Step 1: Identify Manager Admin

Provide the **name** and **email address** of the user within your organization. The Manager Admin will have the ability to set up the Azure AD synchronization, set up Multi-Factor Authentication (MFA), or configure Federated Login for Single Sign-On (SSO). Manager Admins can also set up and manage Simulated Phishing Campaigns and update Dark Web Monitoring.

Send the name(s) and email address(es) of the user(s) who will have Manager Admin access in the ticket open with the Telesystem Service Delivery Team. Billing has already begun for the contracted services.

Telesystem Setup

Step 2: Dark Web Monitoring

1. Identify what domains you wish to be set up for Dark Web Monitoring by replying to the Telesystem Onboarding Ticket with the domain names.

NOTE: You can monitor up to 3 domains with the subscription. If you need more than three, additional monthly charges will be applied.

Step 3: Feature Setup

The following features will be enabled automatically for you:

☒ Yearly Security Quiz

☒ Weekly MicroTraining

☒ SRA - Once a year, we will do a security risk assessment based on NIST standards

☒ Leaderboards - Employees will be able to see where they stand for their security score

☒ Simulated Phishing Campaign – Employees will receive mock phishing emails to test their ability to identify phishing attacks. An initial campaign will be set up for you on a monthly basis

☒ Service Provider Contracts - repository to store your provider contracts

☒ DR Plan - repository to store your DR plan

☒ Security Incident - Consolidate platforms by logging security-related incidents into this portal

☒ Server Room Access – Consolidate platforms by logging people who have accessed the server room directly into this portal

Identify if you would like to use the default system policies for employees to acknowledge, or if you have custom policies you'd like to upload, or if you would like this feature left disabled.

☐ Other Policies - load your HR policies for employee acknowledgements

Reply to your Onboarding Ticket with the features you wish to enable/disable and send any Policies, Contracts and documentation you wish to make available within the portal at this time.

Step 4: Policies and Procedures

The platform comes with several pre-written security policies and procedures for your benefit. Please download and review them here.

Notify your Telesystem Implementation Coordinator if you want to use our policies, upload your own policies, or shut these policies off in our portal.

Step 5: Create Manager Admin Account

Manager Admin account(s) will be created by Telesystem at this time and the login information will be emailed to designated user(s). At this time, your onboarding ticket will be closed.

Customer Responsibility

Step 6: User Guide Downloads

User guides and training videos are available on the Resources page at https://telesystem.us. Here are some direct links that we think will be helpful:

1. Solution Overview Video
2. Portal Tour Video for Managers
3. Portal Tour Video for Employees
4. Manager User Guide
5. Employee User Guide
6. Whitelisting Instructions
7. Azure Active Directory Sync Instructions
8. CatchPhish Plug-in Information and Setup Guide
9. Phishing Campaigns Setup Guide

Step 7: Whitelist Our Domains

To ensure that all emails from the platform will be successfully delivered to your employees, you'll need to ensure that you have properly whitelisted the system IP Addresses and Domains.

Download the Whitelisting Instructions here.

Step 8: Employee Synchronization - Azure AD Sync

1. Download our Azure Active Directory Sync Instructions
2. Follow instructions to set up AD sync by setting up required Security Groups within your Azure Tenant.

Step 9: MFA/SSO (Optional)

The Security Awareness Training portal supports Multi-Factor Authentication (MFA) and Federated Log-In for Single Sign-On (SSO). If you wish to take advantage of these features, please download and follow the available guide to configure these options.

- Security Awareness Training Federated Login or Native MFA Setup Guide

Note: To complete the setup for MFA and/or SSO, you must have Manager Admin Access within the Security Awareness Training portal as well as admin access in your third-party integration platform (Azure, Okta, Google, etc)

Step 10: Communicating Training to Employees

Now that we are starting onboarding of your account, it's essential that you let employees know that you are implementing a threat mitigation and employee cybersecurity training service. We have pre-written an email for you. Download it here.

PLEASE SEND THIS EMAIL TO YOUR EMPLOYEES ASAP.

Please send this out to your employees within 24-48 hours of receiving your Manager Admin Account Setup.

Step 11: Welcome Email

You're ready to send login information to your users. To do this, log in to the Security Awareness Training portal with your Manager Admin credentials and follow these steps:

NOTE: If you wish to customize the Welcome Message that is sent to your users to include information such as how to use an Authenticator App for MFA Configuration or to notify them that SSO has been configured, go to the Directory Sync menu and enable "Use custom message". Then click on the "Welcome Message" button and modify the text as needed. You must do this before you send the "Welcome Message" to users on the "Employees" menu.

1. Go to "My Company" on the left-hand navigation pane
2. Go to the "Employees" menu
3. Check the box(es) in the first column for the corresponding row of the employee(s) you wish to notify, or click the box in the header row to select all users
4. Click on the "+ Actions" box and then select "Welcome Message". The portal will send an email to each selected user advising them that there is a new Cybersecurity Awareness Program that will include a link to set their initial password.
    a. The link in this email should only be used to establish the initial password. Users should then use https://portal.breachsecurenow.com/#/login for each subsequent login.

Step 12: Deploy Catchphish to Employees (Optional)

This Outlook plugin will allow your employees to mark suspicious emails and allow us to tell them if they caught one of our phishing emails or perhaps even a more nefarious real phishing scam. Not only does it allow a user to check suspicious emails, but it ALSO builds our weekly training right into Outlook. It's one of the hottest features of our platform. This tool only works on O365.

- Access the CatchPhish Setup Guide on how to deploy CatchPhish