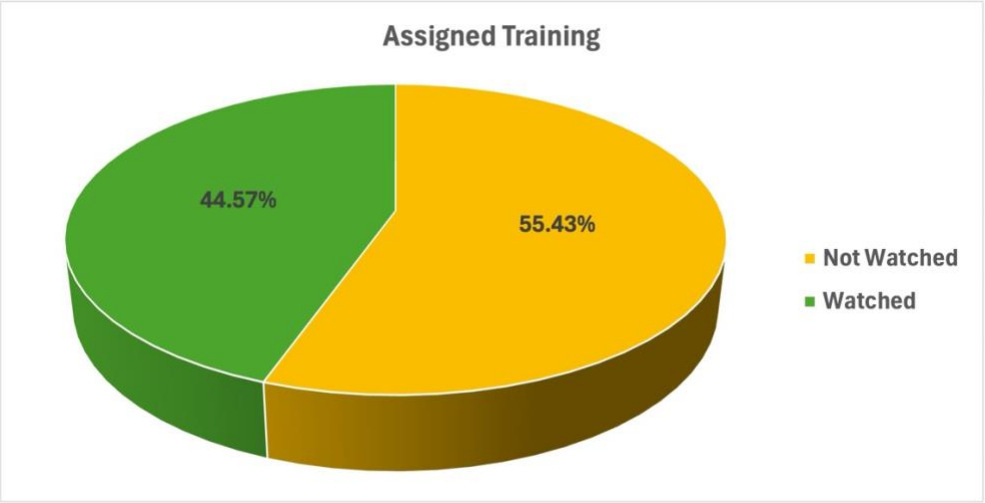
Knowing Is Half the Battle

According to Verizon's 2024 Data Breach Investigations Report, human error was often a contributing factor to data breaches, playing a role in 68% of cases occurring through accidental actions, the use of stolen credentials, and social engineering. This highlights the critical need for comprehensive awareness training. At CSHL, we have been assigning training and running phishing tests for about a year, and while the program is still maturing, test results and course completion rates have been disappointing to date.

TRAINING - Based on the last training module sent in September (SMS Smishing Fraud), only 45 percent of all users completed the training. The untrained CSHL colleagues are also in the majority of our incident response actions and impact lists when comparing training and our CSHL phishing metrics. By increasing compliance for training just a bit, we increase needed awareness that will build greater CSHL protections. By comparison, those who completed the training are very successful with testing and real-life outcomes, earning 97 percent accuracy with the security questions at the end of the training.



Considering these insights, we are adjusting our training strategy to improve compliance notifications for supervisors. We will be implementing shorter, less frequent training modules from each month to 3 - 5 per quarter. Compliance will be measured quarterly, rather than monthly. This approach is designed to give CSHL colleagues more flexibility for when the courses are taken and ensure that key information and cybersecurity principles are consistently reinforced.

TESTING - As phishing is still the predominant manner that cyber criminals gain access to Research environments, we run phishing test campaigns to educate the community on recognizing and responding to potential threats. Over the past 12 months we have conducted three assessments, and the outcomes have shown a concerning downward trend.

Campaigns (3)

Sent	Campaign	Users	Reported	Clicked	Submitted
08-15-2024	Phishing Simulation Campaign #3	1195	13	226	9
04-15-2024	Phishing Simulation Campaign #2	1099	13	77	76
12-11-2023	Phishing Simulation Campaign #1	677	24	60	101

Falling for a real phishing attack (**clicking** on links/attachments, **submitting** credentials) can give cyber criminals keys to our CSHL environment. Every CSHL person can potentially fall for a phishing scheme and jeopardize research data, the computer systems and operating environment for everyone. Our best defense is to support improved awareness and to avoid phishing. To support better outcomes, we will reach out to users who click on links or submit information during our tests, offering them guidance and support.

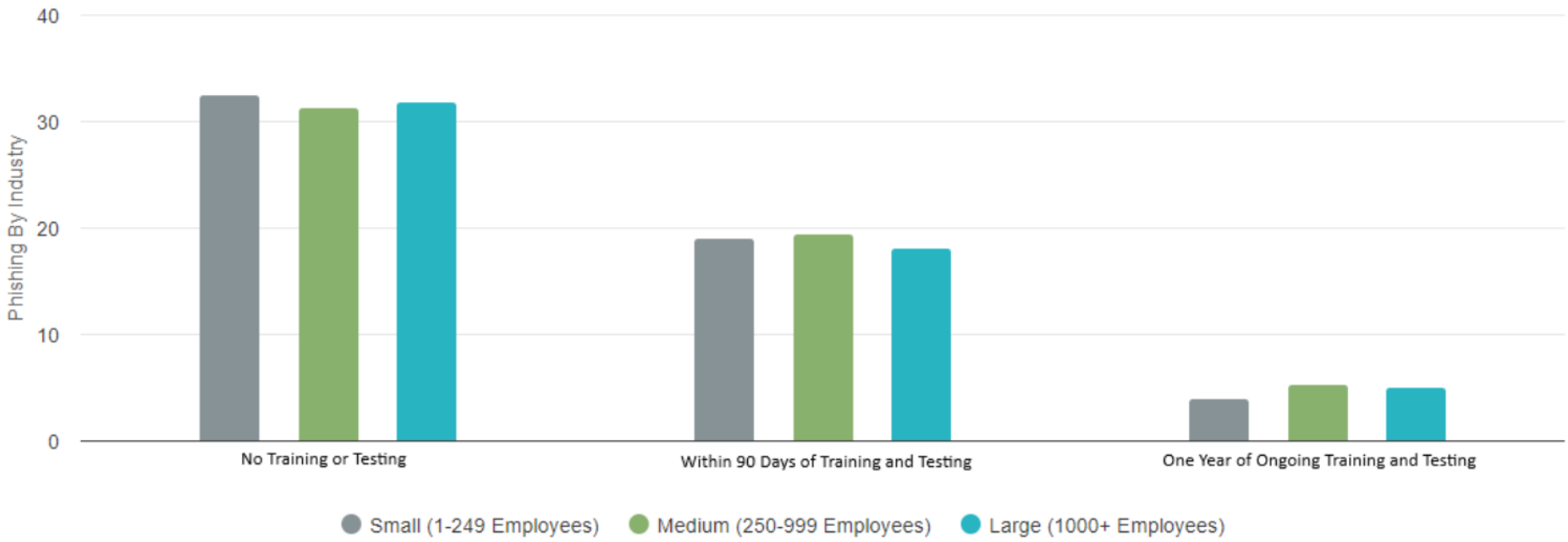
As before, if a phishing email is suspected, **report** it then delete it (See our Reporting Phishing Email guide). If it is your first time falling for one of these simulated messages, you will be given a gentle reminder about phishing. Additional training will be provided for users who fall for phishing more than once (consecutively) within 12 months. By increasing awareness and education on phishing simulations and real-life detection of phishing attacks, we can significantly reduce the likelihood of a data breach caused by these specific means.

A 2024 KnowBe4 phishing benchmark study revealed that organizations improve their ability to detect phishing attacks when they conduct phishing tests and training more frequently. The metric representing each organization's vulnerability to phishing attempts is termed *Phish-prone Percentage* (PPP). An organization's PPP reflects the proportion of employees who are susceptible to social engineering or phishing scams at any given time. The study showed that after 1 year of ongoing testing and training, the Education industry improved from a 31% phish-prone average to 4 %.

Cold Spring Harbor Laboratory

Cybersecurity Management Office

2024 Education Industry Phish-Prone Percentage



I am highly confident that the CSHL community can and will improve as our cybersecurity awareness program progresses. More attention to training can empower the CSHL community to recognize and respond to phishing attempts more effectively, thereby strengthening the overall security posture of the Laboratory.

We must balance scientific freedom with the needs to establish compliance with federal funding agency requirements and protect the organization from threats that could disable our work at CSHL, so I appreciate your patience while we raise the bar. Our cybersecurity mission for digital resilience is a commitment to safeguarding the future of Cold Spring Harbor Laboratory. We do this in service to the CSHL community and to support their legacy of meaningful science.

If you have any questions or concerns, please don't hesitate to contact me or the team directly at lissade@cshl.edu or cyber@cshl.edu.