Go Beyond Cyber Awareness... to Cyber Preparedness

THREATREADY

Turn Your People Into Cyber Heroes

ThreatReady Cyber Preparedness Training is a new kind of training, based on the latest science on learning.

It offers a proven model to establish new and safer behaviors among your staff - to make cyber safe habits as automatic as putting on a seatbelt.

Why companies need higher-level cyber training

>90% of breaches are tracked back to employees.

Traditional employee training approaches have not been effective for establishing cyber-safe behavior.

Risk audits show companies have continuing vulnerability due to employee behaviors – DESPITE having had training.

Despite the prevalence of cyber security training, 51% of employees are not prepared for today's cyber world! (UMASS Dartmouth Study)

- As organizations have invested and built up their cyber defenses, employees have become the weak link in cyber security.
- With the average cost of a data breach estimated at $8 million, that's a big problem.
- New regulations are requiring that organizations have continuous effective training in place – it's no longer acceptable to just "check the box" with traditional training approaches
- Compliance mandates for banks, insurance companies and other institutions require the ability to measure and report on training effectiveness.

Most training just makes people aware of cyber issues
Threat Ready prepares people to act cyber-safely

Because the only way to truly minimize the risk from unsafe employee behaviors is to change those behaviors.

ThreatReady teaches employees how to recognize and deal with dozens of threat vectors—from proper password management to incident response—and we deliver it in an enjoyable and engaging way so that employees actually do it! We keep campaigns fresh and deliver content through multiple channels, including social media.

Through real-world phishing simulations, employees are prepared to identify and react to actual phishing events. Advanced reporting provides detailed insights on end-user activity and enables targeted remediation.

ThreatReady then follows up with a full year-long implementation program - so that learning will translate into instinctive long-term behavior change, like putting on a seat belt or reaching for a fire extinguisher at the smell of smoke.

THREATREADY

Based on the latest learning science

ThreatReady uses state-of-the-art training methodologies based on how people actually learn to provide learning that truly sticks - and results in safer habits.

- Make it short
- Make it personal
- Make it engaging
- Make it stick

Delivered as a year-long program, this approach drives the lasting behavior change needed to ensure employees react instinctively to phishing and other attacks to protect the organization.

Drawing on recent discoveries in cognitive psychology and other disciplines, it offers concrete techniques that enable employees to become more productive learners. These include:

Active practice—applying concepts learned instead of passively receiving information.

Spaced retrieval—retrieving information regularly over time strengthens the pathways to permanent retention.

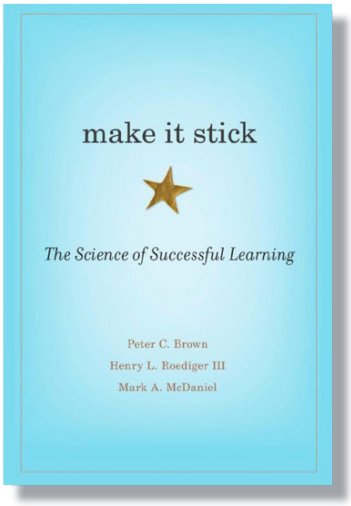
Interleaving—presenting concepts learned previously together with new concepts exposes the brain to a combination of events that more closely relates to everyday experiences.

Memory cues—taking advantage of the way human brains create memories to make concepts stick, by using mnemonics, vivid images, analogies, rhymes, or slogans.

Nudge theory—using continuous positive reinforcement and gentle frequent reminders to significantly influence the motives, incentives and decision making of large groups of people.

Microlearning—delivering short, bite-sized communications to drive engagement

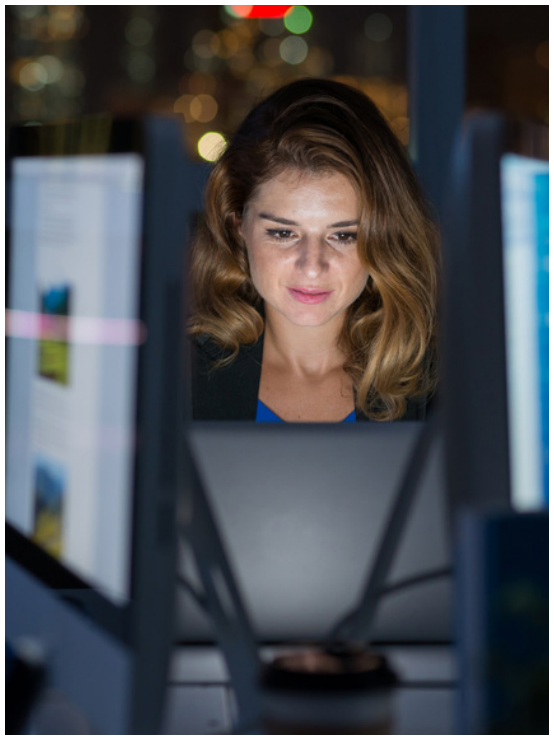
Company advisor Henry L. Roediger is a Professor of Psychology at Washington University in St. Louis. ThreatReady follows the principles outlined in his book Make It Stick: The Science of Successful Learning.



"ThreatReady's Cyber Security campaign implements well the principles advanced in my book" – Henry L. Roediger

Multiple modalities for maximum engagement

ThreatReady delivers content through a wide range of formats, across various media channels to accommodate different learning styles - and keep learning varied, interesting, engaging and even fun.



- Check-in Surveys
- Security Challenge Games
- Cyber Wire Newsletters
- Simulations
- “Make Me Care” Videos
- “Close-Up” Videos
- Interactive Courses
- Threat Check Assessments

Addresses all threat vectors

ThreatReady prepares staff to protect against all forms of cyber breach that can compromise a company.

- Internal Phishing
- External Phishing
- Vishing
- USB Drops
- Policy Awareness & Certification
- External Devices
- Safe Password Practices
- Social Engineering
- Malware
- Ransomware
- Malicious Links, Attachments & Apps
- Danger of Pop-up's
- Phishing Red Flags
- Dangers of Web Usage
- Dangers of Public WIFI
- BYOD
- Physical/Device Security
- Visitor Control
- Physical Access
- Shoulder surfing
- Data Protection
- Internal Threats
- Encrypting Confidential Information
- Data Backup
- Personal Use
- Drive Culture/Team & Importance
- Speak Up
- Make Them Care
- E-mail Distribution Sensitivity
- Identify & Protect Sensitive Information

Includes advanced phishing training

Phishing is the primary attack vector

- #1 attack vector targeting employees*
- As much as two-thirds contains malware**
- Busy employees are prone to "clicking without thinking", exposing their organization

SOURCES: * NTT Security GTIC 2017 Q2 Report,
** Verizon 2017 Data Breach Investigations Report

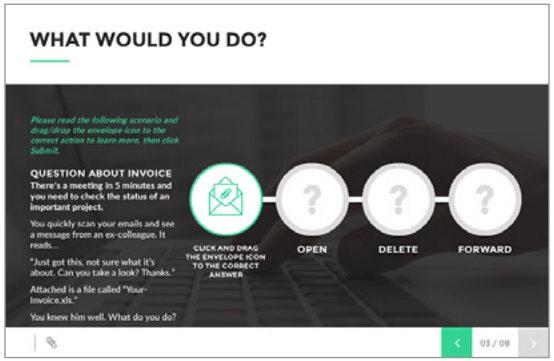
ThreatReady provides a comprehensive solution

Proactive Training

- Teaches employees to spot signs of a phishing email before they receive one
- Prepares employees to respond appropriately

Reactive Training

- Company-configurable "real-life" phishing simulations
- Educates against mistakes with no risk to the organization
- Employees directed to training if they fail
- Employers get full reporting on staff who click



THREATREADY

Implementation is easy & affordable

Aggressive pricing plus staff cost savings

ThreatReady beats or meets the cost of traditional cyber security training programs that offer less.

Plus, most training programs require fulltime trained employees to mount. ThreatReady works with your existing resources to develop a year-long program customized to specific needs - and assists with implementation of the program throughout the year.

Choice of content delivery

Cloud Hosted

- Training is hosted in the cloud and can be deployed using provided links
- Client simply distributes links internally via email, social, intranet, etc (all formats supported)

On-premise via client LMS

- SCORM industry standard packages are provided for all assets
- Customers simply download the SCORM package, load into their LMS, and deploy as they do for other training

Fully managed service

- Dedicated Client Services Team handles all campaign setup
- Assists with consistent campaign deployment
- Campaigns individualized to support an organization's specific risk profile and objectives
- Twice a month touchpoints
- Continuous measurement, monitoring and proactive reporting

THREATREADY

Frequently asked questions

How is ThreatReady different from other cyber security training?

Traditional cyber security training is a one-way flow of information from a human trainer or video courses. And your people are expected to absorb it and know how to apply it. But that's not reality.

Research shows people forget over 90% of what they learn through this method in just 6 days. Based on latest learning science, ThreatReady employs repetition over time, opportunities to practically apply what one learns, and multiple forms of content delivery to assure knowledge retention and long-term behavior change.

Also, while there is a place for computer-based training modules, too many programs rely on them completely as an awareness program - and there is definitely no such thing as "one size fits all" security training.

ThreatReady incorporates a wide variety of preparedness tools, including newsletters, posters, games, newsfeeds, blogs, phishing simulations, and more to assure success.

Why is this form of cyber security training even necessary?

The Internet is great for connecting the whole world – unfortunately it also connects us all to bad actors all over the world. Today every company is under constant barrage of attack from cybercriminals looking for a way in to steal money or valuable (and sensitive) data.

Over 90% of cyber breaches occur as a result of employees' unintended wrong actions. So the only way to truly protect one's company is to transform your people from the weakest security link to a hardened line of defense - by assuring that staff is not only aware of cyber security issues, but also have established cyber-safe work habits so that they don't fall victim to them.

What are the technical requirements for ThreatReady training? Can clients use their own LMS?

ThreatReady training modules can be delivered through any Internet-connected device and through any browser. Our content can be provided to clients to deliver through your own LMS (if you have one) or we can deliver it from the cloud directly to your staff.

How does ThreatReady assure security of client company data?

As you would expect from a cyber security company, we meet the highest standards of data security. We employ Amazon Web Services (AWS) to host our servers and data. More, we only store the minimal amount of data required for service delivery - typically email addresses with recorded clicks – and this data is encrypted and not shared with anyone.

How scalable is ThreatReady training?

Digital and cloud-based, there is no upper limit to the number of employees our training can serve. Further, we recommend and that all employees of a company undergo the training we provide to assure maximum cyber security.

What does it cost?

ThreatReady is aggressively priced to meet or beat most other cyber security training programs. Furthermore, ThreatReady client services manages the whole implementation process for you – and that saves you the cost of a full-time employee having to manage the program which virtually all other training programs require.

Contact us for a demo today!

THREATREADY
Turn Your People Into Cyber Heroes

ThreatReady Resources
34 Main St. Extension
Plymouth MA 02360

Phone: 857-293-6642
Email: info@GetThreatReady.com

GetThreatReady.com