CECIL COLLEGE — CS & CYBERSECURITY CLUB
NCAE-CD DESIGNATED INSTITUTION
VOL. 2 — ISSUE 5
NOVEMBER 2026 / HOLIDAY SECURITY EDITION

// HOLIDAY SCAM SEASON · SHOP SAFE · STAY ALERT

CyberShield

BULLETIN · CECIL COLLEGE

🛒 PROTECT YOURSELF THIS HOLIDAY SEASON

$10B+
HOLIDAY ONLINE SHOPPING 2026

34%
PHISHING EMAILS SPIKE NOV-DEC

#1
HOLIDAY SCAM: FAKE SHOPPING SITES

72hrs
AVG. TIME TO ACT AFTER CARD FRAUD

// A MESSAGE FROM YOUR FACULTY ADVISORS

November arrives with cooler weather, grateful hearts — and unfortunately, a sharp rise in cybercrime. The holiday shopping season is **the most dangerous time of year for online consumers.** Scammers know that people are busy, distracted, and eager to find deals. They exploit every moment of it.

This issue of the CyberShield Bulletin is your holiday security survival guide. We're covering the top scams targeting shoppers, families, and travelers in November and December — and exactly what to do to stay safe.

We also have two important pieces of club news to share: first, a look back at a truly remarkable October — our NCSAM Special Edition month — and second, a very exciting announcement about new club leadership. Read on.

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

// CLUB LEADERSHIP ANNOUNCEMENT

Welcome, Lincoln Nguyen

NEW PRESIDENT — CECIL COLLEGE CS–CYBERSECURITY CLUB

We are thrilled to announce that **Lincoln Nguyen** has been elected as the new President of the Cecil College Computer Science–Cybersecurity Club. Lincoln's election represents an exciting new chapter for our club as we continue to grow our presence on campus and in the community.

Lincoln brings energy, fresh ideas, and a genuine passion for cybersecurity education to the role. Faculty Advisors Dr. James Morgan and Professor Jacqueline Wilson could not be more pleased with the membership's choice.

> // PASSING THE TORCH
>
> Our club was founded in 2017 under the visionary leadership of Elijah Smith, who guided us through eight issues of the CyberShield Bulletin and built the community we're so proud of today. Elijah's legacy lives in every event we host and every reader we reach. Lincoln Nguyen now carries that torch forward — and the future looks bright.

Congratulations, Lincoln! The entire Cecil College community is behind you.

NCSAM RECAP

October Wrap-Up: A Month to Remember

Cybersecurity Awareness Month 2026 at Cecil College was our most active month yet. Under the "Secure Our World" banner, our club ran four themed weeks that reached students, staff, and community members across campus. Here's what we accomplished together:

WEEK 1 · PASSWORDS

Password Manager Workshop — dozens of attendees secured accounts and moved to passphrases. Real accounts audited against breach databases on the spot.

WEEK 2 · PHISHING

Phishing Simulation Lab drew strong attendance. Live email dissection, a click-rate competition, and hands-on reporting practice. Cecil's IT team partnered with us.

WEEK 3 · DEVICES

Device Security Drop-In: full-disk encryption checks, update audits, app permission reviews, and VPN

configuration — all in one session. Dozens of devices secured.

WEEK 4 · CAREERS

Cyber Career Panel brought alumni, a defense-sector recruiter, and a CISA outreach specialist to campus. Community Challenge certificates awarded at close.

// COMMUNITY CHALLENGE RESULTS

The first annual Cecil College Community Cybersecurity Challenge closed October 31. Dozens of participants across students, faculty, staff, and community members completed all four actions. **Certificates will be issued at the November club meeting.** Thank you to everyone who participated — and especially to those who taught a family member or neighbor a security skill this month.

// HOLIDAY SECURITY ALERT · NOV–DEC 2026

The Season of Giving — and Scamming

The stretch from Thanksgiving through New Year's is the most profitable quarter for online retailers — and for cybercriminals. Fake storefronts, charity fraud, package delivery phishing, and gift card drains surge every November. Here is what's hitting consumers hardest in 2026, and how to fight back.

FAKE SHOPPING SITES | CHARITY FRAUD | DELIVERY PHISHING | GIFT CARD SCAMS

SHOP SAFELY | VERIFY BEFORE YOU BUY | TRUST YOUR GUT

TOP HOLIDAY SCAMS

The 2026 Holiday Threat Landscape

Every year attackers refine their playbook. These are the highest-volume scams active in November and December 2026:

🛍

// THREAT #1

Fake Online Storefronts

Scammers spin up convincing clone websites mimicking real retailers — complete with stolen logos, product images, and fake reviews. You pay, they vanish. Red flags: prices too good to be true, no physical address, newly registered domain, checkout-only accepting gift cards or wire transfer.

🎁

// THREAT #2

Package Delivery Phishing

Fake texts and emails impersonating UPS, FedEx, USPS, or Amazon claim your package is held, needs a fee, or has an address problem. The link goes to a credential-harvesting page or installs malware. Rule: **never click** — go directly to the carrier's official site and enter your tracking number there.

🎁

// THREAT #3

Gift Card Drains & Scams

Physical gift cards are tampered with in stores (barcodes replaced). Online scams ask victims to "pay fees" or "unlock prizes" with gift card numbers. If anyone — a government agency, tech support caller, or online seller — demands payment in gift cards, it is 100% a scam. Full stop.

🎗

// THREAT #4

Charity & Disaster Fraud

Fake charities proliferate in November (Giving Tuesday, Thanksgiving) and after natural disasters. They often use names nearly identical to legitimate organizations. Before donating: verify on **Charity Navigator** (charitynavigator.org) or **GuideStar**. Give through the charity's official site — never a link in an email or social post.

✈

// THREAT #5

Holiday Travel Scams

Fake flight deals, hotel booking clones, and vacation rental fraud peak in November as people book Thanksgiving and Christmas trips. Book only through airlines' official sites, major OTAs (Expedia, Hotels.com), or properties you can independently verify. Use a credit card — not debit — for travel purchases.

👤

// THREAT #6

Social Media & Ad Scams

Paid social ads for too-good-to-be-true products from unknown brands have exploded. The product either never arrives or is a cheap imitation. Scammers run short-lived ad campaigns targeting holiday shoppers. Research unfamiliar brands with a "[brand name] scam" web search before purchasing. Check return policies before you buy.

SAFE SHOPPING GUIDE

SAFE SHOPPING GUIDE

Your Holiday Shopping Security Checklist

Print this. Save it to your phone. Share it with your family. These habits make the difference between a happy holiday and a very stressful January.

- **Check the URL.** Look for `https://` and the padlock icon — but remember, scam sites can have these too. Verify the full domain name matches the real store exactly (amazon.com vs. amazon-deals-nov.com).
- **Use a credit card, not debit.** Credit cards have stronger fraud protection and allow chargebacks. Debit card fraud comes directly out of your bank account and is harder to recover.
- **Never shop on public Wi-Fi without a VPN.** Coffee shops, airport lounges, and hotel networks are hunting grounds for attackers intercepting payment data. Use your phone's hotspot or a trusted VPN.
- **Verify sellers on marketplaces.** On Amazon, eBay, and similar platforms, check seller ratings, review dates (fake reviews cluster), and whether the seller ships from an unusual country for the product.
- **Monitor your accounts weekly.** Set up transaction alerts on all payment cards. November and December are the months to check your statements closely — catch fraud before the billing cycle closes.
- **Research charities before you donate.** Use Charity Navigator, BBB Wise Giving Alliance, or GiveWell. The name "American Cancer Support Fund" is not the American Cancer Society — scammers count on the confusion.
- **Be suspicious of "too good" deals.** If a site is selling a $400 item for $89 with no explanation, trust your instincts. Scarcity and urgency ("Only 2 left! Offer expires in 10:00") are manipulation tactics.
- **Use virtual card numbers.** Many banks and credit cards offer single-use virtual card numbers for online purchases. Use them — if the virtual number is stolen, your real card is safe.

> // IF SOMETHING GOES WRONG
>
> Act within 72 hours. Contact your bank or card issuer immediately to dispute fraudulent charges. File a report with the FTC at **ReportFraud.ftc.gov**. If your credentials were stolen, change your password and enable MFA on that account right now.

TIP OF THE MONTH

The Holiday Security Gift

Last month we asked you to have a "Kitchen Table Conversation" about cybersecurity with one person in your life. This month, we're asking you to give someone a **security**

gift that costs nothing.

Sit down with a parent, grandparent, or friend who shops online and walk them through just three things:

- **How to spot a fake website** — examine the URL, look for trust seals, search for "[store name] scam"
- **Why they should never pay with gift cards** — if anyone asks for gift card payment, hang up and call a family member
- **How to set up transaction alerts** — log into their bank's mobile app and enable push notifications for every purchase

> // THE IMPACT
>
> Older adults lost over $3.4 billion to fraud in 2023 (FBI IC3). The people in our lives who didn't grow up with digital commerce are the most vulnerable during the holidays. One conversation from you could save someone you love from a devastating loss.

CLUB CORNER

Nine Issues — and Just Getting Started

With this issue, the CyberShield Bulletin reaches its **ninth edition.** What began as a campus newsletter has grown into a publication that reaches students, faculty, staff, alumni, and community members across Cecil County.

Under incoming President Lincoln Nguyen's leadership, the club is planning an ambitious spring semester: new partnerships, expanded community outreach, and initiatives that connect our NCAE-CD designation to real opportunities for students interested in federal cybersecurity careers.

Watch club channels in late November for the spring 2027 event calendar. There is a lot to look forward to.

> // COMING UP
>
> **December 2026:** Year in Review — The Cybersecurity Moments That Defined 2026
> **December submissions due December 1, 2026.** Share your highlights, learnings, or a security resolution for 2027.

🚨 Holiday Scam Alerts

NEVER pay with gift cards. No legitimate business or government agency will ever demand gift card payment.

Don't click delivery texts. Go directly to UPS.com, FedEx.com, or USPS.com and enter your tracking number.

Verify charities independently. charitynavigator.org before you donate.

Too cheap = too risky. Research unknown brands before buying.

November Events

NOV 1 **December Submissions Open**
Year in Review — send your highlights

NOV TBA **NCSAM Certificate Ceremony**
Community Challenge certificates awarded

NOV TBA **Holiday Shopping Security Workshop**
Hands-on: safe online shopping practices

NOV TBA **Club Meeting**
Welcome President Lincoln Nguyen — new leadership, spring plans

NOV 27 **Thanksgiving / Black Friday**
Peak phishing season — stay alert

Safe Shopping Quick Ref

- 💳 Use credit card — not debit
- 🔒 HTTPS + verify the full domain
- 📶 VPN on public Wi-Fi
- 🔔 Enable transaction alerts now
- 🎁 Gift card demands = SCAM
- 🎗️ Verify charities at charitynavigator.org
- 🚩 Report fraud: ReportFraud.ftc.gov

Vol. 2 — Issue Tracker

✓ Done **July 2026** — Back to School

✓ Done **August 2026** — Fall Preparation

✓ Done **September 2026** — Cloud Account Takeover

✓ Done **October 2026** — NCSAM ☆ Special

► Now **November 2026** — Holiday Scams

Next **December 2026** — Year in Review

Club Leadership

President:
Lincoln Nguyen

Faculty Advisors:
Dr. James Morgan
Professor Jacqueline Wilson

Founded: 2017 by Elijah Smith

Designation: Cecil College NCAE-CD

Holiday Security Links

- ReportFraud.ftc.gov — Report scams
- CharityNavigator.org — Vet charities
- IC3.gov — FBI Internet Crime Complaint
- CISA Holiday Shopping Tips
- consumer.ftc.gov — Consumer advice

CyberShield Bulletin

Cecil College Computer Science–Cybersecurity Club | Founded 2017 | North East, Maryland

Faculty Advisors: Dr. James Morgan & Professor Jacqueline Wilson | President: Lincoln Nguyen

Vol. 2 — Issue 5 · Holiday Security Edition · November 2026

This newsletter is for educational purposes and community awareness. Links to external resources do not constitute endorsement by Cecil College. If you believe you have been a victim of fraud, contact your financial institution immediately and report to the FTC at ReportFraud.ftc.gov.