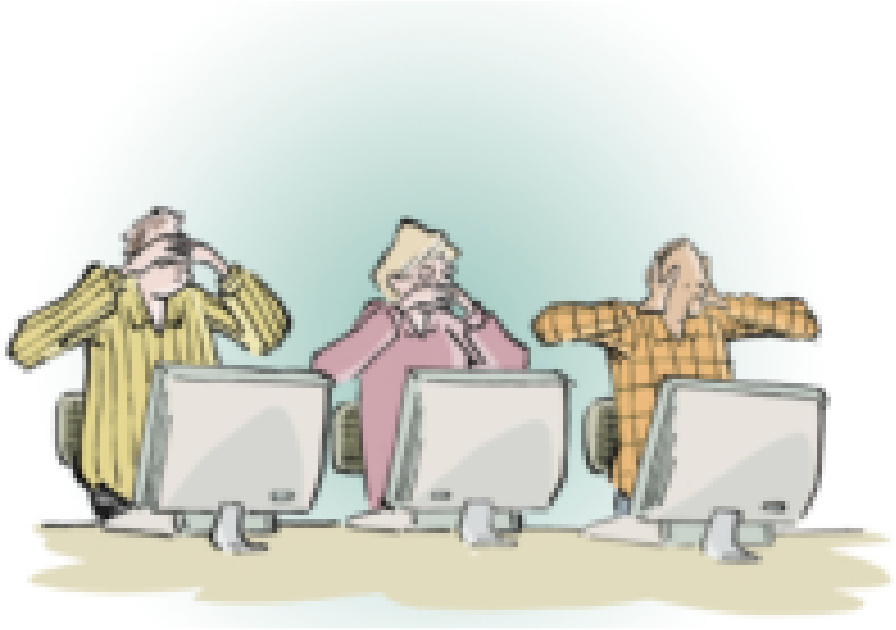
How to Transform Employee Worst Practices Into Enterprise Best Practices

It’s easy to dismiss security awareness training as unworkable. After all, its results are poor in most organizations. Osterman surveys show that less than a quarter of executives consider it e□ective. With an IT department continually having to put out □res due to the latest employee or senior executive being tricked into handing over sensitive information, it is understandable that they have little faith in attempts to educate users on phishing and its various schemes.

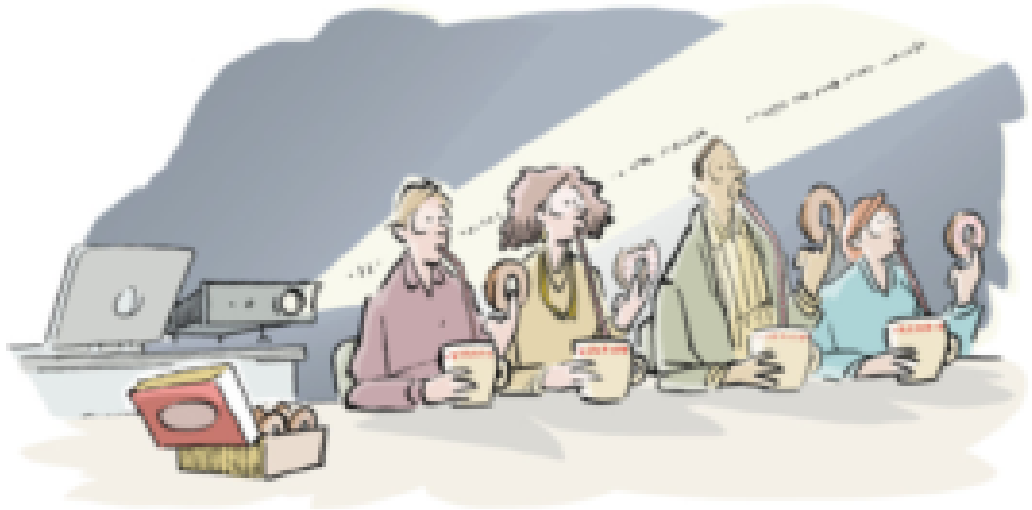
But the problem is not with the concept of user training itself but rather with the way it is being executed. Here are some of theways it is traditionally carried out

Worst Practice #1: Do Nothing and Hope for the Best
Only about one in □ve organizations admit to this as their “strategy” against the rise of phishing. But the actual number is probably much higher. The logic goes, “We haven’t had a company-threatening data breach to date, and we can live with these minor outbreaks which keep IT busy. So let’s hope ‘the big one’ doesn’t happen to us.”Aberdeen Group put a hefty price tag on reliance on this strategy. The analyst □rm said that there is an 80%
likelihood that infections from users will result in total costs of more than $2.5 million per year.

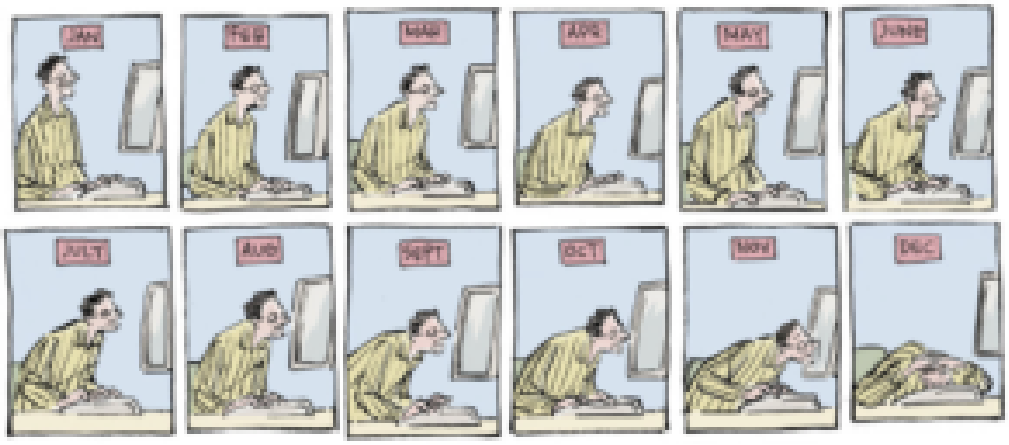


Worst Practice #2: Break Room Training

About 30% of organizations favor the break room approach. They gather as many employees as they can in the break room, provide lunch and have someone from IT or a security expert lecture on topics such as phishing, spear-phishing and whaling. This is certainly better than nothing, but often attendance is low and most of the audience looks upon the event as a time to make some headway on their email backlog. And the results speak for themselves. Measures of the e□ectiveness of phishing show little change after such brie□ngs.



Worst Practice #3: Monthly Security Videos
This can be done informally with videos made available via email or placed on the website for employees to view, or formally via mandatory classes. These short clips educate users on the perils of promiscuous clicking and on the many snares used by phishers to reel in unsuspecting employees. About one in four organizations gravitate towards this method. At best, this can be categorized as being little more than a super□cial training program. On its own, it can't be expected to do much to diminish the risk of data breach. It also causes training fragmentation because important topics are covered months too late.



Worst Practice #4: Phishing Tests
This approach pre-selects high-risk employees only and sends them simulated phishing emails to see how many fall victim to the attack. This is typically paired with some kind of educational module such as links to training modules for o□enders as well as short videos to view to increase awareness. The plus on this method is that it o□ers some kind of metric about phishing. The minus is that employees soon get wise to it and "prairie dogging" begins to happen – an employee sees a phishing test email and pops his or her head up above the cubicle to let the others know to watch out for it. This approach, then, is both limited and too simplistic.

These Worst Practices are the reason why some IT managers struggle to obtain budget approval for more e□ective security training measures as they struggle to win the □ght against phishing. Unaware of the shallowness of their ongoing e□orts to proof up sta□ against attack, executives redline training expenses as “we are already doing that” and buy into vendor hype by throwing money at new technology to deal with latest threat vector. Alternatively, they disapprove security training as the do-nothing approach appears to be working.