Caught in Week One

Email Security Pilot: three real attacks surfaced and were caught in a single weekend, before a single blocking feature was ever switched on.

The Challenge



A compromised account doesn't look like an attack – not to a spam filter, not to the person who opens it. Any single message can look ordinary. The only way to catch it is to score the pattern across many messages at once.

Two public school districts found this out in their first week on Wizer Email Security, before a single blocking feature was switched on.

At A Glance

Industry:	Public school education
Mailboxes in pilot:	~1,000 (primary district)
Deployment stage:	Watch-only, no blocking turned on
Trial window:	First week of deployment
Real attacks, week one:	4, across two districts
Detection approach:	Pattern scoring across a set of messages, not single-email filtering

The Approach

Both districts started in pilot mode: WES scores every message as production would, logs what it would have done, and takes no action, zero risk while it proves itself.

Instead of judging each email alone, WES scores behavior across a whole set of messages: volume, timing, sender-recipient relationships. That's what surfaced every incident below.

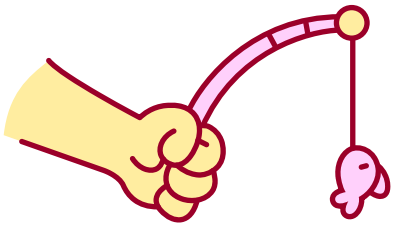
The Results

District A (~1,000 mailboxes): nobody was watching a dashboard, WES was simply logging what it would have done. By the next business day, that log held three real attacks from one weekend:

1 A compromised staff account, caught mid-blast.

~900 emails to ~600 mailboxes in under 13 minutes, in the middle of the night.



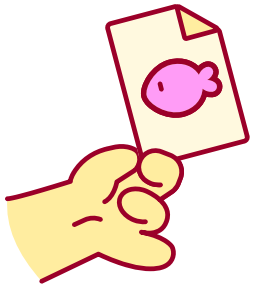


2 A coordinated, multi-district campaign.

Two other districts, in different states, sent the same lure 15 minutes apart. One version impersonating this district's own superintendent.

3 A phishing link disguised as a shared document.

125 messages reached 65+ mailboxes with the link hidden inside a fake "shared" file, not the email itself.



None of these looked unusual email by email. The pattern across many messages is what made them visible.

District B, onboarded that same week: about an hour after rollout, two compromised accounts sent 20+ copies of one phishing email to 10 colleagues in three seconds. WES flagged all of them, zero misses, within seconds.

Staff noticed independently about 8 minutes later. With active protection on, every copy would have carried a warning banner first.

The Ask

Neither district has turned on active protection yet, that's the conversation. Pilot mode proves detection works on live mail, with zero risk of a false positive.

Turning on blocking is what turns that proof into protection: every message above would have been stopped, banner and all, before anyone opened it.

See How Wizer Email Security Would Score Your Own District's

Book a demo

