TECHGUARD® S·H·I·E·L·D™

SECURE · HOLISTIC · INTEGRATED · EMPLOYEE · LEARNING · DEFENSES

Frequently Asked Questions

As you transition from your previous cybersecurity awareness training provider to TechGuard SHIELD, you may have some questions. You can be assured that our dedicated account representatives will help you step-by-step to ensure that your transition is as seamless and easy as possible. Here are some frequently asked questions:

1. Can we demo the training platform first?
    a. Yes, simply fill out the requested information and a dedicated account representative will contact you and give you access to a demo of our training platform.

2. How do we upload our user data to the SHIELD training platform?
    a. TechGuard makes uploading your user data an easy process. We give you the options to use Manual Input, Bulk Import, or LDAP Integration.

3. Does the SHIELD training platform offer the same topics covered in other training platforms?
    a. Compared to our competition, TechGuard SHIELD offers more courses across more topics. We focus on making our training easy to understand by our end users, so our training topics may appear different at-a-glance. Our aim is to develop customized training programs for our users that offer a wide variety, while maintaining relevance and specificity to our users' needs.

4. Does the SHIELD training platform come in multiple languages?
    a. Yes, our platform has 40+ courses with availability in 11 different languages to ensure that we can meet your multilingual needs.

5. Can we tailor/customize content?
    a. Our content is designed to align with specific compliance standards, so editing can potentially risk inconsistencies. While our training platform allows for you to add your organizations' policies and point of contacts, we do not allow for direct editing of our content.

6. Does the TechGuard SHIELD training platform come with a phishing simulator?
    a. Yes, our phishing simulator, PhishingReal, delivers real-world scenarios to your users. With over 70+ customizable email templates, we send out test links, attachments, or web-form phishing threats to your users. If a user clicks on the test threat, he or she is then sent to an educational landing page with in-line talking points. We can also automatically assign courses for remediation if the same users continue to fail these test threats. We then provide you with highly effective analytics so that you can identify susceptible users and compare performance over time.

7. Do learners get a certificate of completion when they finish a course?
    a. Yes, once they have satisfied the completion requirements of the course, they will receive an email with a certificate. They can also print their certificates from the Transcript section of our LMS.

8. I don't want to make targeted assignments or schedule courses throughout the year – I just want all of the content at once, like I have now. Can I do it that way?
    a. Yes, you can have the content all delivered at once; however, we have found that the best way to drive awareness and educate your users is to schedule your courses to be delivered throughout the year. This keeps your users thinking about cybersecurity on a more regular basis. This is the best way to create a security-conscious culture.

9. How often is your content refreshed or new content developed for the library?
    a. Our modules are reviewed in an ongoing manner to ensure they are aligned with the current cyberthreat landscape. We prioritize any needed updates based on each modules' usage and impact on our clients.

10. What's new/different?
    a. We use a comprehensive, programmatic approach to developing a security-conscious culture within your organization. We not only deliver over 40 courses with availability in 11 different languages, but we also deliver real-world training scenarios with our phishing simulator. Our content is highly interactive and engaging through gamification. With our world-class analytics, we can measure key security awareness competencies to identify gaps across your organization. We also provide you with 'managed services', which means we focus on building and maintaining your training program so that you can focus on what matters the most – running your business. You can be assured that we will make this transition process as easy as possible!
    b. Highly engaging, motivating and award-winning content proven to reduce cyber risk behaviors.
    c. Employee training analytics to measure key security awareness competencies to identify gaps across the organization. This drives the training strategy allowing for changes to be made to identify and address any cyber-risk gaps and to measure employee improvements.
    d. Available adaptive trainings allow personalized targeting of employee efficiencies when delivering "refresher" training. This allows your employees to pre-test their knowledge and have their training focused on their deficiencies instead of wasting time with the same content they have a solid understanding of.
    e. Our available rule-driven auto enrollment eliminates the burdens of self-managing a training program and allows for a more effective rollout. Trainings can be "daisy chained" in sequence to be assigned upon completion of the prior course. This provides our customers with an ongoing training program that is automated and customized.
    f. New updates and topics are released to keep pace with the ever-changing threat environment.

11. Why are there some courses covering same/overlapping topics?
    a. '*Multi-Topic Themes'* cover the full spectrum of foundational topics. They cover the major NIST standards and are ideal for annual training for all users.
    b. *'Single Topic Modules'* cover the same topics covered in the Multi-Topic Themes but are focused on one topic, in more detail and with interactive challenges. These are ideal for all users as a targeted reinforcement over time. These modules, layered with the Multi-Topic for all users, satisfy the Role Based & Compliance requirements for specific audiences.

c. *'Micro-Videos'* focus on sub topics with short (less than 5 minutes) and effective refreshers. These are ideal for all users as an on-demand/just-in-time reference. There are designed to be used as needed vs. assigned.

12. Can these solution packages be hosted on a third party LMS, do you support SCORM? Does it change feature availability?
    a. This is not recommended, but is available. We can deliver in SCORM packages; version 1.2 or 2004.
    b. When content is hosted on a third party, you take over as the manager of the system. Many of the Security Awareness features built into the SHIELD LMS would not available. This includes Threat Profile analytics and reporting, PhishingReal simulated e-mails & analytics, and Managed Services.
    c. Updating content as needed would become a burden on Customer's LMS team.
    d. The analytics/reporting and, of course, the 'Learner Center' would not be included, since they are specific to our LMS. Reporting capabilities would be the responsibility of the third party LMS.
    e. Our PhishingReal solution can only be deployed via SHIELD's LMS.