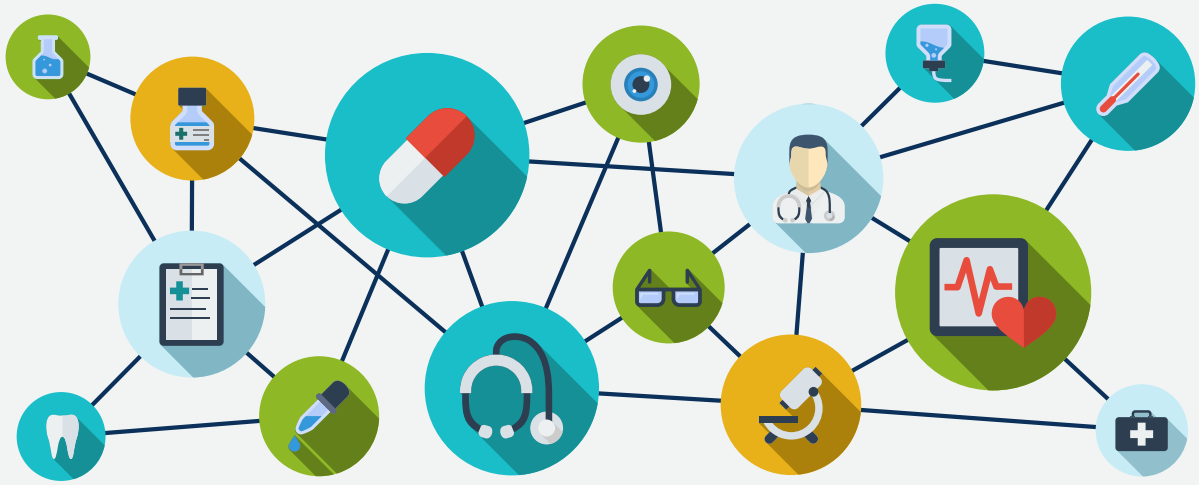
THE HUMAN READINESS COMPANY
CYBEREADY

THE HEALTHCARE INDUSTRY: A PHISHER'S PARADISE



Access to sensitive information has made the healthcare industry a preferred target for hackers. Training employees effectively against phishing methods remains the strongest line of defense.

As a global industry, healthcare has had to completely reinvent its operations over the past decade.

With the advent of web-based portals and cloud-based storage, patient files that once occupied vast amounts of office space have been transferred to remotely-accessible electronic files. Naturally, the information they contain is highly sensitive, including not only diagnostic reports, patient data and healthcare histories, but also confidential insurance and financial information.

Access to such information has made the healthcare industry a preferred target for hackers. Breaching network connections isn't their method of choice, however; they have found success much more frequently via phishing attacks. Their 'easy' marks: the thousands of employees entrusted with handling this information on a day-to-day basis.

Hackers' insidious methods have allowed them to gain employees' trust quickly. This has enabled them to steal passwords and login information, gaining access to internal networks, including patients' records, financial data and other sensitive materials, which they then exploit for profit or ransom.

Adding to that threat is the fact that today, information security professionals working within large healthcare organizations have an ever-growing scope of responsibilities. They are often expected to source third party vendors providing antivirus or antimalware solutions, as well as oversee any critical software updates, hardware maintenance, network security and employee training. Unfortunately, the latter often is relegated to off-the-shelf programs that may not provide the level of readiness employees need in order to avoid even simple phishing scams.

THE INSIDE STORY: EXECUTIVE-LEVEL DILEMMAS

An information security executive from a major countrywide healthcare network in Israel is all too familiar with this balancing act. He cites fraud as a major concern for his organization, as well as those of his peers in the industry.

"We're particularly concerned about the types of fraudulent activities that ultimately lead to transactions and money transfers taking place," he said. "Cryptoware, or ransomware, as it is commonly called, is a virus that hackers use to encrypt all of the data on your hard drive. They then require organizations to pay a ransom in order to decrypt your information, effectively holding your files hostage."

Imagine this worst-case scenario for information security professionals: attacks rendering critical files inaccessible grind all business operations to a halt, leaving organizations with few options once attacked.

"Every large organization has a few of these attacks on an annual basis," the executive added. "They usually originate with phishing, starting with a benign, legitimate-looking email. The email appears convincing enough to persuade the user to click on a link or run a file—and the malicious activity begins."

> **"Every large organization has a few of these attacks on an annual basis."**

THE CHALLENGE: PREPARATION + PREVENTION

Knowing what's at stake and how individuals are trying to steal information is only part of the way toward guaranteed security and peace of mind.

Without full confidence in the right protective methods, information security professionals recognize that they may be compromising their own professional reputations, as well as the critical information they're charged with protecting.

"I was responsible for the security of information across an entire healthcare organization," the executive explained. "Knowing that our employees were undoubtedly the most vulnerable access point for hackers, it was a top priority for me to provide them with the most effective anti-phishing training."

However, resource constraints in terms of human resources required the executive to carefully consider options that would not detract from his team's other roles and responsibilities. He sought to build users' information security skills without sacrificing precious time.

"That's a huge plus. Each of the 70 attacks that they launched in the first year were of a high quality; they were localized to our industry, and showed us exactly where our weak points existed," he said. "Beyond that, CybeReady's leadership was always accessible, listening to our feedback or making quick fixes whenever needed."

"Knowing that our employees were undoubtedly the most vulnerable access point for hackers, it was a top priority for me to provide them with the most effective anti-phishing training."

> **“CybeReady’s program runs on its own, which means that I don’t have to invest my time or that of my team in operating or configuring attacks.”**

“Our selection process involved testing three different systems. We eventually chose CybeReady, and here’s why: they not only increased our employees’ awareness, they offered a service that was unmatched by their competitors. CybeReady’s program runs on its own, which means that I don’t have to invest my time or that of my team in operating or configuring attacks. It literally involved zero effort on our part.”

The company’s level of service was apparent even during the early days of the engagement. “Service from other vendors didn’t come close to this; what had previously taken me up to three weeks annually now involved little more than a few hours a month, at most. I knew that I could trust CybeReady, and have heard colleagues in the industry who chose them say the same.”

The executive cautions others to consider the difference between training and awareness programs. “There are a number of phishing options that appear to have comparable training content and expertise. The differences are often only visible after several months of reports indicate a marked change in employee behavior. As CybeReady’s phishing attacks changed form over time, the organization’s employees responded more intelligently than they had before. Few other options, if any, also offer the availability and attention possible from CybeReady.”

THE RESULTS:
A TANGIBLE IMPACT

With customized training content that carried the health organization's own brand, it looked as though everything had been done in-house.

"The phishing emails themselves were tailored for the healthcare sector, making them appear to be legitimate; CybeReady's approach was very efficient," the executive told us.

CybeReady serves as an invisible partner that leads and designs the training process from start to finish, but doesn't necessarily appear anywhere in employee-facing emails or the responsive content that serves as their phishing lessons.

"Their extensive phishing campaign was highly effective, leading to a lot of emails from employees who raised red flags to our team regarding suspicious mails.

While serving in his leadership role, the executive could tell that the readiness program resonated with many of its 4,000 employees. He smiles when recalling the visibility that the program gave him and his team.

"The level of employee engagement in our case was very high compared to other methods I used in the past."

"For example, when I or my colleagues from information security would be walking down the corridor in our main office, I'd hear people say 'oh—it's you—from the phishing program!' The program made a real positive impact, and this was truly the point: to build our users' defenses, and to do it in a way that would prepare them for future phishing threats."