reading for institutions and individuals.

Bitwarden (Password Manager)

bitwarden.com

Free, open-source password manager. Generate and store strong, unique passwords for every account.



UPCOMING

Dates to Watch

MAR

Club Meeting — Spring Kickoff

15

[CONFIRM: Time/Room]

MAR

National Security Awareness Day

20

Visit our info table in the Student Center

[CONFIRM]

APR

April Newsletter Submission Deadline

1

Submit tips & articles to the club email

APR

Spring CTF Competition

TBD

Capture the Flag — all skill levels welcome!

[CONFIRM DETAILS]

OCT

National Cybersecurity Awareness Month

2026

Mark your calendar — big events planned!



CLUB CORNER

About the CS Cybersecurity Club

The Cecil College Computer Science – Cybersecurity Club is a student-led organization dedicated to building real-world cybersecurity skills, fostering a security-aware campus community, and connecting members with career opportunities in one of the world's fastest-growing fields.

We host workshops, hands-on labs, Capture the Flag (CTF) competitions, and guest speaker events. Whether you're a total beginner or an advanced student, you belong here. **No experience required — just curiosity.**

How to Join

Membership is open to all Cecil College students, faculty, and staff. Attend any meeting to get started — no formal signup required.

[CLUB TO CONFIRM: Meeting day, time, and room number]

[CLUB TO CONFIRM: Club email address and social media handles]

Club Snapshot

Founded

2017

Faculty Advisor

Prof. Jacqueline Wilson & Dr. James Morgan

Meeting Frequency

Bi-Weekly

Focus Areas

Scholarships, Internships, Ethical Hacking, Defense & Awareness

Open to

All Majors & All Levels

Want to contribute to next month's newsletter? Submit an article, tip, or student spotlight by April 1. All authors will be credited by name.

[CONFIRM: Submission email]

APRIL 2026

Password Hygiene & Credential Theft

Deep dive into password managers, passkeys, and what happens when credentials end up for sale on the dark web. Plus: how to check if you've been breached.

MAY 2026

Social Engineering & Human Hacking

Why hackers target people, not just computers. Real examples of vishing (voice phishing), pretexting, and how to build a culture of healthy skepticism without becoming paranoid.

JUNE 2026

Summer Travel & Public Wi-Fi Safety

Traveling for summer? Your devices are at risk on airport and hotel Wi-Fi. Learn how VPNs work, what to avoid on public networks, and how to secure your phone while abroad.

OCTOBER 2026

Cybersecurity Awareness Month — Special Edition

A full special issue aligned with National Cybersecurity Awareness Month. Campus events, workshops, guest speakers, and a community-wide security challenge.

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

We welcome articles, tips, spotlights, and event announcements from all community members. Submissions for each issue are due the 1st of the preceding month.

Send to: [CONFIRM: Submission email]

ABOUT THIS NEWSLETTER

The CyberShield Bulletin is published monthly by the Cecil College Computer Science – Cybersecurity Club. It is a student-produced publication intended for educational purposes only.

For campus IT security emergencies, contact: [CONFIRM: IT Department contact]

