BlueHook
PHISHING MANAGEMENT

Phishing defense built for K-12 districts.

Your staff are the target. We turn them into your strongest line of defense — and when something slips through, we pull it out of every inbox in the district before it spreads.

Fully managed | Staff & student training | District-wide remediation | Board-ready reporting

One-click reporting

A report button built into Outlook and Gmail for every staff member.

District-wide removal

A single action pulls a malicious email out of every inbox it reached.

Evidence on demand

Training records and board-ready reporting whenever you are asked for them.

Managed phishing protection and security awareness for school districts, delivered by **Blue Ridge IT Solutions**.

(423) 292-1922 · info@blueridge-us.com

BLUE RIDGE
IT SOLUTIONS

THE PROBLEM

One click is all it takes.

School districts hold exactly what attackers want: student records, staff payroll, vendor payments, and thousands of email accounts protected by one password each. Nearly every serious incident starts the same way — a convincing email that reaches someone busy.

- **Your staff are the entry point.** Teachers, aides, bus drivers, and office staff all have district email, and most have never been shown what a modern phishing attempt actually looks like.
- **Turnover never stops.** Substitutes, seasonal hires, student workers, and new staff arrive every year, so awareness is not something a district can solve once.
- **Reporting usually goes nowhere.** Staff either ignore a suspicious email or forward it to a help desk address where it waits. Meanwhile the same message is sitting in dozens of other inboxes.
- **Small teams, big surface.** District technology teams are stretched across devices, networks, and classrooms. Very few have time to investigate message headers or hunt an email across every mailbox.
- **The consequences land on you.** Compromised accounts lead to exposed student data, diverted payments, and compliance and insurance obligations that are difficult to evidence after the fact.

BlueHook is the whole program, run for you.

Most tools hand a district another dashboard to staff. BlueHook is a managed service. Blue Ridge runs the simulations, monitors what your staff report, investigates every message, removes the dangerous ones district-wide, and delivers the reporting your board and insurer ask for. Your team keeps full visibility without inheriting another job.

THE RESPONSE LOOP

From reported to removed — usually before it spreads.

Every suspicious email your staff report follows the same path. The work happens on our side; your team sees the outcome.

1 Report
Staff click the button in Outlook or Gmail

2 Investigate
Headers, links, files and reputation checked

3 Contain
Every copy found and removed district-wide

4 Close loop
Reporter thanked, your team alerted

1 Staff report in one click

A BlueHook button sits directly in Outlook and Gmail — no forwarding, no attachments, nothing to remember. Staff are then asked, without blame, whether they clicked a link or entered a password. That answer separates a routine report from an urgent account compromise, so we ask every time.

2 We investigate it properly

The message is scored automatically and opened for full inspection: sending domain, message headers and delivery path, sender authentication results, every embedded link, and any attachments. Domains, addresses, and files are checked against threat reputation sources so the verdict is evidence-based, not a guess.

3 We find every copy and remove it

One report rarely means one recipient. We search every mailbox in the district to establish the true blast radius, then quarantine or delete the message everywhere it landed in a single action — and restore it just as quickly if it turns out to be legitimate.

4 We close the loop

The staff member who reported it receives a branded thank-you confirming what happened. It is the step most programs skip, and the one that keeps people reporting. Your technology team receives an alert with the finding and the action taken.

What your team does

Reviews alerts, opens the portal when they want detail, and acts directly if they prefer. Nothing is required of them for the loop above to run.

What we do

Everything else: monitoring, triage, investigation, district-wide removal, staff follow-up, campaign delivery, and reporting.

BLAST RADIUS

The report is one inbox. The problem is all of them.

When a staff member reports a phishing email, the same message is almost always sitting unopened in other mailboxes across the district. Finding those copies is the difference between an incident and a near miss.

Find every copy, remove them together

ILLUSTRATIVE

Search every mailbox

We query the whole district, not just the reporter, to establish exactly who received the message and whether anyone interacted with it.

Remove in one action

Quarantine or delete every copy at once. Quarantine is reversible, so a false positive is restored to inboxes just as fast.

Block what repeats

Persistent senders and domains are blocked district-wide so the next attempt never reaches a staff inbox at all.

Your team is told, not tasked.

Every action is logged with who did it, when, and why. Your technology team receives an alert with the verdict, the number of inboxes affected, and the action taken — and a flag the moment a staff member tells us they entered credentials, because that is an account compromise, not a phishing email.

WHAT IS INCLUDED

A complete program, not a single tool.

Detection and response, ongoing training for staff and students, and the evidence you need for compliance and insurance — in one managed service.

THREAT RESPONSE

Active Threat Manager

A live queue of everything your staff report, triaged and investigated by us.

- Automatic risk scoring and categorization
- Full header, link, and attachment inspection
- Sender authentication and delivery path review
- Threat reputation lookups on domains and files
- Assignment, notes, and a full audit trail

CONTAINMENT

District-wide remediation

Find and remove a malicious message everywhere it landed, in one action.

- Search every mailbox to confirm blast radius
- One-click quarantine or delete across the district
- Restore instantly if a message was safe
- Block a sender or domain going forward
- Works across Microsoft 365 and Google Workspace

SIMULATION

Phishing simulations

Realistic, safe tests that show who needs help before an attacker finds out.

- Large library of realistic templates
- Scheduled campaigns run for you
- Open, click, and submission tracking
- Teachable-moment landing page on click
- Per-user and per-campaign results

AWARENESS

Staff training library

Short, plain-English video lessons written for school staff, not IT departments.

- 40+ episodes covering real district scenarios
- Topics from gift-card scams to ransomware
- Built-in knowledge checks
- Completion tracking per staff member
- Shareable links for onboarding and substitutes

STUDENTS

Student Academy

Age-appropriate digital-safety learning that students actually engage with.

- Gamified modules with points and badges
- Class and campus leaderboards
- Assign by class or grade level
- Progress visible to staff

EVIDENCE

Compliance & reporting

The documentation your board, auditors, and insurer ask for.

- Training completion evidence by staff member
- Support for FERPA and CIPA obligations
- Trend reporting and highest-risk users
- Board-ready reports exported to PDF

WHAT YOU SEE

Proof the program is working.

Districts get a live portal carrying your name and logo, plus reporting written for people who do not work in security — the numbers a superintendent, board, or insurer asks for.

Reported threats, as your team sees them

ILLUSTRATIVE VIEW

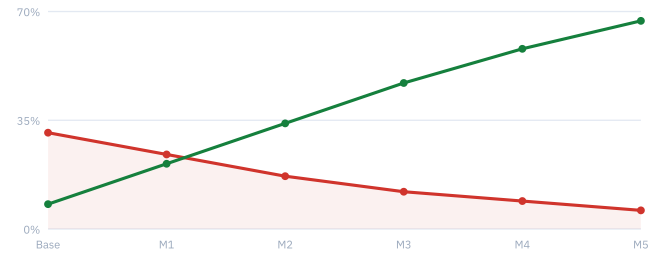
ACTIVE THREAT MANAGER

3	41	128	96%
OPEN THREATS	INBOXES HIT	REMOVED	CONTAINED < 1 HR

SENDER DOMAIN	SUBJECT	INBOXES	RISK	STATUS
district-payro11.com	Direct deposit change required	18	High	Removed
o365-verify-mail.net	Your mailbox is almost full	12	High	Quarantined
gift-rewards-hub.co	Principal needs a quick favor	7	Medium	Removed
vendor-invoices.biz	Overdue invoice #48122	4	Low	Marked safe

Risk down, reporting up

ILLUSTRATIVE



Clicked a simulated phish Reported it instead

Training completion

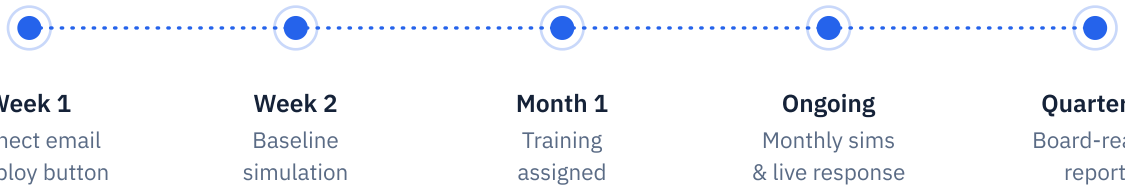
ILLUSTRATIVE

Evidence by staff member, exportable for audits and insurance renewals.

ONBOARDING

Live in days, not months.

We do the setup. Your technology team authorizes the connection and we handle the rest — deployment, campaigns, triage, and reporting from day one.



- ✓ **Connect your email.** A guided, read-and-remediate connection to Microsoft 365 or Google Workspace, authorized by your administrator.
- ✓ **Baseline simulation.** We establish where your district stands before any training begins.
- ✓ **Ongoing management.** We run campaigns, triage reports, and remediate threats continuously.
- ✓ **Deploy the report button.** Pushed to staff automatically in Outlook or Gmail. Nothing for them to install.
- ✓ **Assign training.** Staff library and Student Academy, scheduled on a cadence that suits your calendar.
- ✓ **Reporting rhythm.** Regular summaries for leadership plus board-ready reports on request.

Your district portal

Live campaigns and results, every threat your staff reported and its outcome, inbox search, and self-service removal if you would rather act yourself. Co-branded with your logo.

Alerts to your team

Email alerts on new threats with risk level, blast radius, and action taken — plus an immediate flag when a staff member tells us they entered credentials.

Let's protect your district.

We will walk your technology team through the platform, run a no-obligation baseline simulation, and show you exactly what your staff would do today.

BLUE RIDGE IT SOLUTIONS
SMART SOLUTIONS. STRONGER BUSINESS.

(423) 292-1922

info@blueridge-us.com

blueridge-us.com