"Do Staff Know What They Think They Know?" A Cybersecurity Knowledge Assessment at VDH

Lauren Smith | Pittsylvania-Danville Health District | Cohort 4, 2026

99% Training completion rate at VDH

89% Felt confident identifying phishing emails

53% Caught the hardest phishing scenario

62% Admitted to already failing a phishing email

ISSUE / GAP IDENTIFIED

- VDH maintains a 99% security training completion rate. However, completion alone does not measure whether staff can recognize and respond to real threats.
- New technology rollouts including electronic health records (EHR) and AI tools create additional risks.
- Real-world threats staff must recognize:
  -Phishing
  -Social Engineering
  -Ransomware

METHODS / OUTPUTS

METHODS
Review existing VDH training and consulted Chief Information Security Officer (CISO) and IT staff.

KNOWLEDGE ASSESSMENT
27-question survey covering phishing, ransomware, HIPAA, and self-assessment confidence.

PHISHING EMAIL SCENARIOS
12 mock email scenarios, from obvious threats to legitimate-looking messages, to test awareness.

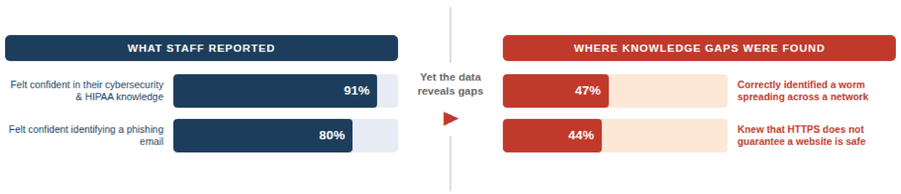
CHALLENGES

- Phishing simulation data is managed by VITA and not directly accessible.
- Limited access to data as an intern.
- Survey participation dependent on staff availability and willingness.
- Phishing scenarios were designed using fictional domain. Staff awareness of the assessment context may have influenced detection rates beyond what would occur in real world conditions.

OUTCOMES

The Confidence Gap — What Staff Reported vs What the Data Shows

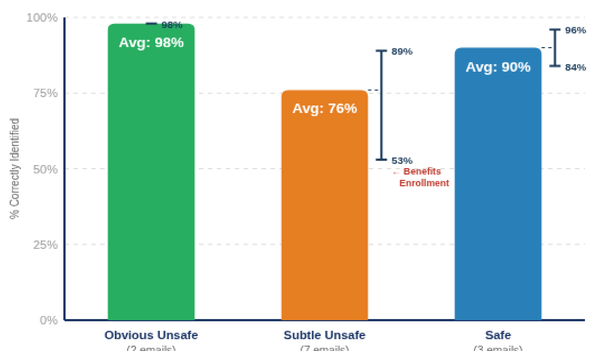
Self-reported confidence compared against actual performance on knowledge questions (n=45)



Key Finding: While **91%** of staff felt confident in their cybersecurity knowledge and **80%** felt confident identifying phishing emails — actual performance revealed critical gaps. Only **47%** could correctly identify a worm spreading across a network, and just **44%** knew that HTTPS does not automatically mean a website is safe. This disconnect between perceived confidence and demonstrated knowledge is a central finding of this assessment.

Phishing Email Identification Rate by Category

Average correct identification rate by email group (n=45). Error bars show the min–max range within each category.



KEY FINDING

Staff correctly identified **Obvious** phishing emails at an average of **98%** — but performance dropped significantly for **Subtle** phishing emails, averaging just **76%** with a range spanning from **53% to 89%**. This 45 percentage point gap demonstrates that sophisticated phishing attacks remain a critical vulnerability. **Safe** emails were correctly identified at an average of **90%**, showing staff can generally recognize legitimate emails.

NOTABLE

Even when staff were primed to look for suspicious emails, a plausible domain variation went unnoticed by nearly half of respondents — reflecting the challenge of maintaining consistent vigilance in a busy work environment.

What Would Make Security Training More Useful?

Based on open-ended survey responses from assessment participants (n=27 responses out of 45 total participants)

33% REAL WORLD & JOB-SPECIFIC EXAMPLES
Staff want scenarios that reflect their actual daily work

22% MORE PRACTICE & SIMULATIONS
Beyond annual training — hands on practice opportunities

19% SIMPLER LANGUAGE & PLAIN ENGLISH
Technical jargon remains a barrier to understanding

15% PRACTICAL RESOURCES & REFERENCE GUIDES
Checklists and visual guides to reference day to day

11% MORE FREQUENT & LESS REDUNDANT TRAINING
Shorter more frequent sessions rather than annual modules

"Understanding the verbiage would help tremendously."
PLAIN LANGUAGE THEME

"Having a visual guide with common phishing email examples like listed above would be awesome."
PRACTICAL RESOURCES THEME

"Use examples related to what we do. Show good examples of a real phishing or unsafe email so people are aware of the items that make it suspicious."
REAL WORLD EXAMPLES THEME

"Gamification of training with simulations beyond test emails."
PRACTICE & SIMULATIONS THEME

ACKNOWLEDGEMENTS

I would like to express my appreciation to those who helped me along the way: Michael Dolianitis, Brenna Link, Othello Dixon, Chris Andrews and all of those who helped me at the PDHD. Special thanks to Jeff Stover and Bridget Cochran for making this program possible.