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

- Conduct training only once per year. That’s too infrequent for knowledge retention and lasting changes in behavior.
- 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%

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

- 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.

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.

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.

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

Healthcare breaches are far costlier than those in other sectors.

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

HEALTHCARE’S CYBERSECURITY KNOWLEDGE GAP

WHAT WE FOUND

- Healthcare workers are vulnerable to data-entry phishing.
- In simulated phishing attacks, only 8% of healthcare workers took the bait. That’s slightly lower than the 9% average across all industries.
- Healthcare workers are more likely than most to enter sensitive data—including account credentials—when prompted.

WHAT TO EXPLORE

- Security Awareness Assessments
- Simulated Phishing Attacks

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.

PROTECTING MOBILE DEVICES AND INFORMATION

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.

RESEARCH REFERENCES

2 American Journal of Managed Care.

www.wombatsecurity.com/himss-training-modules