



TECHGUARD[®]
S ★ H ★ I ★ E ★ L ★ D[™]
SECURE · HOLISTIC · INTEGRATED · EMPLOYEE · LEARNING · DEFENSES

Frequently Asked Questions

As a Qualified AIG CyberEdge Policyholder, you get access to the complimentary cybersecurity awareness training provided by TechGuard Security. Whether you are transitioning from another training provider, or you are currently managing your own internal training program, we are here to help you with any questions or concerns that you may have. Utilizing this complimentary service is very simple, and very beneficial. Here are some Frequently Asked Questions (FAQ's) that we have received from other policyholders.

1. What is included with our complimentary cybersecurity awareness training?

- a. TechGuard Security provides a comprehensive training platform with over 40 courses, with availability in 11 different languages. In addition to our courses, we also provide a phishing simulator, and world-class analytics, giving your organization a true comprehensive cybersecurity awareness training platform.

2. How do we get started using this complimentary service?

- a. Getting started is easy, simply go to our registration page [here](#), fill out the required information, and one of our dedicated account representatives will reach out to begin the process. We will assist you with determining which courses your organization should take, and how often you want courses to be assigned. Essentially, we will go over all of the features of the training platform with you and help you build a training program that fits your organization the best.

3. Before implementing the training, can we demo the training platform first?

- a. Yes, to ensure that this complimentary training fits the needs of your organization, your dedicated account representative will not only show you all of the benefits of the platform via an initial presentation, but he or she will give you access to the full training program so that you can demo it yourself.

4. Once we are ready to get started, how do we get our users to the platform, and how do they access the courses?

- a. We make uploading your user data an easy process. You can get us your user list via manual input, bulk import (via CSV), or LDAP active directory integration. Once your users are added to the platform, they can access the training by simply logging in with the username and password that they create. We also provide the option to use Single Sign-On (SSO).

5. Can we add any of our own content or courses to the platform?

- a. Our content is designed to align with specific compliance and regulatory standards, so editing or adding content could potentially cause inconsistencies; therefore, we do not allow for editing or adding content.
- b. We do allow, however, for you to add your organization's security policies to specific courses via policy-linking.

6. Does the training platform come with a phishing simulator?

- a. Yes, our phishing simulator is designed to deliver real-world scenarios to your users. We have over 70 customizable templates – we will send out either test-links, attachments, or web-form phishing threats to your users. If an employee clicks on the threat, they are sent to a landing page with in-line points for education. If users continue to fail these test threats, we also have the ability to automatically assign courses for remediation. And of course, with our phishing simulator we provide highly effective analytics to not only identify your susceptible users, but compare their performance over time.

7. Do we have to manage the training program ourselves?

- a. No. With our training platform, we provide you with Managed Services – this means that we eliminate the headache and concern that comes with managing a training program because we do it all for you. We build and maintain your training program so that you can focus on what matters the most – running your business. We automate enrollment notification, assignment reminders, and reporting to management. We schedule your phishing campaigns, add new users to the platform, and ensure your organization is getting the most out of the training platform.

8. How do we track and measure the results of the training?

- a. We provide world-class analytics with our training platform. We have easy-to-use reporting options so that you can see which users have pass, failed, or not started/completed their training. With our analytics, we can identify vulnerabilities and gaps within your organization, and we can use that information to schedule courses for remediation.

9. Can we host the training on our own LMS?

- a. Yes, we can deliver the trainings in SCORM packages. If you want to host the trainings on your own LMS, keep in mind that many features of our trainings will not be available – this includes all reporting and analytics, our phishing simulator, and our ability to manage the training for you.
- b. If you would like to host the trainings on your own LMS, but would still like to utilize our phishing simulator, we can provide you with our phishing simulator at a discounted price.

10. Are there any special considerations for mid/large organizations?

- a. Our training platform is very scalable. We can help organizations with five users or several thousands of users. We can do this because of our internal processes and our ability to automate much of the training, phishing, and reporting.
- b. We also provide the ability to separate your organization how you see fit. We can create groups for different divisions, departments, roles, locations, projects, and more. You can have different groups take different courses and different phishing campaigns, and you can pull reports just for those specific groups.
- c. If you have multiple supervisors, that's no problem. We can send each supervisor reporting for their department.
- d. Because we email out enrollment and assignment notifications to your employees, and because we can automatically send out reporting to management showing which users have/have not completed the required trainings, we can ensure that even mid/large organizations are utilizing the training and have buy-in from the employees.

11. Does TechGuard Security provide us with any other complimentary/discounted services?

- a. TechGuard Security is a comprehensive cybersecurity firm. We focus on three areas that make up your cybersecurity program – People, Process, and Technology. Our cybersecurity awareness training covers the People portion of your program.
- b. We also can provide you with solutions for your Process and Technology – this includes review of policies and procedures to ensure compliance with regulatory controls and/or security best practice, internal and/or external penetration testing, vulnerability scanning and assessment, physical security assessment, social engineering, and more.
- c. As a qualified AIG CyberEdge Policyholder, not only do you get our cybersecurity awareness training complimentary, but you also get access to our other services with a 10% discount. If you are already having IT services like penetration testing and vulnerability scans performed, saving 10% is an enormous benefit. Don't just choose our training, choose TechGuard!