CERIAS

The Center for Education and Research in Information Assurance and Security

Does Phishing Training Work?

A Large-Scale Empirical Assessment of Multi-Modal Training Grounded in the NIST Phish Scale

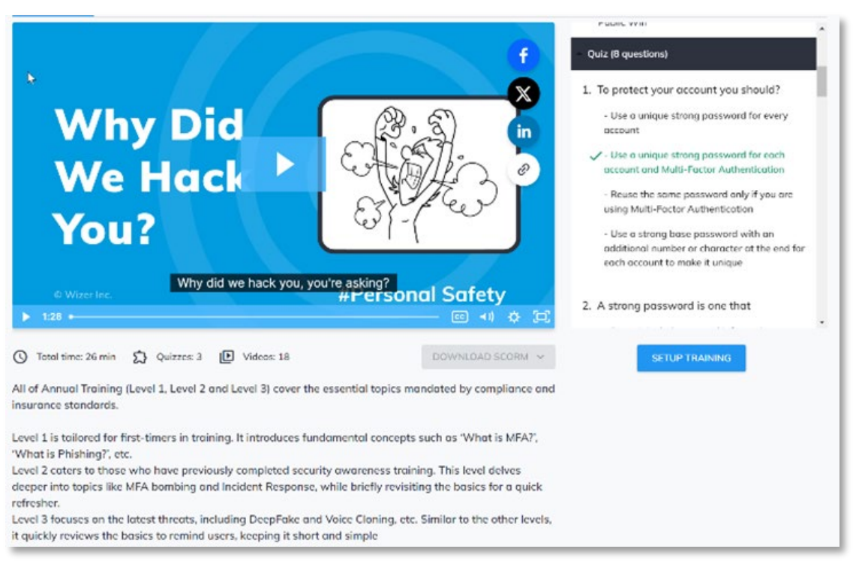
A. Rozema Purdue
Prof. J. Davis Purdue ECE

Background

- Phishing remains a critical cybersecurity threat.
- Effectiveness of cybersecurity training unclear across lure difficulties.
- Using NIST Phish Scale to measure effectiveness.

Research Questions

- Does phishing training reduce susceptibility?
- Is interactive training more effective than lecture?
- Impact of lure difficulty on training outcomes?



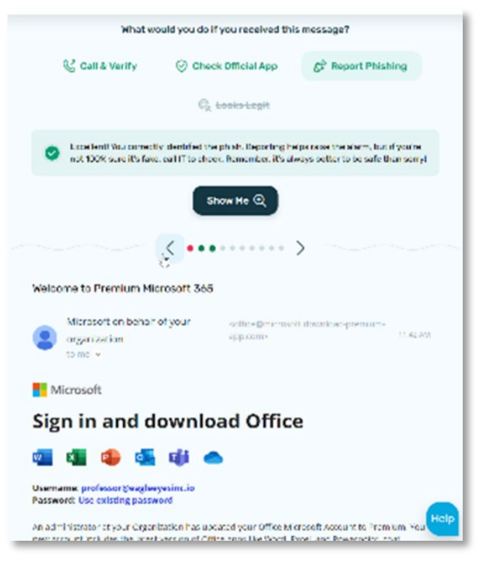
Quiz (8 questions)

1. To protect your account you should?
   - Use a unique strong password for every account
   - ✓ Use a unique strong password for each account and Multi-Factor Authentication
   - Reuse the same password only if you are using Multi-Factor Authentication
   - Use a strong base password with an additional number or character at the end for each account to make it unique
2. A strong password is one that

Total time: 26 min Quizzes: 3 Videos: 18

All of Annual Training (Level 1, Level 2 and Level 3) cover the essential topics mandated by compliance and insurance standards.

Level 1 is tailored for first-timers in training. It introduces fundamental concepts such as 'What is MFA?', 'What is Phishing?', etc.
Level 2 caters to those who have previously completed security awareness training. This level delves deeper into topics like MFA bombing and Incident Response, while briefly revisiting the basics for a quick refresher.
Level 3 focuses on the latest threats, including DeepFake and Voice Cloning, etc. Similar to the other levels, it quickly reviews the basics to remind users, keeping it short and simple



What would you do if you received this message?

Excellent! You correctly identified the phish. Reporting helps raise the alarm, but if you're not 100% sure it's fake, call IT to check. Remember, it's always better to be safe than sorry!

Welcome to Premium Microsoft 365

Microsoft on behalf of your organization

Microsoft

Sign in and download Office

Username: professor@wagleyesinc.io
Password: Use existing password

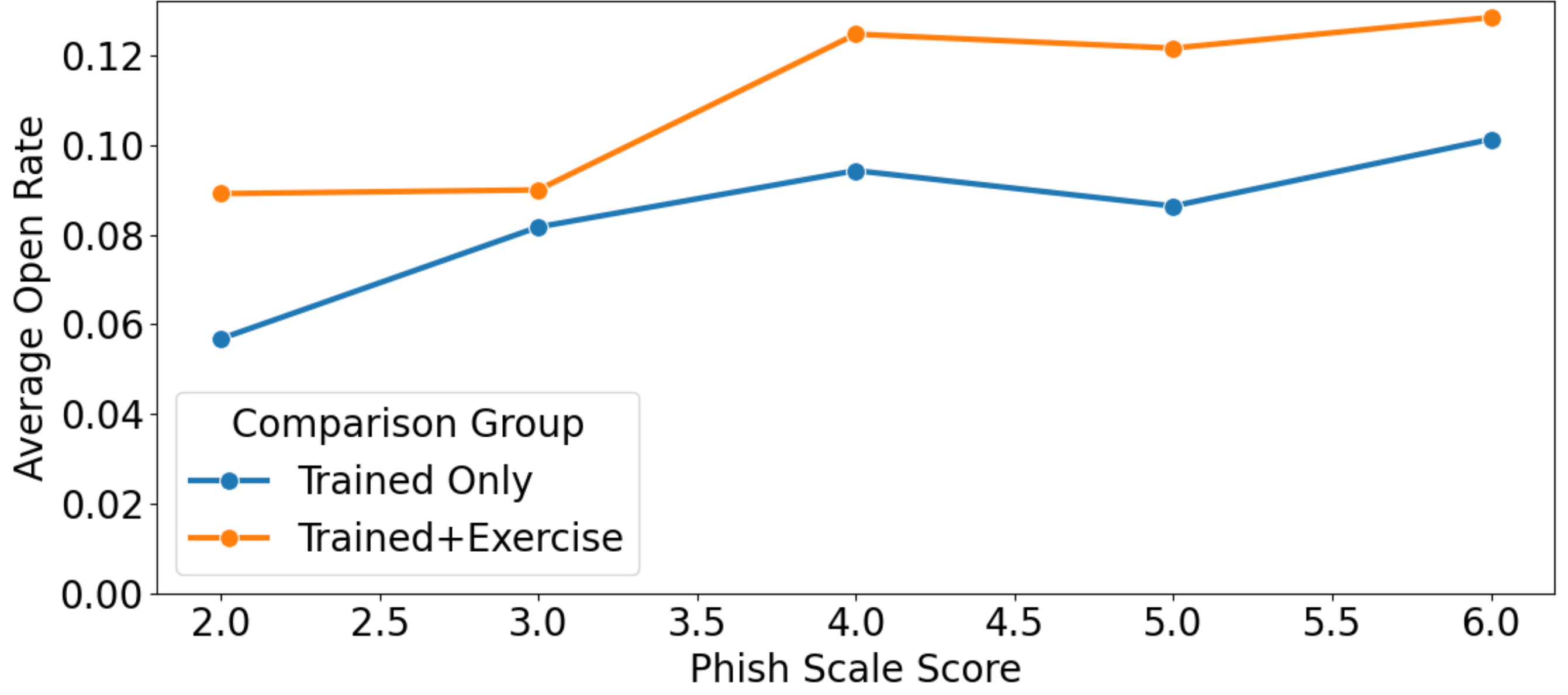
NIST Phish Scale

- Ranks phishing lure difficulty
- How similar is the Content to my every day?
- How many Cues let me know it is a phish?

Methodology

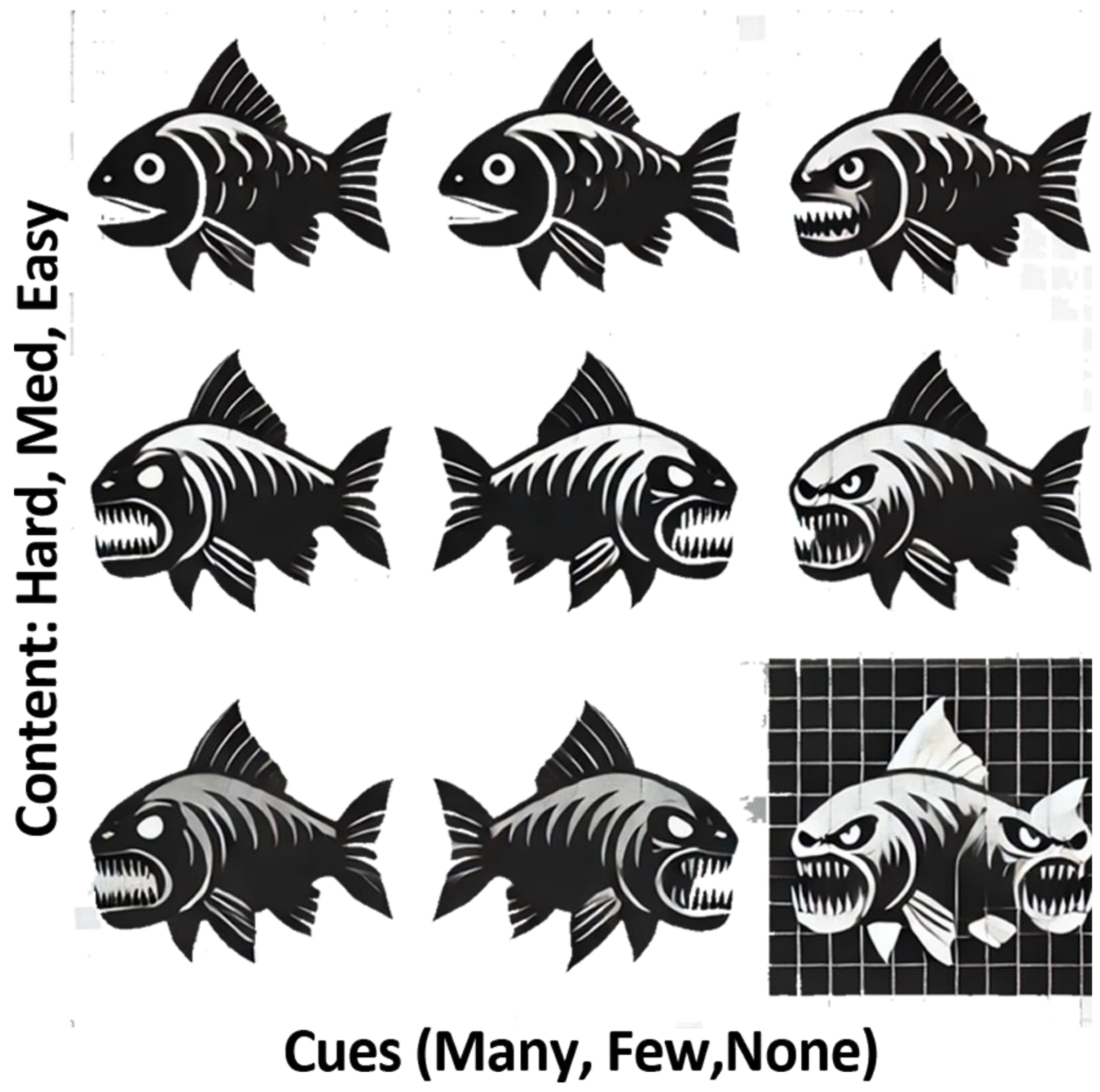
- ~4,000 employees from US fintech firm.
- Randomized trial: Control, Traditional, Interactive.
- Metrics: Email open rates, Click Through Rate (CTR), Reporting rates, Lure difficulty (NIST Phish Scale).

Average Open Rate by Phish Scale Score and Comparison Group

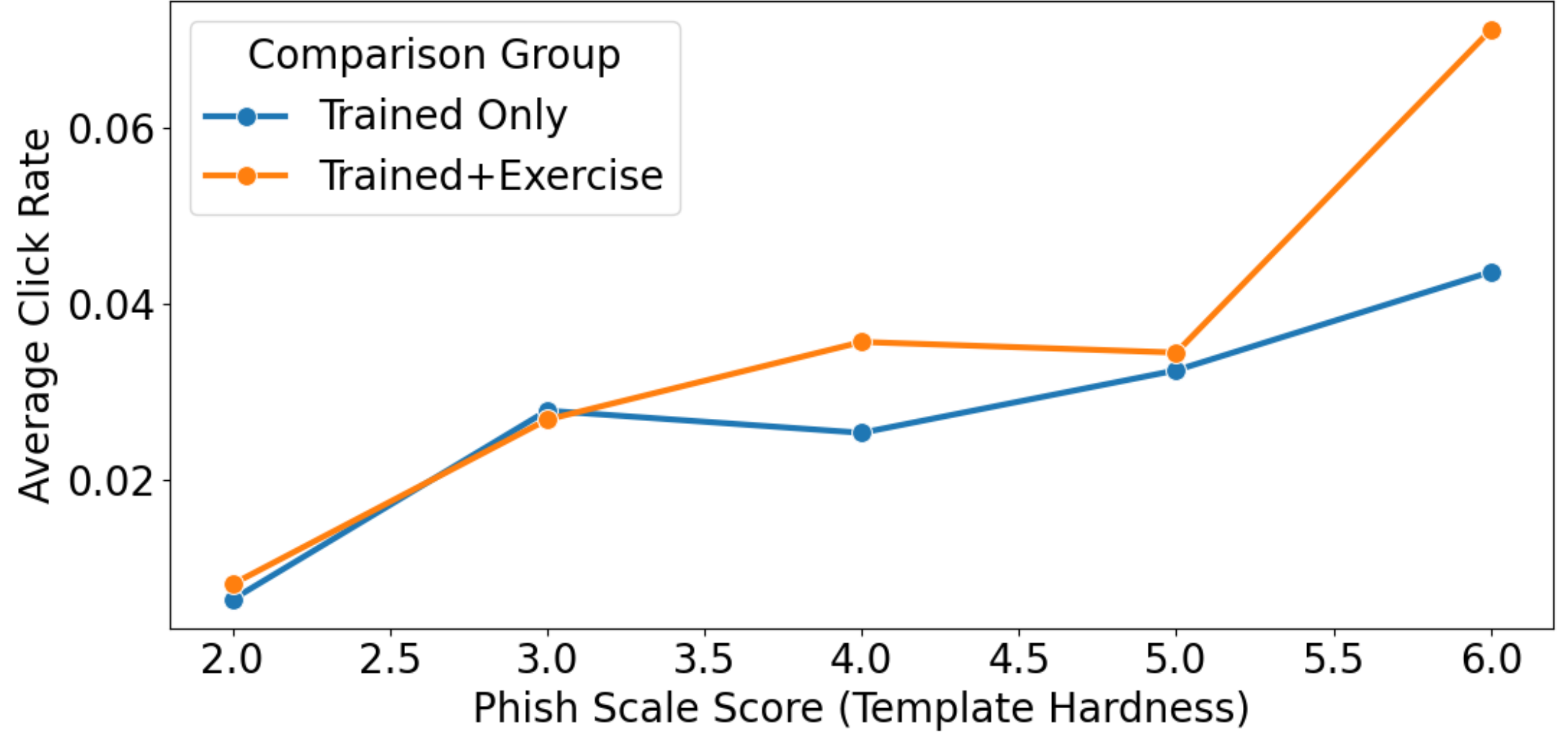


Paper:

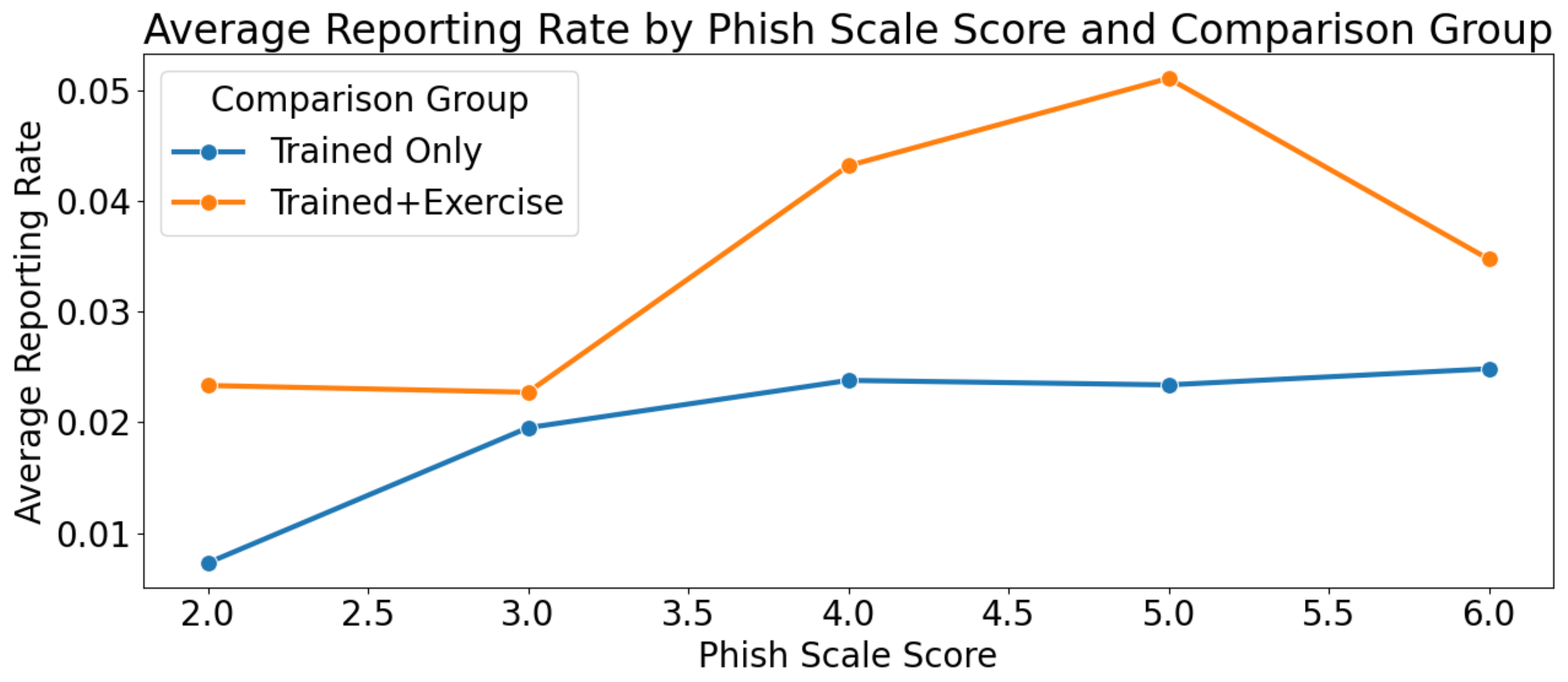
NIST Phish Scale



Average Click Rate by Phish Scale Score and Training Group



Average Reporting Rate by Phish Scale Score and Comparison Group



Key Findings

- Training has an impact!
- Interactive increased reporting by 37% vs. control.
- Higher difficulty lures correlate with higher CTR.

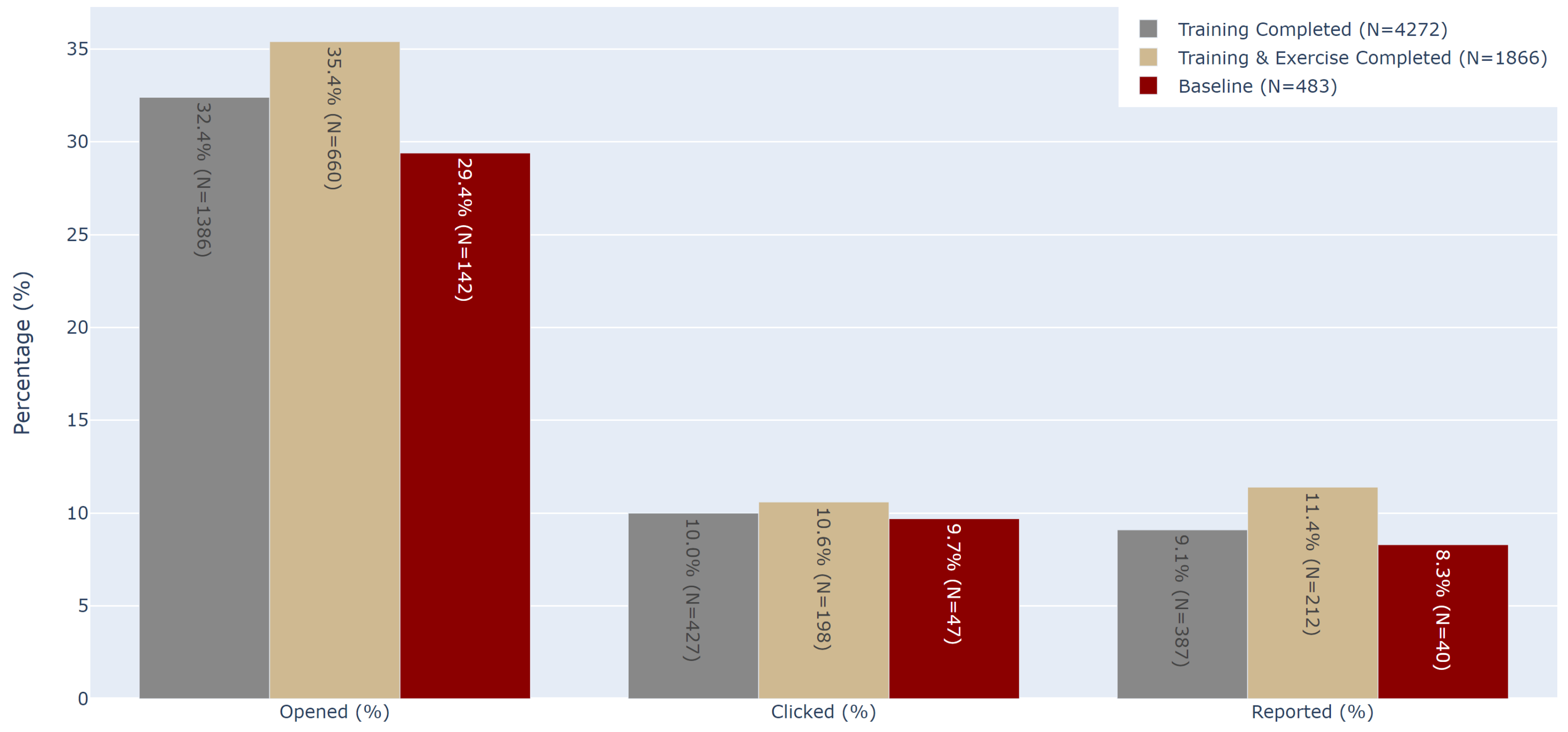
Recommendations

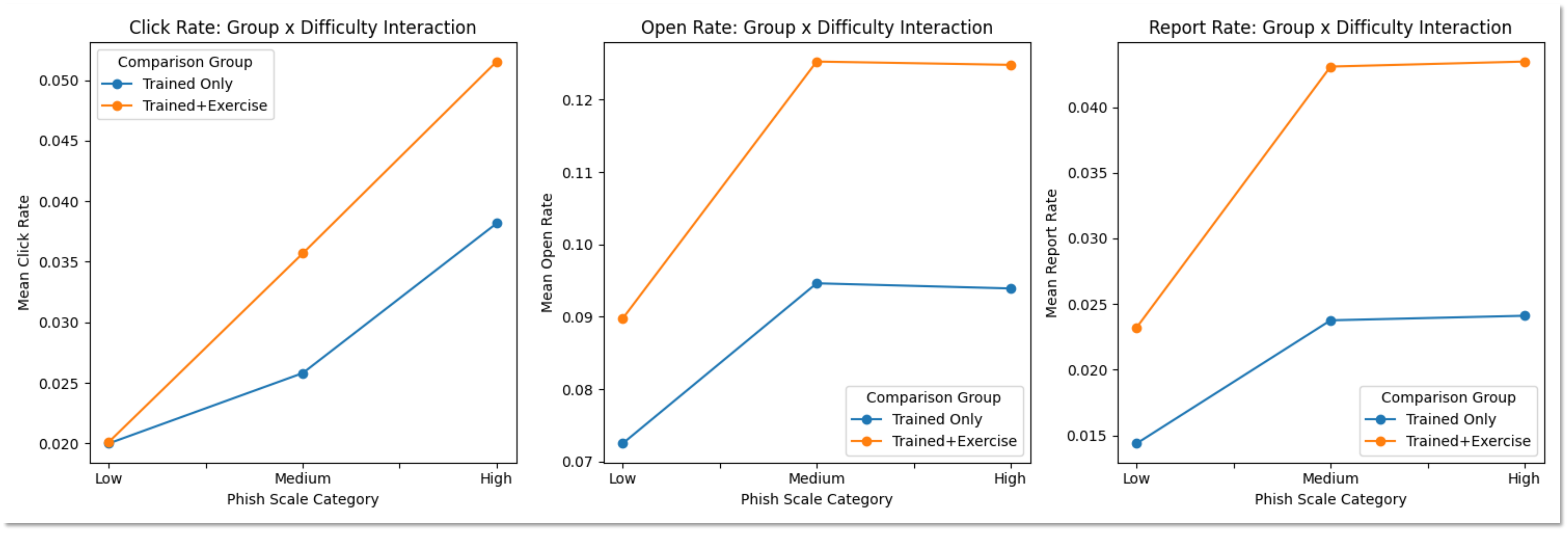
- Employ interactive training.
- Standardize metrics (NIST Phish Scale).
- Supplement with defensive strategies.

Conclusions

- Interactive training significantly improves reporting.
- NIST Scale predicts lure difficulty & susceptibility.
- Traditional training insufficient for advanced phishing.

Phishing Metrics Comparison by Group





PURDUE
UNIVERSITY

CERIAS