What Is a Cybersecurity Training Platform & Does Your SMB Need One?

Devolutions

CYBERSECURITY SPECIALISTS SERVE AS A STRONG LAST LINE OF DEFENSE AGAINST HACKERS

Before they're cleared for takeoff, pilots spend many hours in flight simulators so they can develop their skills and knowledge, and to ensure they are prepared to handle problems and risks. In the same vein, a growing number of companies are enrolling employees in cybersecurity training platforms, so they can learn how to avoid cyber threats. Ultimately, these cybersecurity specialists serve as a strong last line of defense against hackers.

About Cybersecurity Training Platforms

A cybersecurity training platform is an online portal that provides employees with self-paced, hands-on, and skills-based threat detection and mitigation training in a live and dynamic simulated environment. These threats can include ransomware, phishing, DDoS, and so on, and the training program can be customized to cover specific topics, such as social engineering, email security, mobile device security, safe web browsing, safe social networking, protection of health information, etc.

Employees get immediate feedback on their decision-making and move forward through the training based on their performance. Managers can also log into a dashboard and monitor each employee's progress, and then identify an individual's strengths and weaknesses. For example, an employee may be competent in safe web browsing, but need additional training in mobile device security.

Cybersecurity Training Platforms for SMBs

In the "old days", hackers primarily targeted large enterprises and government agencies — because that was where the most valuable data was stored. However, over the last several years, hackers have turned their attention to SMBs, because they typically have weaker (and in some cases virtually non-existent) defense systems. According to Verizon's 2019 Data Breach Investigations Report, 43% of cyberattacks target small businesses, and research by the U.S. National Cyber Security Alliance found that 60% of small firms go out of business within six months of a cyberattack.

In light of these alarming statistics, SMBs should seriously consider investing in a cybersecurity training platform, so that their employees can effectively serve as the last line of defense instead of unwittingly opening the door for hackers. Naturally, there is a fee involved (typically an annual subscription based on the number of employees). However, considering the staggering costs and consequences of a breach — including lasting reputation damage — it may be well worth the investment. Think of it like an insurance policy.

Cybersecurity training platforms, such as those offered by Quebec-based Terranova and Proofpoint (which acquired Wombat Security in 2018), are geared towards general employees instead of cybersecurity experts. For example, employees learn about different types of attacks, how to identify them, and the proper steps to take if they suspect or detect a threat.

Terranova is the platform we use here at Devolutions and we are proud to do business with a Quebec company that provides a great service for SMBs who need to refine their cybersecurity skills.

All vendors offer a demo, and most have a free trial (although some aspects of the platform may be limited/restricted).

Share Your Experience

If your organization uses a cybersecurity training platform, or has used one in the past, please share your experience. Tell us what you liked, what you didn't, and what you think SMBs should do to keep their data, customers and reputations safe. Because as far as cyber crime goes, it's not getting any better out there. It's only getting worse.