proofpoint.
Security Awareness Training

HEALTHCARE'S CYBERSECURITY KNOWLEDGE GAP

Phishing and other cyber attacks can hit anyone. But the stakes are especially high for healthcare firms. Successful attacks can interrupt clinical practices and jeopardize patient safety.

COST OF A HEALTHCARE BREACH

Healthcare breaches are far costlier than those in other sectors.[1]

$408 PER RECORD — **HEALTHCARE**

$148 PER RECORD — **AVERAGE**

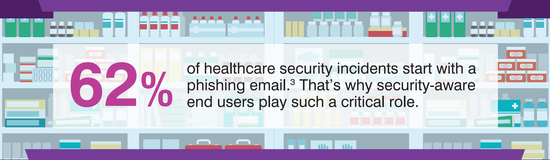
Breached hospitals also spend more to maintain their brand image and retain customers.[2]

38% Overall Providers

68% Breached Hospitals

Increase in Advertising Spend

ARE YOUR END USERS PREPARED?



62% of healthcare security incidents start with a phishing email.[3] That's why security-aware end users play such a critical role.

CRITICAL KNOWLEDGE GAPS

To measure healthcare workers' security awareness, we analyzed two key areas:

SECURITY AWARENESS ASSESSMENTS
We asked users nearly 85 million questions that spanned 12 major security topics.

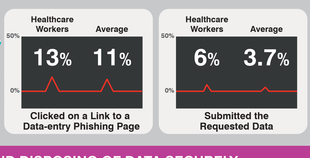
SIMULATED PHISHING ATTACKS
Our customers sent tens of millions of simulated phishing emails to their workers over a 12-month period.

WHAT WE FOUND

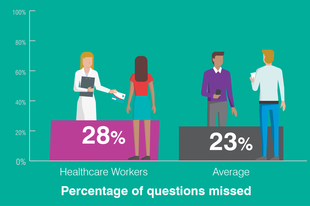
Healthcare workers are vulnerable to data-entry phishing

The good news: In simulated phishing attacks, only 8% of healthcare workers took the bait. That's slightly lower than the 9% average across all industries.

The bad news: Healthcare workers are more likely than most to enter sensitive data—including account credentials—when prompted.[4]



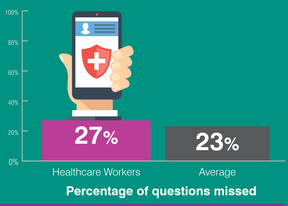
PROTECTING AND DISPOSING OF DATA SECURELY



Healthcare workers **missed 22% more questions than average** about the data lifecycle and handling personally identifiable information (PII)—despite the highly sensitive nature of the data they store and transfer.[5]

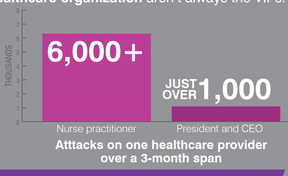
PROTECTING MOBILE DEVICES AND INFORMATION

Widespread use of mobile devices in healthcare makes end-user awareness critical to securing patient and company data. But healthcare workers show **below-average knowledge** of best practices.



HIGHLY TARGETED ROLES IN HEALTHCARE

Attackers target people in a wide range of roles and titles. The **Very Attacked People™ (VAPs) in a healthcare organization** aren't always the VIPs.



FREQUENCY OF SECURITY AWARENESS TRAINING

Lack of security awareness is a major problem for many healthcare firms. Here's what the 2018 HIMSS Cybersecurity Survey found:

NEARLY **52%** conduct training only once per year. That's too infrequent for knowledge retention and lasting changes in behavior.

MORE THAN **12%** either don't have a training program or don't know how often they conduct security training.

Reduce End-User Risk With Proofpoint Security Awareness Training

A comprehensive security awareness training program can make a big difference. Customers that have applied our anti-phishing tools and training have reduced their vulnerability as much as **86%**

LEARN MORE

www.wombatsecurity.com/himss-training-modules

1 Ponemon Institute. "2018 Cost of a Data Breach Study: Global Overview." July 2018.
2 American Journal of Managed Care.
3 HIMSS. "2018 HIMSS Cybersecurity Survey." March 2018.
4 Proofpoint. "State of the Phish Report." January 2018.
5 Proofpoint. "State of Security Education: Healthcare." February 2018.

0119-018