proofpoint.

Security Awareness: A Tale of Two Perspectives

How effective are awareness programs—and do employees agree?

Who decides whether an awareness program is effective—or what even makes it effective? Is it the cybersecurity professionals who design and administer the training? Or is it the employees who complete it?

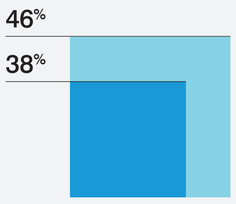
Proofpoint commissioned ISMG to interview security pros and general users to find out what each group thinks about awareness training today. And the results were surprising.

Top 3 program gaps

Both groups agree the top two gaps are related to engagement.

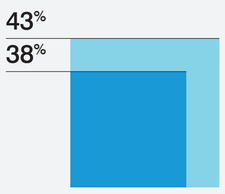
■ Security Pros ■ Employees

1. No carrot, all stick



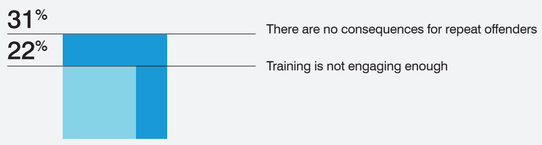
There are no incentives for good behavior

2. Phoning it in



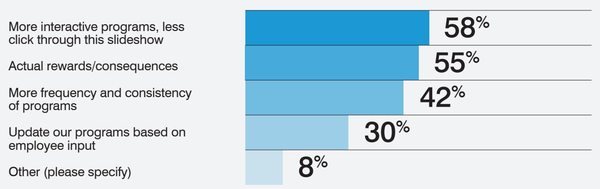
Employees are “just going through the motions”

3. Placing the blame



Filling the gaps

Security pros know that training programs could be more engaging. These are their top ideas for turning the tide.

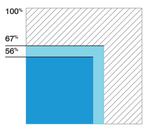


Common ground

Security pros and employees have differing opinions on a range of topics. But they agree on several key points.

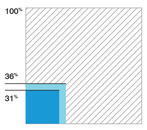
■ Security Pros ■ Employees

Training efforts measure up



Both groups think their organization’s **cybersecurity awareness efforts are more effective than their peers**’.

One tactic works best

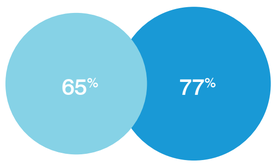


Both agree that **phishing simulation is the most effective** cybersecurity training tactic.

A reward/reality mismatch

■ Security Pros ■ Employees

Rewards



Both groups agree that rewards and consequences enhance program success

Reality

Yet only

8%

of employees say they’re rewarded good behavior

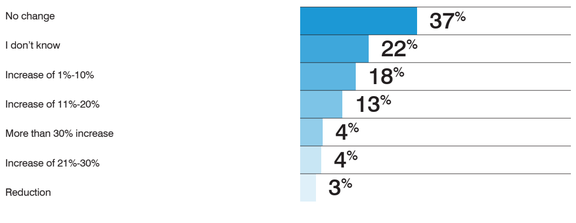
And only

28%

of security pros plan on implementing incentives in 2023

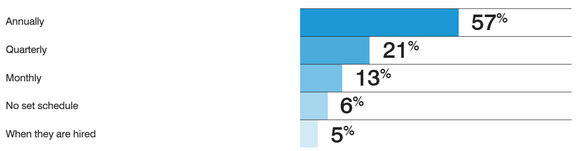
Budget issues

A lack of funding may be holding many programs back. Since 2021, 40% of programs have either had budget cuts or seen their budgets stagnate.



Threats are fast, but training is slow

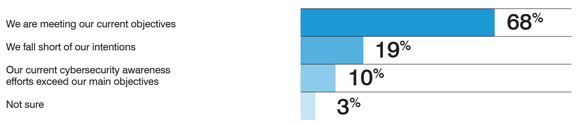
Threats evolve quickly in cybersecurity. Yet 57% of security pros say their security awareness training is annual or semi-annual.



The effectiveness disconnect

Despite infrequent training, security pros have a tendency for positive thinking when it comes to program effectiveness.

68% of security pros believe they meet or exceed their security awareness objectives



What experts say

The forgetting curve theory says people forget

90%

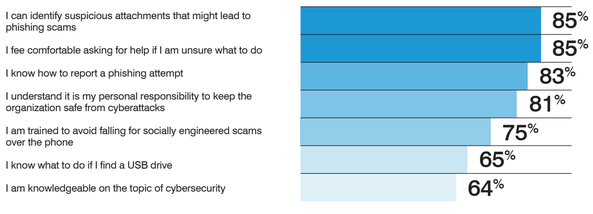
of the things they learn after seven days

A lack of insight may be the problem

The metrics security pros commonly use to assess their programs may not provide a complete picture. Phishing tests and education completion rates aren’t everything.

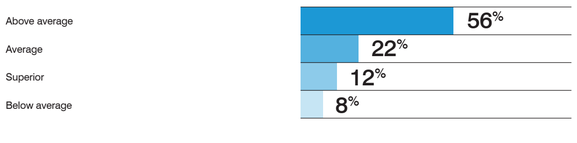
Top employee training takeaways

The topic of phishing repeatedly ranks highest. Employees are also most comfortable asking for help.



Employees don’t know what they don’t know

Although many common cyber threats don’t make the list of training takeaways, a whopping 69% of employees consider themselves extremely knowledgeable on the topic of cybersecurity.



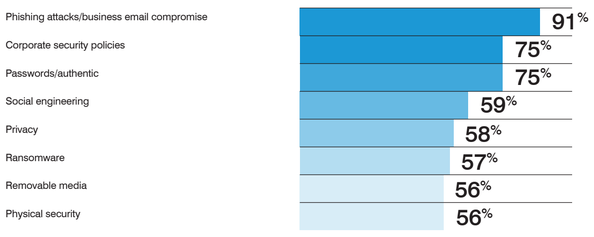
The content divide

What topics should be the focus of 2023 training programs? Security pros and employees want different things.

Rank	Topics security pros think should get more attention in 2023	What employees want to learn in 2023
1	Social engineering (62%)	Phishing attacks/business email compromise (BEC) (54%)
2	Phishing attacks/business email compromise (BEC) (58%)	Social engineering (45%)
3	Ransomware (55%)	Home/remote networking standards (44%)
4	Supply chain risk (46%)	Ransomware (40%)

Cybersecurity while working at home? Employees have no clue

It’s no surprise that home/remote networking standards are high on employees’ list for 2023. Here are the topics they say are covered by their current awareness programs.



What’s planned vs what works best

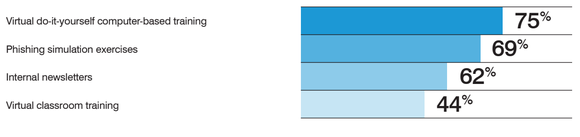
Planned training investments for 2023 don’t match up with how employees like to learn.

Rank	Where security pros plan to invest in 2023	What employees say works best
1	Phishing simulation exercises (49%)	Phishing simulation exercises (36%)
2	Virtual do-it-yourself computer-based training (40%)	In-person classroom training (16%)
3	Third-party programs (videos, story-based training) (31%)	Virtual self-paced computer-based training (16%)
4	Internal newsletters (30%)*	Virtual classroom-based training (12%)

*While internal newsletters are a priority for security pros, employees show no interest in them.

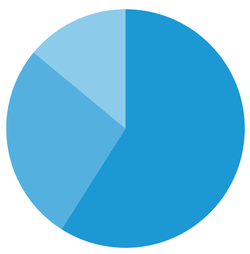
Another newsletter? No thanks

According to employees, newsletters are currently the 3rd most common type of training.



Who’s in charge

Who’s creating the programs

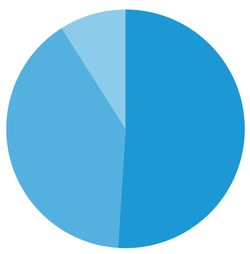


59%
of security pros say training designed in combination with outsiders

27%
say it’s in-house

14%
say it’s external-only

Who’s running them



51%
of security pros say training is run in-house

40%
say it’s a combination of external/internal

9%
say it’s external-only

Get the full results

Want to learn more? Download the 2023 Security Awareness Study for the full results. You’ll also get expert analysis on key findings to help you improve your own organization’s awareness efforts and make your people more resilient.

Download the 2023 Security Awareness Study