## PHISHING IS BIG BUSINESS

It’s no secret that phishing is highly profitable for hackers. Conversely, phishing attacks continue to represent a fiscal disaster for organizations.

A recent study shows just how staggering this threat vector has become: The average 10,000-employee company spends $3.7 million a year dealing with the aftermath of phishing attacks. The average employee wastes 4.16 hours a year on phishing scams.

Top costs that organizations incurred as a direct result of phishing attacks involved the following: data breaches caused by compromised credentials and malware, as well as the costs of containing malware before it infects an entire network.

Are your employees adequately prepared against this threat, or are they vulnerable to falling for phishing scams?

> “The average employee wastes 4.16 hours a year on phishing scams.”

## WHY AWARENESS WON'T SOLVE YOUR PHISHING PROBLEM

**As security professionals, we're interested in proven practices rather than personal convictions.**

Because of this, we know that the mere acknowledgment of an existing issue is not the same as being adequately prepared to deal with it.

**Put simply, awareness does not drive action.**

From a corporate security perspective, readiness beats awareness in every risk scenario. For example, employees who open a seemingly benign email attachment may not recognize the subtle signs of a sophisticated hacker simply because they're aware that phishing scams exist.

Most awareness programs are focused on making employees aware of phishing, and are measured accordingly. We at CybeReady believe that this is only half the battle.

If phishing concerns you, it's important to take steps that will reduce the chances your employees will actually fall prey to an attack.

## DON'T UNDERESTIMATE THE COSTS & COMPLEXITIES OF IN-HOUSE TRAINING

When looking to purchase training-related content or technologies, most organizations only examine upfront costs. Focusing mostly on money spent means that they're missing a significant portion of their investment. The actual bill lies ahead once a program is deployed.

When measuring the costs of security training programs, it is critical to factor in three elements: cost of training preparation, time lost on employee training and engagement costs.

LET'S BREAK THESE INTO SUBCATEGORIES:

### ENGAGEMENT COSTS:

These are the subtle costs of any training program. Do your employees think favorably of security? Did they feel that your program has wasted their time? A good training program brings employees onboard, while a bad one pushes them away.

### TIME LOST ON EMPLOYEE TRAINING:

These indirect costs involve time spent on both training and associated travel costs. (By travel costs, we mean the time required to get everyone to the training, whether that involves all your empolyees in a conference room or having to troubleshoot remote login technical issues.)

### COST OF TRAINING PREPARATION:

These direct costs include money paid to external parties, such as consultants, software licenses and time-related costs, such as those associated with running the program, monitoring the learning software performance and time running around hoping everything works.

**Some of the world's leading organizations representing a variety of industries, such as healthcare, insurance and banking, among others, trust CybeReady with their companywide readiness training against phishing.**

CybeReady offers Phishing Readiness programs with an unmatched level of service that is full customizable to your region, industry and brand.

READINESS ANALYTICS REPORT

**You'll know your weak points.** It's critical that you obtain visibility into what triggers your employees to act on phishing scams, which departments are most vulnerable, and other risk factors. CybeReady empowers you to ground your decisions with detailed data that demonstrates improvement over time.

END-TO-END SERVICE

**We close the service loop.** The company's expertly designed and deployed Readiness Program leaves no stone unturned. You can monitor your organizational readiness with an annual solution that continuously implements phishing attempts, effectively teaching employees how to avoid them--even providing answers to unexpected events that otherwise might serve as a lure to your employees.

FAKE-ATTACK FREQUENCY

**Our training mimics reality.** Instead of a single simulation, CybeReady deploys a sequence of attacks, contextualized to both external events (holidays, conferences) and internal events (software upgrades, retirement plans). Now, you're able to prepare your employees for any hacker's diverse approaches to phishing.

NO INSTALLATION NEEDED

**You can leave onboarding to us.** CybeReady's cloud-based service means there's no software to install, no hardware to purchase, and no equipment to maintain. In under 48 hours, our customers are able to engage in an expert-led process with zero headaches or pitfalls.

FULLY CUSTOMIZED CONTENT

**We believe templates are for robots.** You can only be assured of employees' readiness with the most rigorous behavioral training. CybeReady specializes in highly convincing phishing attacks at varying levels of difficulty, from sector-specific, tailor-made messages to department and position-specific messages. All content is customer-branded and simulation-specific, and is linguistically and culturally adapted to your needs.

## WHY CYBEREADY?

**We believe that traditional information security is failing organizations by rarely addressing the unique risks posed by their most critical asset: people.**

CybeReady is the outcome of years of collaboration, during which its founders explored the 'Human Genome' of Information Security leading to the development of a new paradigm: Employee Cyber Readiness.

The team brings deep understanding and insight into required processes and solutions to manage human-centered risks led to the development of their highly effective readiness program. CybeReady specializes in the highly specific information security risks that employees pose, which are rarely (if ever) addressed by traditional awareness programs.

In response, CybeReady has created its readiness solution, best summarized by one of Shakespeare's most memorable quotes:

**"READINESS IS ALL."**

THE HUMAN READINESS COMPANY
CYBEREADY

info@cybeready.com | www.cybeready.com