CyberNut

CYBERNUT WHITE PAPER

Securing K–12 Schools Through Human-Centric Cybersecurity Awareness

Issued Date
04.28.2025

Scan the QR code to
get a free phishing
assessment

CyberNut.com
Hello@CyberNut.com

TABLE OF CONTENTS

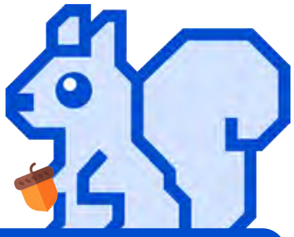
1. EXECUTIVE SUMMARY

PURPOSE

This white paper explores how the CyberNut platform delivers highly effective cybersecurity and phishing awareness training tailored for K–12 schools. It addresses the rising tide of cyber threats in education—from phishing scams to AI-driven attacks—and outlines how CyberNut's gamified, user-friendly approach significantly reduces click rates and bolsters real threat reporting.

CyberNut uniquely differentiates itself by not only serving as a compliance-driven security awareness training platform but also by empowering school district employees with an integrated real threat reporting solution. This proactive combination teaches users to identify, report, and mitigate real cybersecurity threats effectively, significantly enhancing overall district safety.

EXECUTIVE SUMMARY



Built for K–12: Advisory board of school CTOs/IT directors shaped CyberNut's design.

Adaptive, Micro-Trainings: 1-minute lessons integrated directly into users' email experience, ensuring better retention.

Gamification: Rewards (acorns), leaderboards, and friendly competition increase user engagement.

Actionable Security: The built-in reporting tool and dashboard allow IT teams to instantly remove malicious emails district-wide.

Easy Implementation: Quick setup and automated campaigns significantly reduce administrative burdens and IT workload.

Cost-Effective: Specifically designed to align with educational budget constraints, making robust cybersecurity accessible to schools of all sizes.

Student-Friendly Content: Age-appropriate phishing and cyber-threat modules available for middle and high school students, promoting district-wide cybersecurity literacy.

CYBERNUT IS TRUSTED BY OVER
100+ SCHOOL DISTRICTS

CyberNut.com | Hello@CyberNut.com

CyberNut

2. THE K-12 CYBERSECURITY CHALLENGE

Cyber threats in K–12 schools have rapidly escalated, reaching critical levels that directly threaten students, educators, and entire districts:

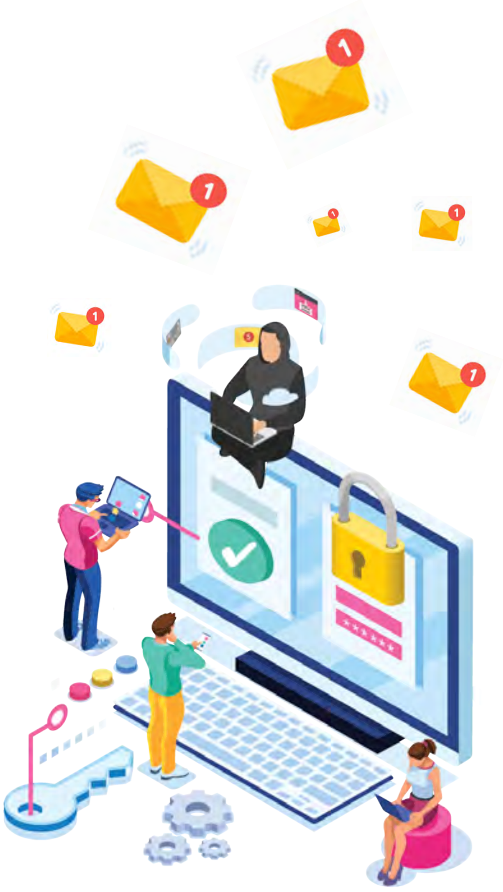
82% of K–12 districts reported experiencing direct impacts from cyber threats.

92% of data breaches are caused by phishing attacks.

Over 14,000 security events have taken, with 9,300 confirmed incidents disrupting school operations.

Cybercriminals exploit human errors 45% more often than technical vulnerabilities, specifically targeting staff and students.

Cyberattacks intensify during critical academic periods—such as exams—deliberately disrupting education, creating chaos, and forcing administrators into difficult, costly decisions.



The fallout from these attacks is severe. According to a 2022 U.S. Government Accountability Office report, cyberattacks have cost K–12 districts anywhere from $50,000 to $1 million per incident, with disruptions to education lasting from three days to three weeks of lost instructional time. Unsurprisingly, cybersecurity remains the top concern for school district technology leaders, according to CoSN, holding this troubling position consistently for over five years.

WHY K–12 IS UNIQUELY VULNERABLE:

Students, faculty, staff, and administrators share a common network; **a single click puts everyone at risk.**

Limited budgets often restrict schools from accessing advanced, effective cybersecurity solutions typically available to corporations, leaving districts especially vulnerable.

Current training solutions are **boring and made for the "corporate world"** leading to low teacher & staff engagement.

Traditional training methods that rely primarily on video-based content **fail to effectively engage participants and do not adequately equip** school administrators and teachers with the skills needed to protect themselves and their school in the event of a phishing attack.

Schools promptly need a cybersecurity solution that directly addresses the human vulnerabilities criminals rely on—training every person in the district to recognize and prevent attacks before they cause widespread damage.

> "CyberNut has transformed cybersecurity in our district. It significantly reduced phishing click rates while making awareness engaging for teachers. Instead of forwarding suspicious emails to IT, they report them via the 'little blue squirrel,' earning rewards and reinforcing safe practices. CyberNut's K-12 focus makes it a perfect long-term partner for our schools."

Dr. Scott Haselwood

CIO at Deer Creek Public Schools

Watch Full Testimonial Now!

3. INTRODUCING CYBERNUT

CyberNut

A security awareness training platform built exclusively for K-12 schools

CyberNut was designed in collaboration with school district CTOs and IT professionals. By serving only schools, we've developed a highly specialized training solution tailored specifically to the unique needs of the K-12 education sector.

CyberNut's automated campaigns train your school's **faculty**, **staff,** and **students** to recognize and report phishing emails and deep fake AI scams that are targeting your school district.

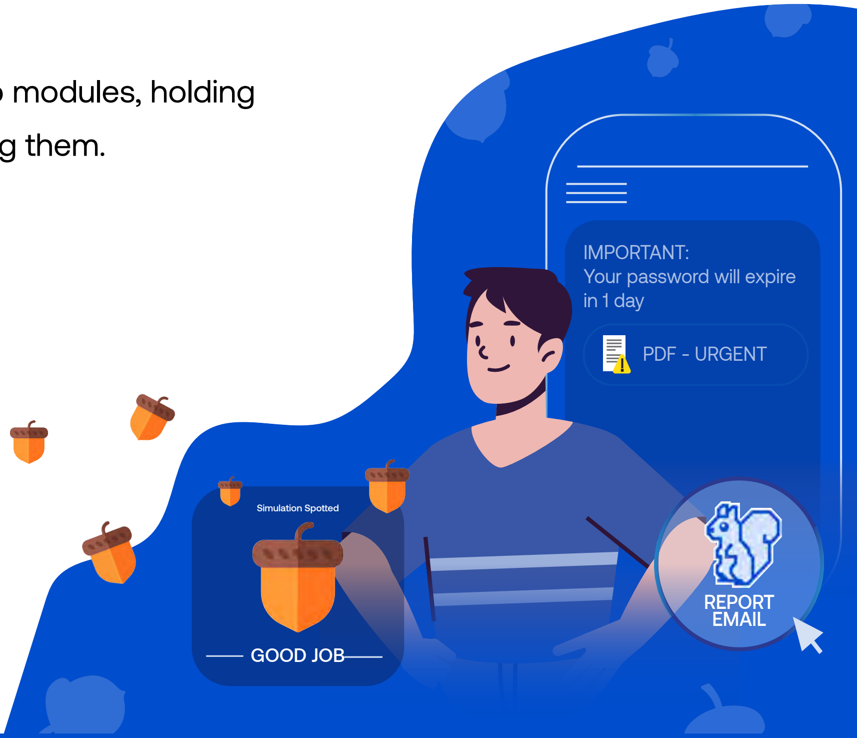
KEY DIFFERENTIATORS

Quick & Enjoyable

Micro-trainings replace lengthy video modules, holding users' attention without overwhelming them.

Real-World Impact

Users learn to spot—and immediately report—actual malicious threats, not just simulations.



Personalized Learning Journey

CyberNut uses adaptive learning to match each user’s skill level.
Phishing simulations and micro-trainings adjust automatically—starting simple, then increasing in difficulty as users improve. This builds confidence, reinforces learning, and keeps all staff—from teachers to support teams—engaged, regardless of their starting point.

LEVEL 1 Non-personalized emails with typos and bad branding

LEVEL 2 Personalized emails with typos and bad branding

LEVEL 3 Personalized emails with decent grammar & decent branding

LEVEL 4 Well-branded, personalized emails with proper grammar—often using spoofed senders and insider details to appear legitimate

LEVEL 5 AI-driven phishing emails hyper-personalized targeting

I conquered all the levels... think your district can too?

4. HOW DOES CYBERNUT WORK?

FREE TRIAL

PHASE 1

BASELINE CAMPAIGN

2 weeks

Free Phishing Test

- Helps determine your district's level of phishing vulnerability
- No plugin installed
- No gotcha emails
- Redirect to generic pages
- Goes undetected (no CyberNut branding)
- Can run in parallel to the current campaign

PHASE 2

ONBOARDING CAMPAIGN

Onboarding

- Short and simple educational initiative
- Aims to teach faculty, staff, and students how to use CyberNut
- Introduces users to the platform
- Guides users on how to report suspicious emails using the CyberNut plug-in
- Entire process takes under 2 minutes

PHASE 3

TRAINING CAMPAIGN

Training

- Training campaign runs on autopilot for the rest of the school year
- Personalized learning journey begins
- Plugin is deployed
- Leaderboard goes live
- Gamification goes live
- Threat reporting is activated
- Active threat monitor goes live

4.1 BASELINE CAMPAIGN

Baseline Campaign:
Free Phishing Vulnerability Assessment

What is the Goal?

The goal is to quickly and discreetly identify your district’s cybersecurity vulnerabilities.

CyberNut's baseline phishing assessment quickly and quietly measures your district's current cybersecurity risk—without disrupting school operations.

✓ **Quick & Invisible:**
A discreet two-week test sends realistic phishing emails to staff.

✓ **Zero Setup Required:**
No plugins, no CyberNut branding, no IT configuration, and absolutely no "gotcha" emails or alerting pages.

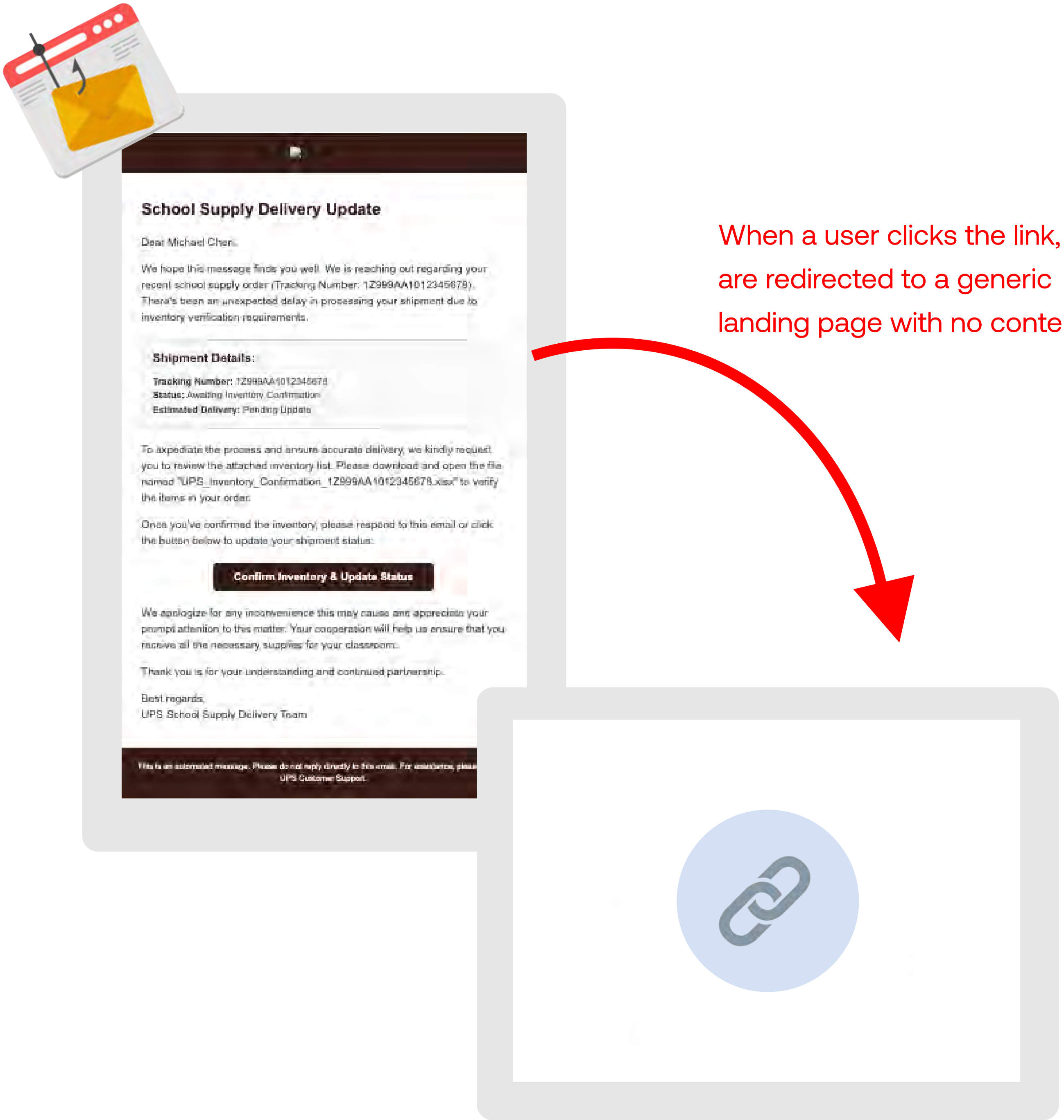
✓ **Actionable Results:**
Receive a clear, detailed report identifying your district’s phishing vulnerability—highlighting open rates, click rates, and top-clicked themes.

✓ **Budget-Friendly Evidence:**
Data-backed insights help justify cybersecurity training initiatives or budget expansions.

Empower your district by clearly understanding its vulnerabilities—effortlessly and confidentially.

Over ~2 weeks, each user receives two covert phishing emails.

Clicking reroutes to a generic “dead” page—no “gotcha” messaging or brand references.



School Supply Delivery Update

Dear Michael Chen,

We hope this message finds you well. We is reaching out regarding your recent school supply order (Tracking Number: 1Z999AA1012345678). There's been an unexpected delay in processing your shipment due to inventory verification requirements.

Shipment Details:

Tracking Number: 1Z999AA1012345678
Status: Awaiting Inventory Confirmation
Estimated Delivery: Pending Update

To expedite the process and ensure accurate delivery, we kindly request you to review the attached inventory list. Please download and open the file named "UPS_Inventory_Confirmation_1Z999AA1012345678.xlsx" to verify the items in your order.

Once you've confirmed the inventory, please respond to this email or click the button below to update your shipment status:

We apologize for any inconvenience this may cause and appreciate your prompt attention to this matter. Your cooperation will help us ensure that you receive all the necessary supplies for your classroom.

Thank you is for your understanding and continued partnership.

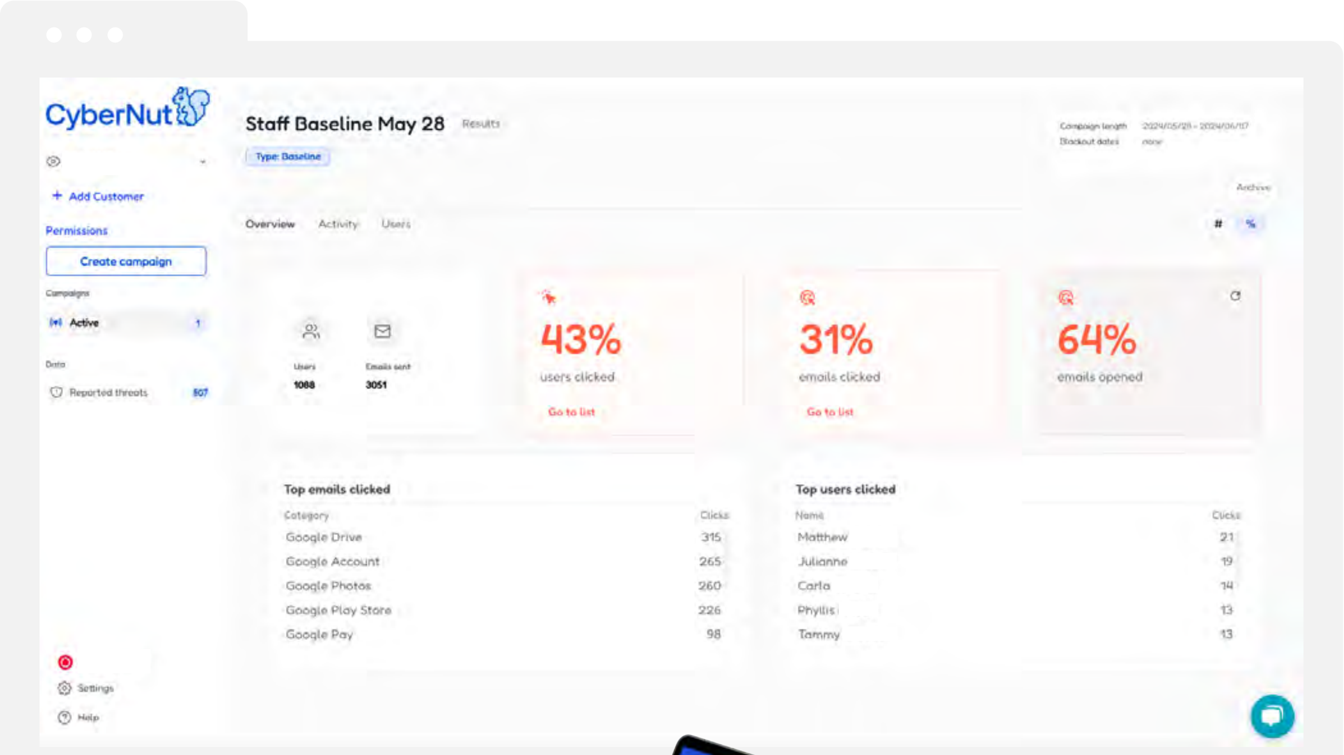
Best regards,
UPS School Supply Delivery Team

This is an automated message. Please do not reply directly to this email. For assistance, please
UPS Customer Support.

When a user clicks the link, they are redirected to a generic landing page with no content.

Review Your Baseline Data

- The district receives a confidential report showing open rates, click rates, and most-clicked email themes.
- Results justify budget or initiative expansions for cyber training.
- Easily export your data.



CyberNut

+ Add Customer

Permissions

Create campaign

Campaigns

Active 1

Data

Reported threats 507

Settings

Help

Staff Baseline May 28 Results

Type: Baseline

Campaign length 2024/05/28 – 2024/06/17
Blackout dates none

Archive

Overview Activity Users

# %

Users 1088

Emails sent 3051

43% users clicked — Go to list

31% emails clicked — Go to list

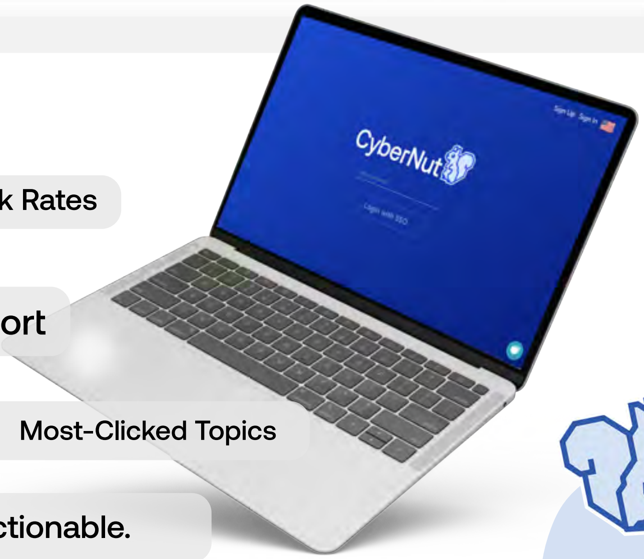
64% emails opened

Top emails clicked

Category	Clicks
Google Drive	315
Google Account	265
Google Photos	260
Google Play Store	226
Google Pay	98

Top users clicked

Name	Clicks
Matthew	21
Julianne	19
Carla	14
Phyllis	13
Tammy	13



- ✓ Click Rates
- ✓ Confidential Report
- ✓ Most-Clicked Topics
- ✓ Clear. Accurate. Actionable.

Interested in learning more?

Book a 15 min demo

HERE!

What You'll Learn From Your Baseline Data

CyberNut provides a clear snapshot of your district's phishing risk:

EMAIL ENGAGEMENT:

Quickly see how many users opened phishing emails, revealing the initial exposure level.

TOP THREATS:

Quickly see how many users opened phishing emails—and which threat types they were most vulnerable to, including top-clicked categories.

CLICK RATES:

Understand how many users clicked links, pinpointing your staff's vulnerability to real threats.

ACTIONABLE INSIGHTS:

Leverage concrete data to justify security initiatives, demonstrate compliance, and secure necessary funding.

> "I prefer CyberNut over KnowBe4 because it's built for K-12. Instead of long, 30-minute trainings, CyberNut offers short, gamified micro-trainings. With leaderboards and acorns, it turns security training from 'I have to do this' into 'Do I get to do this?'"

Joe Reed

Director of IT at Sacred Heart

Watch Full Testimonial Now!

4.2 ONBOARDING CAMPAIGN

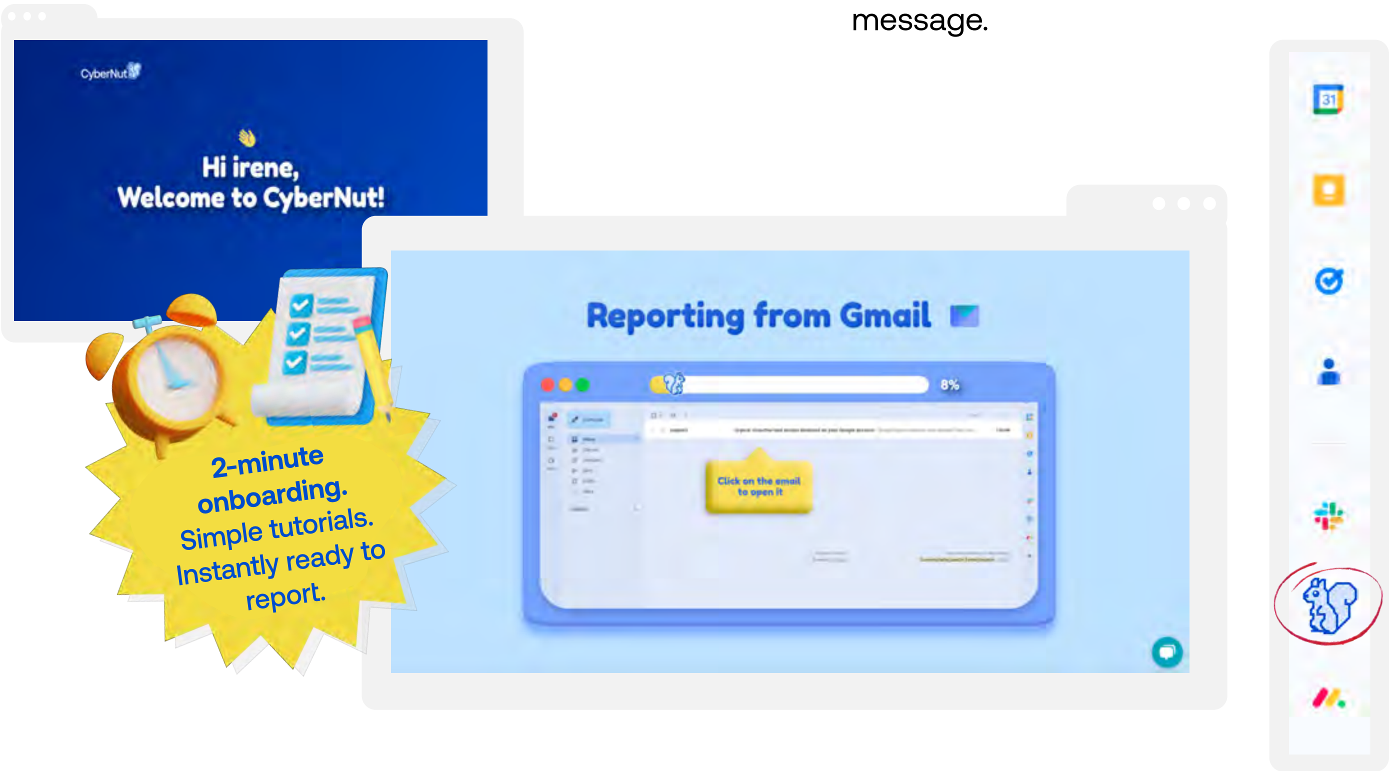
Once a district commits to full deployment, CyberNut launches a focused onboarding campaign—**designed to ensure all faculty, staff, and students quickly learn how to use the platform and report suspicious emails with confidence.**

1 FRIENDLY WELCOME EMAILS

- Explains the new CyberNut plug-in (Gmail or Outlook).
- Builds a positive tone—this is training, not a punitive "gotcha" program.

2 QUICK TUTORIALS

- Takes under 1 minute to show how to identify the "blue squirrel" plug-in and submit suspicious emails.
- Ensures staff know exactly what to do when they see a questionable message.


CyberNut

Hi irene,
Welcome to CyberNut!

Reporting from Gmail

2-minute onboarding. Simple tutorials. Instantly ready to report.
8%
Click on the email to open it
31

> "Rolling out CyberNut was refreshingly smooth. The setup was quick, the training was intuitive, and our staff felt confident using it right from the start."
>
> **Estill Frodge**
>
> Director of Technology at Mercy Academy

4.3 TRAINING CAMPAIGN

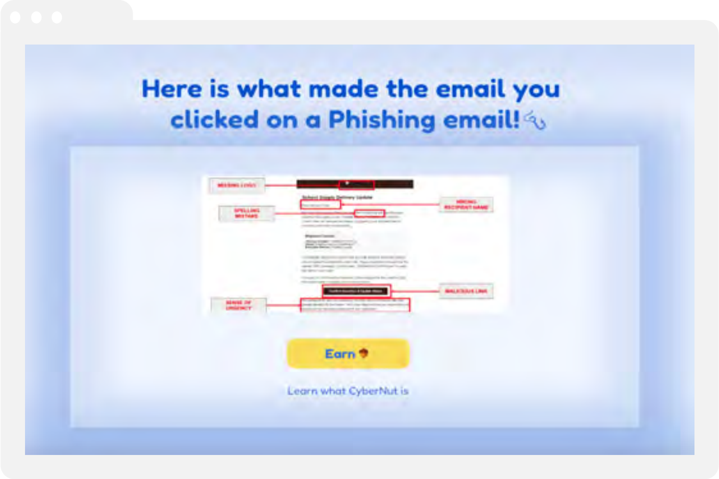
CyberNut's training campaign provides an ongoing learning experience for all enrolled faculty, staff, and students. Powered by CyberNut, the program runs automatically in the background—continuously delivering phishing simulations to help users sharpen their ability to identify and report suspicious emails. The goal is to build a strong, district-wide "human firewall" that can recognize and respond to real threats if and when a phishing attack occurs.

Report Using the Gmail or Outlook Plugin

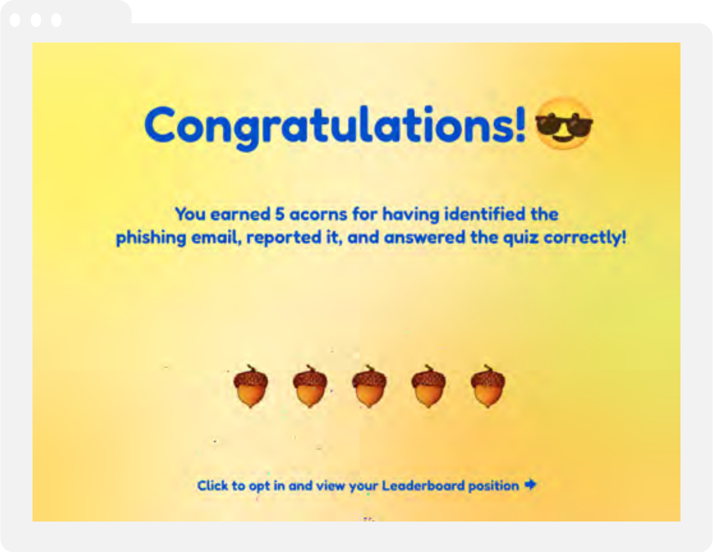
- Users enrolled in CyberNut training will report phishing simulations directly through the plug-in.
- Each user progresses through a personalized learning journey at their own pace, gaining skills and confidence along the way.

Micro-Training and Instant Feedback

- When a user reports a phishing email using the CyberNut plug-in, they're rewarded with acorns—our gamified reward system.
- If a user clicks on a phishing email, they receive a gentle, real-time prompt that provides instant feedback and explains exactly what went wrong—turning mistakes into learning moments.



Here is what made the email you clicked on a Phishing email!



Congratulations! 😎

You earned 5 acorns for having identified the phishing email, reported it, and answered the quiz correctly!

5. GAMIFICATION & ENGAGEMENT

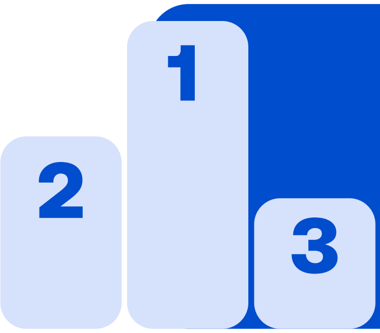
CyberNut is the only cybersecurity training solution that truly gets teachers and administrators excited and engaged in their mandatory phishing and cybersecurity training.

ACORNS & POINTS

Users earn “acorns” for correct reporting of suspicious emails — and get extra acorns when they answer quiz questions correctly!

POSITIVE REINFORCEMENT

- Encourages staff to stay alert, turning them into “cyber defenders” for the entire district.
- Helps foster a culture of security awareness.



LEADERBOARD

- Optionally group staff by building, department, or role for friendly competitions.
- Some districts offer small prizes (gift cards, school-branded swag) to top reporters.

One of our customers keeps the energy high by posting the leaderboard right in the teachers’ lounge!

One of our customers loves recognizing people with fun swag and giveaways.

6. CYBERNUT DELIVERS REAL THREAT REPORTING AND ACTIVE THREAT MANAGER

Beyond simulated training, CyberNut also streamlines actual threat response:

1

REAL THREAT REPORTING:

If a user suspects a real phishing email, they report it the same way they would a simulated one—by clicking the CyberNut Report button. With one click, IT is instantly notified, enabling a fast, coordinated response to real threats.

2

IT GETS INSTANTLY NOTIFIED:

When a faculty member, staff, or student reports a real threat, school IT admins are immediately alerted.

They can view the report in their dashboard, preview the suspicious email, and quickly assess the threat—all in one place.

3

TAKE IMMEDIATE ACTION ON REAL THREATS

When a real phishing email is reported through CyberNut, IT admins are instantly alerted. They can preview the threat in their dashboard and, with one click, delete it from every inbox and block the sender—providing fast, district-wide protection.

4

INSTANT USER FEEDBACK

The user who reported the threat receives instant positive feedback, reinforcing that they took the right action by spotting and reporting a real potential threat.

HOW THE ACTIVE THREAT MANAGER WORKS

Overview

The Active Threat Manager **empowers administrators to rapidly respond to user-reported threats, enhancing overall cybersecurity and reducing district-wide risk**. By streamlining the threat-handling process, schools achieve faster mitigation and stronger protection against malicious attacks.

Key Features

Comprehensive Threat Visibility
View all user-reported phishing emails in one centralized dashboard as soon as they're flagged.

Detailed Email Insights
Dive into full metadata—sender details, timestamps, and more—to accurately gauge each threat's severity.

Simplified Threat Management
Quickly dismiss harmless emails or delete malicious ones from all user inboxes with a single click.

Proactive Protection (Microsoft Users Only)
Block senders to prevent repeat phishing attempts, stopping threats before they reach your staff again.

Interested in learning more?

Book a 15 min demo

HERE!

> “In the past three months, we've reported over 600 potential threats through CyberNut. It's made identifying and removing real phishing emails fast and simple.”
>
> **Scott Roth**
> Director of Technology & CIO at Orchard Park

CYBERNUT COMPLIANCE TRAINING

Effortlessly Meet State and Cyber Insurance

CyberNut Compliance provides streamlined, DIR-certified cybersecurity training designed specifically for K–12 schools. With eight focused video training modules, our simple approach ensures your district meets all required state standards and insurance mandates—without overwhelming staff or disrupting learning.

Key Benefits of CyberNut Compliance

SIMPLE, VIDEO-BASED MODULES

Engaging, self-paced video training that faculty and staff can complete quickly—making compliance easy and accessible for all.

ALIGNED WITH STATE & INSURANCE REQUIREMENTS

Every module is built on the NIST framework and aligns with state cybersecurity mandates and cyber insurance policy standards, ensuring you're always audit-ready.

AUTOMATED TRACKING & REMINDERS

Real-time dashboards let you instantly see who's completed training, with automatic email reminders for anyone still pending.

EIGHT ESSENTIAL TOPICS

Covers all core areas of K–12 cybersecurity compliance in eight structured modules.

DIR-CERTIFIED & TRUSTED

CyberNut is a DIR-certified vendor, trusted by over 100 school districts to deliver effective, scalable compliance solutions.

Compliance Standards

2024-2025 STATE CERTIFIED
DIR
CYBERSECURITY TRAINING PROGRAM

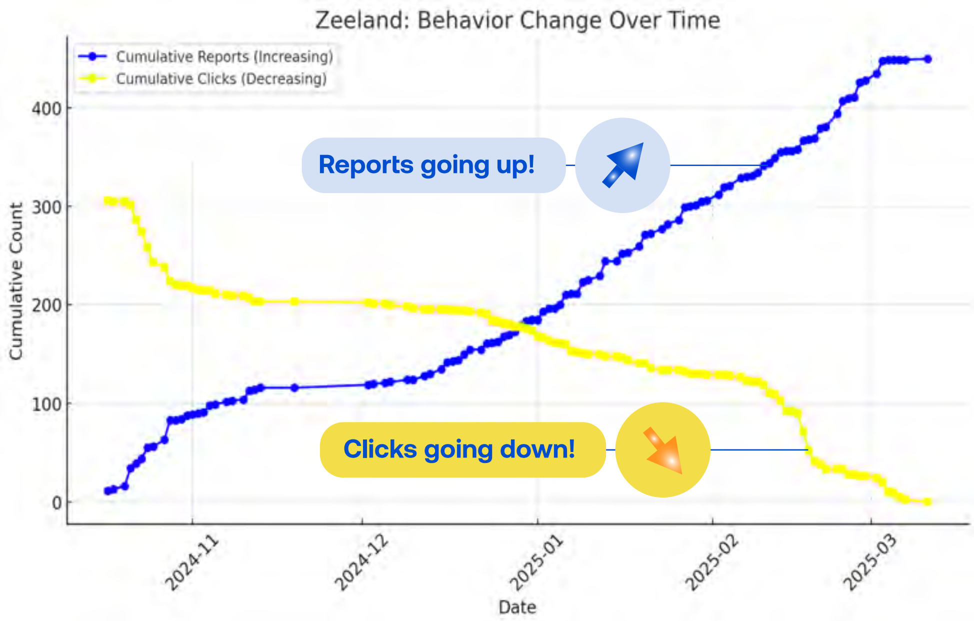
GDPR
READY

At CyberNut, we prioritize data security and privacy.

We are **DIR-certified** and compliant with **EU GDPR**, ensuring that schools and organizations meet the highest standards for protecting sensitive information.

Our policies are designed to safeguard user data, enhance transparency, and maintain compliance with industry regulations.

7. CYBERNUT DELIVERS REAL RESULTS & ROI



This graphic illustrates CyberNut's sustained impact over time, demonstrating a consistent increase in phishing reports alongside a steady decline in risky clicks.

These trends highlight the effectiveness of ongoing cybersecurity awareness and training in strengthening schools' security posture.

Click-Rate Reduction

Districts typically see a significant dip in phishing clicks within the first 2–3 months of training.

Threat Interception

Quicker elimination of real malicious emails across inboxes

Cyber Insurance & Compliance

- Having documented training and real-time threat reporting can help with insurance renewals.
- Meets or exceeds many K–12 data privacy and cybersecurity requirements.

8. CASE STUDY HIGHLIGHTS

CyberNut

Case Study:

CyberNut Implementation in K-12 Education

ORCHARD PARK

Orchard Park Central School District, like many K–12 schools, faced rising cyber threats—91% caused by human error, mostly phishing. With over 1,619 incidents reported nationwide, they turned to CyberNut for a tailored solution.

Results

After implementing CyberNut, Orchard Park observed significant improvements in their cybersecurity posture:

- **Increased Engagement:** Over 50% of faculty and staff actively participated in CyberNut training since the program's introduction.
- **Effective Behavioral Change:** 512 users reported at least one phishing simulation, totaling 4,499 reported phishing simulations since deployment.
- **Enhanced Threat Detection:** 463 real threats were reported by 242 unique users, substantially improving the district's cybersecurity posture.
- **Reduced Risk:** Individual users demonstrated remarkable progress, highlighted by success stories like Sarah, who shifted from initial vulnerability to consistent threat reporting after just one training interaction.

BEFORE CYBERNUT

Audience:
Faculty, Staff, & Administrators at Orchard Park

Results from a phishing audit conducted by an independent cybersecurity consulting firm.

Phishing Audit Date: May 28, 2024

Total # of participants: 1,088

TOTAL LINKS CLICKED: 618
TOTAL CLICK-THROUGH RATE (%): 31%

WITH CYBERNUT

After 10 months of CyberNut Training Orchard Conducted an additional independent phishing audit.

Phishing Audit Date: December 2, 2024

Total # of participants: 946

TOTAL LINKS CLICKED: 357
TOTAL CLICK-THROUGH RATE (%): 2%

In just 7 months, CyberNut reduced their phishing **click rate to 2%.**

ZEELAND PUBLIC SCHOOLS

Background

Mark Washington, the Director of Technology at Zeeland Public Schools (ZPS), has dedicated over 34 years to education technology. Like many school districts nationwide, ZPS faced an increasing challenge: a growing frequency of sophisticated phishing attacks.

Initially, ZPS relied on a generic phishing training solution provided through their cyber insurance company. Unfortunately, this resulted in consistently low engagement and minimal improvement. Recognizing the urgent need for change, Mark explored new options—and discovered CyberNut.

Results

After implementing CyberNut, Zeeland Public Schools observed significant improvements in their cybersecurity posture:

Increased Engagement: Teachers became more motivated to participate in the training, leading to higher reporting rates of suspicious emails.

Reduced Click Rates: The click rates on phishing emails dropped dramatically. For instance, the percentage of users clicking on links in phishing simulations decreased from 25% to just 2%.

Improved Reporting: The number of users reporting suspicious emails increased, providing the IT Department with valuable data to address potential threats.

Enhanced Security Awareness: Teachers became more vigilant and proactive in identifying and reporting phishing attempts, contributing to a safer digital environment.

BEFORE CYBERNUT

Audience:
Faculty, Staff, & Administrators at Zeeland Public Schools

Results from a phishing audit conducted by an independent cybersecurity consulting firm.

Phishing Audit Date: February 12, 2024

Total # of participants: 1,081

TOTAL LINKS CLICKED: 366
TOTAL CLICK-THROUGH RATE (%): 25%

WITH CYBERNUT

After 10 months of CyberNut Training Zeeland Conducted an additional independent phishing audit.

Phishing Audit Date: December 9, 2024

Total # of participants: 1,081

TOTAL LINKS CLICKED: 211
TOTAL CLICK-THROUGH RATE (%): 2%

In just 10 months, CyberNut reduced their phishing **click rate to 2%**.

CYBERNUT IS TRUSTED BY OVER
100+ SCHOOL DISTRICTS

CyberNut.com | Hello@CyberNut.com

CyberNut

READY TO LEARN MORE & START YOUR FREE TRIAL?

CyberNut empowers K–12 districts to tackle the human side of cybersecurity. By blending personalized phishing simulations, real threat reporting, and gamified learning, school communities actively defend themselves in an era of AI-driven threats.

Ready to Understand Your District's Cybersecurity Risk?

Sign Up for CyberNut's Free Baseline Campaign

Cybersecurity threats to schools are real, costly, and increasing. Take the first step towards protecting your district with our no-cost, 2-week Baseline Security Assessment.

Recommended Next Steps

- **Run a Baseline Campaign –** Free initial assessment to gauge your district's vulnerability.
- **Deploy the Onboarding & Training Campaign –** Instantly start building a culture of awareness and reporting.
- **Monitor & Optimize –** Use the dashboard to track click rates, real threat reports, and user engagement.
- **Actionable Data –** get detailed results you can immediately use to secure superintendent, cabinet, and board support for ongoing cybersecurity training.

Empower your district to move forward confidently with the cybersecurity solutions you need.

TAKE THE FIRST STEP TODAY

Click here to get your
Free Baseline Assessment