THREATREADY™
RESOURCES
Preparing Your People

Your Employee Cyber Defense - Is It Enough?

The problem persists
According to new research, typical cyber safety training offers inadequate protection against your single greatest security threat: your people. When 95%* of all breaches are caused by human error, preparing your people is the most critical factor in keeping your company cyber safe. But are your people truly threat ready?

They thought they had it covered – and then they were hacked
Most companies are not prepared to thwart a cyber attack. The sheer number of victims is proof alone: AT&T's latest Cybersecurity Insights Report reveals that 90% of U.S. organizations were affected during the past year. Many of these companies had training programs in place they believed were effective — but the problem goes well beyond phishing.

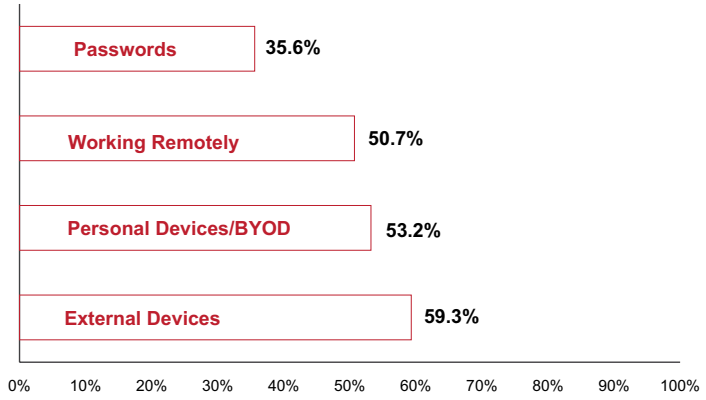
"The risk exposure is enormous and companies have a false sense of security. They are walking on a minefield and don't know it."

Dr. Timothy Shea, D.B.A
Associate Professor of Management Information Systems, University of Massachusetts

* IBM 2014 Cyber Security Intelligence Index

UMass study reveals vulnerabilities
The recently released Employee Cyber Readiness Survey, conducted by the University of Massachusetts, clearly shows that not enough is being done to prepare employees as their company's first line of defense. The findings show that many employees did not recall receiving any training in nine important areas that are common entry points for hackers.

Percent of employees that *did not recall* company communcations on:



A new approach is needed
Lengthy and infrequent conventional training sessions might tick the "training" checkbox, but they do nothing to create the long-term instinctive behavior change needed to mitigate the employee "weak link" of cyber defense.

ThreatReady provides a scientifically proven methodology

ThreatReady is uniquely qualified to close the serious gaps in today's typical cyber safety communications. We actively work with our clients to implement a custom-fit, research-based cyber security awareness campaign that includes:

1

Broad scope of multimedia, multichannel communications

Our broad scope of communications covers all of the key risk entry points, going beyond phishing to include proper password management, policy awareness, external devices, wireless security, importance of data backups, device theft, visitor control, incident response, and more. We provide a wide variety of content and styles to keep employees engaged and campaigns fresh, and use multiple channels, including social media, to deliver our communications. Because we are constantly creating new and current material, no piece of content is ever repeated.

2

Advanced learning techniques for long-term retention

The platform is built on proven principles to create long-term behavior change as described by ThreatReady Resources advisory board member Dr. Henry L. Roediger III, James S. McDonnell Distinguished University Professor | Co-Author of *Make It Stick: The Science of Successful Learning*.

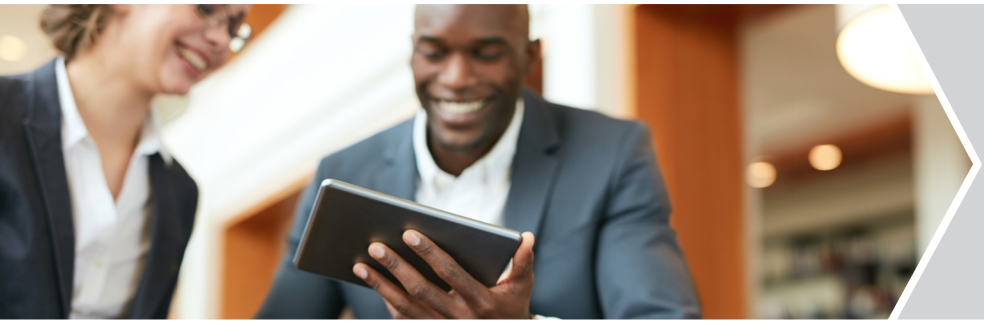
3

Year-round implementation assistance

ThreatReady provides full-service implementation to all of our clients. We begin by working with clients to develop a year-long awareness campaign customized to their specific needs, and then we actively help them implement the program throughout the year. Our ongoing service commitment ensures that building a cyber-secure culture is not an internal burden, but a true partnership that creates lasting results.

"The managed campaign service is critical for taking the work off my plate and has exceeded my expectations! The assistance in customizing content specific to our goals and the ongoing advice and guidance from the ThreatReady team has been extremely valuable."

Head of Information Security & Data Protection at Alexander Mann Solutions



Click here for a demo that will show you how to be cyber safe before a hacker gets in. To learn more, visit our website at www.threatreadyresources.com.