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

VOL. 1 — ISSUE 2
APRIL 2026
PASSWORD HYGIENE EDITION

// MONTHLY CYBERSECURITY AWARENESS

CyberShield BULLETIN

⚡ SECURE YOUR WORLD — ONE CLICK AT A TIME

EDITOR'S WELCOME

FROM THE CLUB PRESIDENT & FACULTY ADVISORS

Welcome back to the **CyberShield Bulletin** — Volume 1, Issue 2! Thank you to everyone who read our inaugural March edition. The response from our Cecil College community has been truly encouraging, and we are committed to bringing you timely, practical cybersecurity guidance every month.

This April, we are diving deep into one of the most widespread and preventable security vulnerabilities in existence: **weak and reused passwords**. Whether your password is "password123," your pet's name, or your birthday — this issue is for you. We will walk through what credential theft looks like, how the dark web marketplace for stolen logins works, and most importantly, exactly how to protect yourself starting today.

We also spotlight an exciting upcoming event — our **Spring Capture the Flag (CTF) Competition**. Whether you are a seasoned hacker or have never written a line of code, we want you there. See the Club Corner for details.

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

⚠ THREAT SPOTLIGHT

// APRIL 2026 FEATURED THREAT

Credential Theft & the Dark Web Marketplace for Your Passwords

Risk Level: HIGH — Over 24 billion username and password combinations are currently circulating on dark web marketplaces. Your credentials from a breach years ago may still be actively sold today.

What Is Credential Theft?

Credential theft is exactly what it sounds like: attackers steal your usernames and passwords. This can happen through phishing emails (as we covered in March), malware that records your keystrokes, or — most commonly — through **data breaches** at companies you have accounts with. When a company's database is hacked, millions of user credentials are often exposed at once.

Here is the critical part most people miss: **you may not even know your credentials were stolen.** Companies are sometimes slow to disclose breaches, and attackers frequently sit on stolen data for months before using or selling it.

The Dark Web Marketplace

> // HOW IT WORKS
>
> The dark web is a hidden part of the internet not accessible through standard browsers. Within it, cybercriminals operate marketplaces — similar in function to eBay or Amazon — where stolen credentials are bought and sold for as little as a few dollars per account. Email and password combinations are bundled into massive lists called **"combo lists"** and traded in bulk. A single combo list may contain hundreds of millions of entries.

The Password Reuse Problem

This is where it gets dangerous for most people. When attackers buy a combo list, they use automated tools to test those stolen username/password pairs against hundreds of websites simultaneously — a technique called **credential stuffing**. If you use the same password on your email, your bank, and your Cecil College portal, a breach at one site becomes a breach at all of them.

```
// Password Strength Examples

"password123"
⚠ Weak — cracked in under 1 second

"Cecil2017!"
⚡ Moderate — cracked in hours to days

"BlueSky#River$Lamp42!"
✅ Strong — billions of years to crack
```

How to Protect Yourself

Use a unique, strong password for every account. Yes, every single one. We know this sounds overwhelming — that is exactly why password managers exist (see our Tip of the Month). A strong password is long (16+ characters), random, and uses a mix of letters, numbers, and symbols.

Check if you have been breached. Visit **haveibeenpwned.com** right now and enter your email address. The site will tell you which known data breaches your email appeared in — for free, instantly, and safely.

Change passwords after any breach. If a service you use notifies you of a breach — or if Have I Been Pwned shows a hit — change that password immediately on that site, and on any other site where you used the same password.

💡 TIP OF THE MONTH

Start Using a Password Manager Today

You cannot realistically remember 50 unique, strong passwords — and you should not have to. A password manager does it for you, and it takes less than 10 minutes to set up.

🔑 People with password managers are 3x less likely to experience account takeover.

— Security.org Password Manager Report, 2025

What Is a Password Manager?

A password manager is an app that securely stores all your passwords in an encrypted vault, protected by one single **master password** that only you know. It can also generate strong random passwords for you automatically when you create new accounts or update old ones.

Our Recommendation: Bitwarden (Free)

Bitwarden is free, open-source, and independently audited for security. It works on every device and browser. Here is how to get started:

1. Go to **bitwarden.com** and create a free account using your email.
2. Create a strong, memorable **master password** — this is the only one you will need to remember. Try a passphrase: four random words strung together, like "BlueLampRiverSky." Write it down and store it somewhere physically safe.
3. Install the **browser extension** (Chrome, Firefox, Edge, Safari) so Bitwarden can auto-fill passwords on websites.
4. Download the **mobile app** on your phone for access anywhere.
5. Start adding your accounts. When you visit a site and log in, Bitwarden will offer to save the credentials. Over time, your vault fills itself naturally.
6. Use Bitwarden's built-in **password generator** to update weak or reused passwords — prioritize your email, bank, and college accounts first.

Other solid options: 1Password (paid, excellent for families), Dashlane (free tier available), and Apple Keychain (built into iPhones/Macs). Any of these is dramatically better than reusing passwords or storing them in a notes app.

🎓 CAREER CORNER

Spotlight Role: Identity & Access Management (IAM) Analyst

Last month we introduced CompTIA Security+. This month, let us spotlight one of the most in-demand entry-to-mid-level roles in the field — directly connected to our April theme of passwords and credentials.

What Does an IAM Analyst Do?

An **Identity and Access Management (IAM) Analyst** is responsible for ensuring that the right people have access to the right systems — and that nobody else does. This includes managing user accounts, enforcing password policies, implementing Multi-Factor Authentication (MFA), and investigating unauthorized access attempts. Every organization with more than a handful of employees needs IAM professionals.

Relevant Certifications

CompTIA Security+ | SSCP (ISC²) | SC-300 (Microsoft) | SailPoint IdentityNow

Average Salary: $75,000–$110,000 nationally for entry/mid-level roles. Maryland and the DC metro area offer some of the highest IAM salaries in the country, given proximity to federal agencies and contractors.

How to Get Started: Practice with free tools like Microsoft Entra ID (formerly Azure AD) through Microsoft's free developer tenant program. Document your hands-on experience for your resume and LinkedIn. Join the club — we can help you build a portfolio.

DID YOU KNOW?

24B

Username & password combinations exposed on the dark web

SOURCE: Digital Shadows, 2025

81%

Of confirmed data breaches involved weak, stolen, or reused passwords

SOURCE: Verizon DBIR, 2025

$4.45M

Average global cost of a data breach — credential theft is the #1 root cause

SOURCE: IBM Security Report, 2025

65%

Of people reuse passwords across multiple sites, including banking and email

SOURCE: Google/Harris Poll Survey

RESOURCES

Password & Credential Tools

Have I Been Pwned?
haveibeenpwned.com
Check instantly if your email appears in known data breaches. Free and trusted by security professionals worldwide.

Bitwarden
bitwarden.com
Free, open-source password manager. Generate strong passwords and store them securely across all your devices.

Password Monitor (Edge)
microsoft.com/edge

Built into Microsoft Edge — automatically alerts you if saved passwords appear in breaches.

NIST Password Guidelines

pages.nist.gov/800-63-4

The official federal standard for password security. Surprisingly readable and very relevant for all users.

Kaspersky Password Checker

password.kaspersky.com

Test the strength of a sample password and see how long it would take to crack. Eye-opening!

UPCOMING

Dates to Watch

APR 5 — **Club Meeting**
Spring CTF Team Formation
[CONFIRM: Time/Room]

APR 19 — **Spring CTF Competition**
All skill levels welcome — prizes awarded!
[CONFIRM: Details/Location]

MAY 1 — **May Newsletter Deadline**
Submit articles & tips to the club email

MAY TBD — **Guest Speaker Event**
Industry professional — topic: Social Engineering
[CONFIRM DETAILS]

OCT 2026 — **National Cybersecurity Awareness Month**
Special issue + campus-wide events!

CLUB CORNER

Spring CTF Competition — Join the Challenge!

Capture the Flag (CTF) competitions are one of the best ways to build real cybersecurity skills. Participants solve a series of security-related puzzles and challenges — cracking codes, finding hidden data, exploiting intentionally vulnerable systems — to capture digital "flags" worth points.

Our Spring CTF is open to **all Cecil College students regardless of experience level**. Beginners are encouraged to participate — we will offer a pre-competition workshop to get you started. Past participants have used their CTF experience as portfolio material for internships and job applications.

How to Join

Attend our April 5th club meeting to form teams and get the details. Solo participants are also welcome — we will help match you with a team.

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

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

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**

Contribute to the May issue! Submit articles, tips, or a student spotlight by May 1. Topic: Social Engineering & Human Hacking. [CONFIRM: Submission email]

📅 COMING UP: EDITORIAL CALENDAR PREVIEW

MAY 2026

Social Engineering & Human Hacking

Why hackers target people, not just computers. Real examples of vishing, pretexting, and how to build healthy skepticism without becoming paranoid.

JUNE 2026

Summer Travel & Public Wi-Fi Safety

Traveling for summer? Your devices are at risk. Learn how VPNs work, what to avoid on public networks, and how to secure your phone while away.

SEPTEMBER 2026

Back to Campus: Securing Your Devices

A fall semester checklist for students and faculty — securing laptops, smartphones, cloud accounts, and campus network connections before the semester ramps up.

OCTOBER 2026

Cybersecurity Awareness Month — Special Edition

A full special issue for 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]
