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

VOL. 1 — ISSUE 3
MAY 2026
SOCIAL ENGINEERING EDITION

// MONTHLY CYBERSECURITY AWARENESS

CyberShield BULLETIN

⚡ SECURE YOUR WORLD — ONE CLICK AT A TIME

EDITOR'S WELCOME

FROM THE CLUB PRESIDENT & FACULTY ADVISORS

Welcome to **Volume 1, Issue 3** of the CyberShield Bulletin — and what a semester it has been! After covering AI-powered phishing in March and credential theft in April, we close out the spring semester with what many security professionals consider the most dangerous threat of all: **social engineering**.

Social engineering is the art of manipulating people into giving up confidential information or taking actions that compromise security. Unlike technical hacking, it targets something no firewall can patch — **human nature itself**. Curiosity, trust, urgency, and helpfulness are all traits attackers exploit. This month, we arm you with the knowledge to recognize and resist these manipulations.

We also have a few exciting club updates — including a recap of our spring guest speaker event and a reminder about summer opportunities in cybersecurity. On behalf of our entire club, thank you for reading, sharing, and staying secure. Enjoy your summer and we will see you in September!

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

⚠ THREAT SPOTLIGHT

// MAY 2026 FEATURED THREAT

Social Engineering: When the Hacker Is the Person on the Phone

☠ **Risk Level: CRITICAL** — Social engineering is responsible for over 90% of successful cyberattacks. No amount of technical security can fully compensate for a person who has been manipulated into handing over access.

What Is Social Engineering?

Social engineering is any psychological manipulation that tricks people into revealing confidential information, transferring money, or granting access to systems. The attacker does not need to break through a firewall — they simply convince a human to open the door for them.

Think of it as the cybercriminal's version of a con artist. They study their target, craft a believable story, and use your own instincts — your desire to be helpful, your fear of consequences, your trust in authority — against you. The attack is not on your computer. **It is on your mind.**

The Most Common Social Engineering Attacks

🎣 Phishing (Email)

Fraudulent emails impersonating trusted entities — banks, colleges, government agencies — designed to steal credentials or install malware. We covered AI-powered phishing in our March issue. It remains the #1 delivery method for social engineering.

📞 Vishing (Voice Phishing)

Attackers call you by phone, pretending to be IT support, your bank's fraud department, the IRS, or even a campus administrator. AI voice cloning now allows them to sound exactly like someone you know. In 2025, a Maryland company lost $240,000 when an employee received a call that sounded exactly like their CEO.

💬 Smishing (SMS Phishing)

Text messages claiming your package is delayed, your account is locked, or you have won a prize — with a link to a fake site designed to harvest your login or payment information. These are increasingly personalized using data from previous breaches.

🎭 Pretexting

The attacker invents a fabricated scenario (a "pretext") to extract information. Example: someone calls the Financial Aid office claiming to be an IT auditor who needs the student database password to run a security check. The story is entirely invented — but plausible enough to work.

🎁 Baiting

Leaving a USB drive labeled "Payroll Q1 2026 — Confidential" in a campus parking lot or hallway. Human curiosity is powerful — studies show that 45–98% of people who find an unlabeled USB drive will plug it in. That drive often contains malware.

A Real-World Scenario

// REAL-WORLD EXAMPLE

A student receives a text: "*Cecil College IT: Your account will be suspended in 24 hours due to suspicious activity. Verify your identity here: [link].*" The link goes to a convincing fake portal that captures their username and password. The attacker now has access to the student's email, financial aid portal, and any other accounts where that password is reused. The entire attack took under 3 minutes and required zero technical skill.

How to Protect Yourself

Slow down. Social engineering attacks almost always create artificial urgency — "Act now or your account will be closed." This urgency is intentional. It bypasses rational thinking. When you feel pressured, that is the moment to pause and verify.

Verify independently. Never use contact information provided in a suspicious message. If your "bank" calls you, hang up and call the number on the back of your card. If "IT support" emails you, forward it to the real IT department directly.

Healthy skepticism is not paranoia. It is perfectly acceptable — even expected — to tell a caller "I'll need to verify this through official channels before proceeding." Legitimate organizations will never pressure you to bypass security procedures.

`// RED FLAGS — STOP AND VERIFY IF YOU SEE THESE`

- Urgent demands with threats of immediate consequences ("your account will be locked")
- Requests for passwords, PINs, or MFA codes — **no legitimate organization will ever ask for these**
- Pressure to keep a request secret or bypass normal procedures
- Unexpected contact from someone claiming to be in authority
- Offers that seem too good to be true (free gifts, prize winnings, job offers)
- Phone numbers, email addresses, or links that are almost-but-not-quite correct

TIP OF THE MONTH

Build a Personal Verification Protocol

> *The best defense against social engineering is a simple habit: pause, question, and verify through an independent channel before acting on any unexpected request.*

STOP → THINK → VERIFY

Apply this to every unexpected request for information, money, or access — regardless of who appears to be asking.

Your Personal 3-Step Verification Protocol

1. **STOP.** Do not click, call back, or comply immediately. Urgency is the attacker's most powerful tool. Giving yourself even 60 seconds breaks their psychological pressure.
2. **QUESTION.** Ask yourself: Did I initiate this contact? Was I expecting this request? Does this make sense coming from this person or organization? Is there unusual urgency or secrecy involved?
3. **VERIFY.** Use a contact method you already know and trust — not one provided in the suspicious message. Call the official number. Visit the official website by typing the URL directly. Ask a colleague or supervisor if in doubt.

Practice scenario: You get an email from "President@CecilCollege.edu" asking you to urgently purchase $500 in gift cards for a staff appreciation event and email the codes. What do you do? **STOP.** This is one of the most common CEO fraud / gift card scams — affecting organizations of all sizes. Call the college directly using the official number to confirm before doing anything.

Bonus: How to Report Suspicious Contact at Cecil College

If you receive a suspicious email, text, or phone call claiming to be from Cecil College, forward it to `[CONFIRM: IT Department email]` immediately. Your report could protect every other student and staff member who receives the same message.

🎓 CAREER CORNER

Summer Cybersecurity Opportunities — Don't Let Break Go to Waste

Summer is the single best time to build your cybersecurity résumé and skills. Here are concrete opportunities available right now to Cecil College students.

Free Online Learning Platforms

TryHackMe | **Hack The Box** | **SANS Cyber Aces** | **Coursera / Google**

TryHackMe.com offers guided, beginner-friendly rooms covering everything from Linux basics to web exploitation. Their free tier is substantial. Complete the "Pre-Security" and "SOC Level 1" paths over the summer and you will have real, demonstrable skills for your résumé.

Federal Internship Programs

The **NSA Pathways Internship**, **DHS Cybersecurity Internship Program**, and **CISA's CCEP** (Cybersecurity and Infrastructure Security Agency College program) all accept community college students. Most applications open in August–September for spring/summer placements. Ask Dr. Morgan or Professor Wilson for guidance on applications.

Cecil College CAE-CD Advantage

Cecil College is a **NSA/DHS Center of Academic Excellence in Cyber Defense (CAE-CD)** designated institution. This designation makes our students **highly competitive** for federal internships and scholarships that specifically target CAE-CD school graduates. Mention this in every application.

> **Scholarship alert:** The **CyberCorps® Scholarship for Service (SFS)** pays full tuition plus a stipend in exchange for federal service after graduation. Cecil College students are eligible. Applications typically open in the fall. `[CLUB TO CONFIRM: Club email for more info]`

📊 DID YOU KNOW?

98%

Of cyberattacks rely on social engineering at some stage of the attack

SOURCE: Positive Technologies, 2025

$2.9B

Lost to Business Email Compromise (BEC) — a form of CEO fraud — in 2025 alone

SOURCE: FBI IC3 Report, 2025

82 sec

Average time before the first victim clicks a link in a phishing campaign

SOURCE: Verizon DBIR, 2025

45%

Of people will plug in an unknown USB drive they find — rising to 98% when labeled with something enticing

SOURCE: University of Illinois Study

RESOURCES

Social Engineering Defense Tools

SANS Security Awareness
sans.org/security-awareness

Free posters, tip sheets, and training modules for recognizing social engineering. Ideal for sharing with family and coworkers.

Social Engineer.org
social-engineer.org

The definitive resource on social engineering — frameworks, podcasts, and free educational content from industry leaders.

PhishTank
phishtank.org

Community-verified database of known phishing URLs. Check any suspicious link before clicking — or submit one you found.

Google Safe Browsing
transparencyreport.google.com/safe-browsing/search

Check whether a URL has been flagged as dangerous by Google's Safe Browsing service. Free and instant.

FBI — How to Protect Yourself
fbi.gov/scams-and-safety

Official FBI guidance on current scams, fraud, and social engineering schemes targeting individuals and organizations.

UPCOMING

Dates to Watch

MAY TBD — **Guest Speaker Event**
Social Engineering in the Real World — Industry Professional
[CONFIRM: Date/Time/Room]

MAY TBD — **End-of-Year Club Meeting**
Year in review, officer elections, summer plans
[CONFIRM: Date/Time/Room]

JUN — **June Newsletter Deadline**

1 Submit summer travel & Wi-Fi safety tips

SEP 2026 **Club Resumes — Fall Semester**
New members welcome! Watch for the kickoff meeting announcement.

OCT 2026 **National Cybersecurity Awareness Month**
Special edition newsletter + major campus events planned!

🛡 QUICK REFERENCE

When Someone Asks for Access or Info…

✓ VERIFY FIRST

Use a trusted, independent contact method — not one provided in the suspicious message

✓ IT'S OK TO SAY NO

"I need to verify this before proceeding" is always an appropriate response

✓ REPORT IT

Forward suspicious emails to IT. Your report protects the whole community

⊘ NEVER SHARE

Passwords, MFA codes, SSNs, or banking info — with *anyone* over phone, email, or text

🏛 CLUB CORNER

Spring Semester Recap — What a Year!

As the spring semester wraps up, the Cecil College CS-Cybersecurity Club looks back on a remarkable inaugural year for the CyberShield Bulletin and an action-packed season of club activities.

Highlights from Spring 2026

🥈 **2nd Place** at the UMBC Maryland Cyber Cup Community College Division — competing against 29 teams in a daylong virtual CTF competition (full recap in our April issue).

📰 **3 issues** of the CyberShield Bulletin published — covering AI phishing, credential theft, and social engineering — reaching the entire Cecil College community.

🎤 **Guest speaker series** bringing industry professionals to campus to discuss real-world cybersecurity challenges and career paths.

Want to be more involved next year? Officer elections are coming up — contact the club if you're interested in a leadership role for Fall 2026.

`[CLUB TO CONFIRM: Club meeting/election details and 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**

See you in the fall! The CyberShield Bulletin will return in September 2026 with our Back-to-Campus security edition. Have a safe and secure summer!

[CONFIRM: Club email for summer contact]

COMING UP: FALL 2026 PREVIEW

JUNE 2026

Summer Travel & Public Wi-Fi Safety

VPNs, airport Wi-Fi risks, securing your phone abroad, and what to do if your device is lost or stolen while traveling.

SEPTEMBER 2026

Back to Campus: Securing Your Devices

Fall semester security checklist — laptops, smartphones, cloud accounts, and safe use of campus networks.

OCTOBER 2026

Cybersecurity Awareness Month — Special Edition

A full special issue for National Cybersecurity Awareness Month. Major campus events, workshops, guest speakers, and a community-wide challenge.

NOVEMBER 2026

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.

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]
