QUICK-START GUIDE

ESET CYBERSECURITY AWARENESS TRAINING

Log in to ESET CyberCentral (your admin portal) and these links will take you to the user guide to get you right where you need to be. Be sure to check the end of this document for course descriptions.

What would you like to do today?

I'D LIKE TO ADD USERS AND ENROLL THEM IN TRAINING

1 Create groups and add targets (users)

Users who will be enrolled in training and be part of phishing tests (campaigns) are called **Targets**. You'll create a **Group** or (multiple groups), then add or synchronize your targets. You can add users manually, through CSV, or synchronize them with Microsoft 365, Active Directory, LDAP, and more.

USER GUIDE + VIDEO
Create groups & import targets

2 Enroll in training

There are two options for a comprehensive primary training course: **2023—All-in-one Security Training** & **2023—Gamified ESET Cybersecurity Awareness Training**. Both cover all the basic info that most people need in order to better protect themselves and their organizations, and provide a certificate upon passing the quiz, which satisfies insurance & compliance requirements.

+ TIPS

You can subscribe to additional courses for free, under **School** > **Content Library**. Once you've subscribed you can assign to these courses as well. See all course descriptions here.

You can also change your School settings prior to enrollment if you'd like to do any of the following:

- Change enrollment from username/password to **Token**. This means your students don't need to create a username and password to access training. Instead, any enrollment or reminder email will contain a unique link that gets them directly logged into to their School portal to take any courses and view certificates.
- Turn on automatic course reminders, which will go out weekly until the course is completed.

USER GUIDE
Enroll targets into a course

USER GUIDE
School Settings

I'D LIKE TO CONDUCT A PHISHING CAMPAIGN

1 Set up whitelisting/safelisting

Safelisting allows ESET simulated phishing emails to bypass your mail filter. In order for simulations to function properly, our IPs must be whitelisted in your spam filter. Some systems may require safelisting by headers to ensure our test emails are received by your users. See the Safelisting Basics guide below:

USER GUIDE + VIDEO
Safelisting Basics

You'll find instructions for various platforms in the sidebar after clicking the link above. If you use Microsoft 365 for email, the domains of the phishing templates you select also must be added to Microsoft Defender (up to 20 at a time). Follow the guide linked below:

USER GUIDE + VIDEO
Microsoft Defender Advanced Delivery

2 Create Campaign

Before creating your first simulated phishing campaign you may want to authorize your domain (or you can skip this and do it per campaign instead). If you haven't added your targets/groups follow Step 1 on the left.

Once you have created your first group and authorized your target domain(s), you are ready to create your first campaign. You may also want to browse, customize, and add phishing templates first.

We recommend turning *on* **Auto-Enroll failing targets**, which means if any of your targets click on a link, download an attachment, or reply to the phishing test email, they will automatically be enrolled in a course to teach them how to be more careful in the future. The courses entitled TEST FAIL are 5-minute refresher courses for this purpose. See descriptions here.

USER GUIDE + VIDEO
Creating a Campaign

What would you like to do today?

I'D LIKE TO GENERATE REPORTS ON PHISHING CAMPAIGNS AND/ OR COURSE STATUS

1 Choose your report

Go to **Reports** > **Report Generator** and choose the type of report you'd like.

- If you are reporting on a phishing campaign, choose By **Campaign** > **Summary Report**.
- If you would like to report on a training course status (who is enrolled, in progress or completed on any course(s), choose By **Course** > **Course Enrollment Report**.
- You can find additional descriptions of available reports below

USER GUIDE
Report Generator

2 To filter for certain groups or types of targets, click the Filters drop-down

Choose your target filters (such as location-based fields, roles, etc.) and/or select your Group(s) to include in this report.

3 Save the custom report settings (optional)

Turn on the slider to **Save Custom Options**, and give your custom report a name. If you do this, it will appear in the **Select Report** drop-down in the future.

4 Click Submit

You will view the details of your report. You can then click Save PDF or Email PDF in the top right corner.

+ TIPS

You can also create reports from other sources:

- Course reports for specific courses, by going to **School** > **Manage Content**, then clicking **View** next to any course you've assigned. You can save as **CSV**, **Excel**, or **PDF** from there.
- Phishing test reports can also be created from **Tests/Campaigns** > **Manage Tests** (or **Campaigns**) then click **View** on the far right. Scroll down to details and you can click **CSV** or **Excel** to create a report from here.

I'D LIKE TO AUTOMATICALLY ENROLL GROUPS IN TRAINING

1 Edit your group settings

You can have a group set to auto-enroll into a training course or courses, so that any time someone is added to the group (either manually or through auto-sync) the new target will automatically be enrolled. Go to Targets/Groups > Manage Groups, then click **Edit** in the drop-down menu on the far right.

2 Set up Auto Enroll

Click the Auto Enroll Settings tab. Click in the **Adding a Target Auto Enroll** field under **Group Event Triggers** on the right.

Click any course you'd like to have auto-enrolled for targets added to that group. You can click in the field again to assign more than one.

Click **Update Group** on the bottom left.

Anyone added to this group after you do this will automatically be enrolled in the course(s) you specified here.

I NEED TO VIEW MY LEARNERS' CERTIFICATIONS

Go to School > Certificates > Student Certificates. You can View, Download or Print from the drop-down menu on the far right.

You can also use the **Create Certificate** feature for any unique courses you've uploaded into the portal. Click below for more info:

USER GUIDE
Certificates

What would you like to do today?

I'D LIKE TO SEND OUT MICRO-LEARNING COURSES VIA EMAIL

Similar to setting up a phishing campaign, you can set up **Training Email Campaigns** to send out one time or on a scheduled basis. These just-in-time training emails have cybersecurity topcs that are contained entirely within the email, to make sure your organization stays informed and vigilant.

We also add short, more advanced-level videos weekly or bi-weekly on the latest topics in the cybersecurity world, from our global research team at WeLiveSecurity™.

A Set up a whitelisting/safelisting

Safelisting allows ESET training emails to bypass your mail filter. In order for simulations to function properly, our IPs must be whitelisted in your spam filter. Some systems may require safelisting by headers to ensure our test emails are received by your users. See the Safelisting Basics guide below:

USER GUIDE + VIDEO
Safelisting Basics

You'll find instructions for various platforms in the sidebar after clicking the link above. If you use Microsoft 365 for email, the training email domain (trainingemails.com) also must be added to Microsoft Defender. Follow the guide linked below:

USER GUIDE + VIDEO
Microsoft Defender Advanced Delivery

B Set up a training campaign

You start a training campaign the same way you would start a phishing campaign, by going to **Tests / Campaigns > Create Campaign**. Then click **Start** under **Training Campaign**. You may also want to browse, customize, and add **Training Email Templates** first. Click **Training Emails** under **Template Type** to filter just the training emails.

You can also choose new templates as you create a campaign, but browsing the template library first will allow you to view more detail and customer if you choose (or create your own).

See more info in the User Guide here:

USER GUIDE + VIDEO
Creating a Campaign

I'D LIKE TO INSTALL AN OUTLOOK PLUGIN TO REPORT PHISHING

A What is KillPhish™ and what does it do?

Allow your users to scan and report email threats using the included Outlook plugin, KillPhish™.

KillPhish™ is an advanced email threat protection add-in for Office 365. It scans known threats on Windows, Mac/iOS, and Android for Outlook Desktop, Web, and Mobile. It enables reporting phishing and other types of threats. Each inbox's risk profile is unique, and KillPhish can help expose security threat signs.

It gives a "score" within Outlook for how risky an email likely is, based on known bad actors, SPF records, IP addresses, domains, keywords, and more. It also allows users to click a Report button on suspicious email. This data is included in the Net Reporter Score you'll find in ESET CyberCentral, which you can use to gauge improvement over time, along with other data collected as part of your phishing campaigns.

B What devices/platforms is it compatible with?

KillPhish™ works on Microsoft/Office 365 mailboxes. It works on Outlook desktop, Outlook web app (OWA), and the Outlook app for mobile devices.

C How do I deploy it?

Follow the directions in the User Guide below:

USER GUIDE
Microsoft Add-In (KillPhish)

C What if we don't use Outlook?

There is also a lite version of KillPhish for Google Workspace:

USER GUIDE
KillPhish Lite

I NEED TO ADD MORE TARGETS BUT I'M OUT OF SEATS

A Deactivate or delete targets

If you have people who are no longer with your organization, you can delete or deactivate them to free up seats (up to 20% per year). If you are synchronizing users, this will be done automatically (for example with Microsoft Graph for Microsoft 365 or AD).

If you need to do this manually, go to Targets/Groups > Manage Targets, then click the triangle drop-down button on the far right of the target, the click **Delete** or **Deactivate**. If you deactivate them, you can later reactivate them if you have a free seat.

To delete or deactivate several at once, go to Targets/Groups > Manage Groups then click the triangle drop-down button on the far right of the group with the targets you'd like to edit.

Select all targets to edit by clicking the check-box on the left, then scroll to the bottom and click **Delete** or **Deactivate**.

B Purchase seats/enlarge your license

You can purchase additional seats/enlarge your license at any time up to three months prior to expiration. See the section on the right for instructions.

I NEED TO ADD ADMIN USERS TO THE PORTAL

1 Add admin users

You can add an unlimited number of admin users on your account. These are users who will access the admin platform to add users, assign training, run phishing campaigns, view reports, etc.

There are two levels of admin portal users: Admin & User. A User is prevented from seeing the Administration tab in the admin portal, but has access to everything else in the admin platform.

To add an admin account, go to Administration > Manage Portal Users, then click **Create** at the top right. Under **Type** choose **Use**r for limited access, and **Admin** for full access, and add their email and name.

Click **Save**.

+ NOTE

These are not users who will be enrolled in training and be part of phishing campaigns. Those are targets, and will be added under Targets/Groups.

I STILL HAVE QUESTIONS. HELP!

? How do I add users/licenses or renew my account?

If you will have a new total of <100 total seats, follow these steps. For 100+ contact your ESET sales partner or email cybertraining@eset.com if you don't have one.

1. Log in to the Admin portal.
2. Next to your company name, copy the alphanumeric **Username** (beginning with ECAT or ECA2).
3. Go to the ESET License Management page, paste the Username from step 2 and click LOG IN NOW.
4. Navigate to **License Management** in the top left corner. In the **License details** section click **Enlarge License**. Then type or click the + for the new total of **Devices** (users/targets).
5. Select the existing expiraiton date to enlarge your seat count, or the second expiration date to renew and enlarge with your new seat count.
   - For enlargements, you will pay the difference between existing and additional seats. If you are within 90 days of expiration, it will switch to a renewal instead. If you renew now we will add those additional licenses right away as well through the end of your license (up to 20% additional).
   - For renewals, enter the new total of seats, if different. Your account will be valid for an additional year from your original expiration, or one year from today if your account was already expired.
6. Click **UPDATE NOW**, then **PROCEED TO CHECKOUT**.
7. Verify your info (you may need to type the email associated with your account) then click **CONTINUE TO PAYMENT**.
8. Enter your payment information to process the order.
9. Your added seats or renewal will be processed within 4 business hours.

CONTENT LIBRARY COURSE GUIDE

The comprehensinve training courses and others are already in your account. **You can subscribe for free to additional courses by going to School > Content Library. Read descriptions of these to determine what's right for your organization below. See also the Course Flowchart for additional help in choosing.**

2023—ESET CYBERSECURITY AWARENESS TRAINING

FULL COMPREHENSIVE OPTIONS: 80-90 MINUTES, INCLUDES CERTIFICATE

Both options include best practices to protect yourself and your organization against today's cyber threats and crimes. These both fulfill requirements of the vast majority of insurance and compliance. Either course will resume where left off if unable to complete in one session.

OPTION 1: 2023—GAMIFIED ESET SECURITY AWARENESS TRAINING

This **gamified**, interactive training allows the learner to choose the order of topics and includes a reputation score, 5 mini-games to reinforce the learning, 5 scenarios, and a 14-question quiz.

OPTION 2: 2023—ALL-IN-ONE CYBERSECURITY TRAINING

This **linear** format is a more straightforward version of the training. It's structured in a blog style, plus animations, scenarios and interactions. If your organization completed the prior (gamified) version of the training, this one is recommended for the subsequent year, particularly if your insurance or compliance requirements need the training to be different each year.

Both options cover the following topics:

EMAIL
- Phishing
- Email Attachments
- Spam

INTERNET SAFETY
- Public Wi-Fi
- Staying Safe while Working Remotely
- HTTPS
- Web-content Filtering
- Search Engine Safety

PERSONALIZED THREATS
- Social Engineering
- Insider Threats

MALWARE
- Types of Malware
- Malware Targets
- Mobile Security
- How Malware Gets to You

PASSWORDS
- Use Strong Passwords
- Password Hygiene
- Password Management
- Two-factor Authentication

2023—ESSENTIAL SECURITY AWARENESS TRAINING

30 MIN, INCLUDES ESSENTIAL CERTIFICATE

This course program is designed for organizations who are limited in training time or only need to cover the basics. It includes just the animated video and a knowledge check question for the following topics, plus a 5-question Quiz at the end:

This is a **course program**, meaning it's a collection of mini courses. As such, your users will be assigned each course, but will see their progress as they go and be guided through each. It includes:

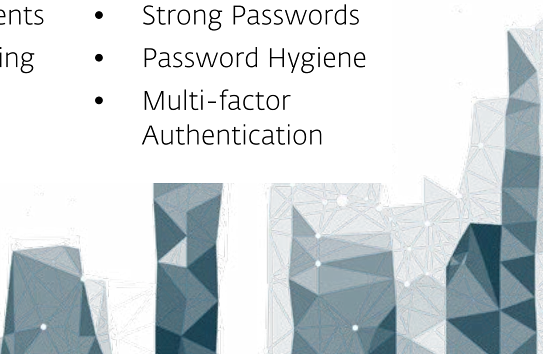
- Phishing
- Social Engineering
- Insider Threats
- Malware
- Secure Browsing
- Strong Passwords

2023—EXPRESS SECURITY AWARENESS TRAINING

50 MIN, INCLUDES EXPRESS CERTIFICATE

This course is an abbreviated version of the All-in-one Cybersecurity Training. While a full story can help engage learners and increase retention, for organizations that don't have the 90 minutes to allot for training and don't need to cover all the topics, this course is a great option. It includes:

- Phishing
- Email Attachments
- Social Engineering
- Insider Threats
- Malware
- Secure Browsing
- Strong Passwords
- Password Hygiene
- Multi-factor Authentication



PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

FOR ORGS THAT HANDLE PII
10 MINUTES

- Introduction to PII
- What is Personally Identifiable Information (PII)?
- Why is it important to protect PII?
- How to protect PII

MINI COURSES / PHISHING TEST FAIL COURSES

COURSES TO ASSIGN AUTOMATICALLY FOR REFRESHERS OR AS PHISHING SIMULATION TEST FAILS
3-5 MINUNTES

These Mini Courses are also part of the comprehensive training courses, and don't need to be assigned to users as part of their regular enrollment if you enroll them in one of the comprehensive training courses.

The Phishing Test Fail mini courses are ideal to use when setting up a phishing campaign for course auto-enrollment. So when a target (learner) clicks on a link, downloads an attachment, etc. in a phishing test, they will immediately learn how to avoid this mistake on an actual phishing scam.

- **PHISHING TEST FAIL—Email attachments**
  Recommended for targets who click on an attachment
- **PHISHING TEST FAIL—Phishing**
  Recommended for targets who click on a link or reply to a phishing test email
- **PHISHING TEST FAIL—Social Engineering**
  Recommended for targets who enter information in phishing tests that include a splash page (such as a mock login page)

The other Mini Courses can be assigned whenever you'd like to refresh a certain group or all employees on a particular topic, or if you chose an express course and would like to add a few topics to what is there. You can subscribe to them for free by going to **School** > **Content Library / Store**. Search for **Mini Course** at the top, then you can **Preview** or **Subscribe** (for free) to any you'd like to enroll.

MINI GAMES

GAMES THAT CAN BE ASSIGNED AS YOU PLEASE TO KEEP EMPLOYEES SHARP
5-8 MINUTES

These 5 Mini Games are part of the Gamified ESET Security Awareness Training. They can be assigned as a refresher game for a certain topic, or in addition to any non-gamified training course as a fun way to reiterate a topic and help it stick.

You can subscribe to them for free by going to **School** > **Content Library / Store**. Search for **Mini Game** at the top, then you can **Preview** or **Subscribe** (for free) to any you'd like to enroll.

Games include:

- Blast off to Defend Against Social Engineering
- Choose Strong Passwords to Protect Your Top-secret Information
- Protect Atlantis from Phishing Attacks
- IoT and Remote Work Data Detective
- Keep Your City Safe from Malware Attacks

ADVANCED BONUS MATERIAL

45+ 5-MIN VIDEOS

Videos from our security experts on the latest security threats and news for advanced users. Search for **Advanced Bonus Material** in the School Library in order to subscribe and enroll.

Videos from 2023 have been moved to **Training Emails** (Micro-learning email courses).

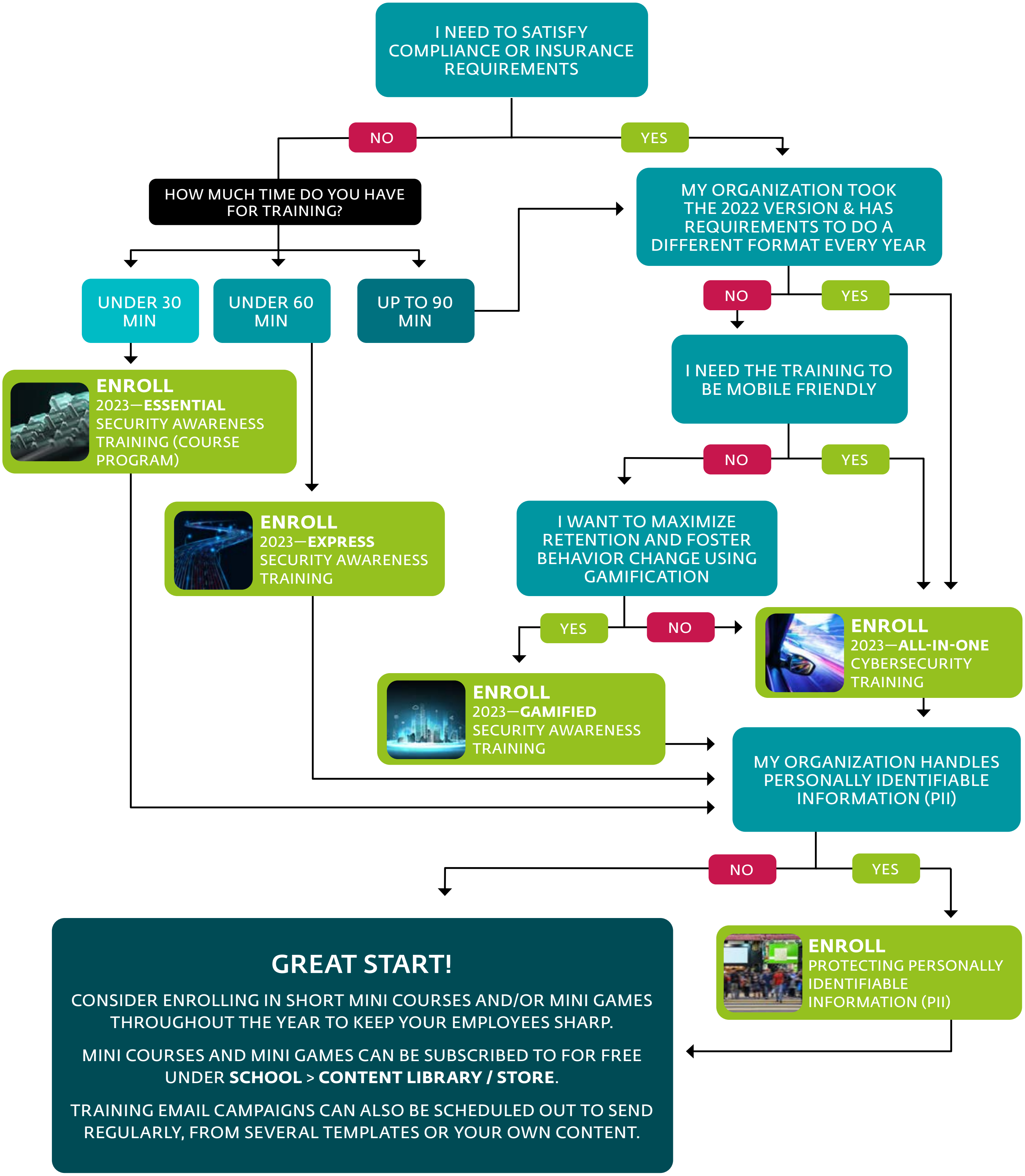
ADDITIONAL OPTIONAL COURSES

5-10 MINUTE OPTIONAL COURSES

- Ransomware
- Spear Phishing
- Wi-Fi
- Credential Theft Protection
- Password Security

COURSE FLOWCHART

HELP ME CHOOSE WHAT COURSE(S) TO ASSIGN



I NEED TO SATISFY COMPLIANCE OR INSURANCE REQUIREMENTS

NO → HOW MUCH TIME DO YOU HAVE FOR TRAINING?

- UNDER 30 MIN → **ENROLL** 2023—**ESSENTIAL** SECURITY AWARENESS TRAINING (COURSE PROGRAM)
- UNDER 60 MIN → **ENROLL** 2023—**EXPRESS** SECURITY AWARENESS TRAINING
- UP TO 90 MIN → MY ORGANIZATION TOOK THE 2022 VERSION & HAS REQUIREMENTS TO DO A DIFFERENT FORMAT EVERY YEAR

YES → MY ORGANIZATION TOOK THE 2022 VERSION & HAS REQUIREMENTS TO DO A DIFFERENT FORMAT EVERY YEAR

- YES → **ENROLL** 2023—**ALL-IN-ONE** CYBERSECURITY TRAINING
- NO → I NEED THE TRAINING TO BE MOBILE FRIENDLY
  - YES → **ENROLL** 2023—**ALL-IN-ONE** CYBERSECURITY TRAINING
  - NO → I WANT TO MAXIMIZE RETENTION AND FOSTER BEHAVIOR CHANGE USING GAMIFICATION
    - YES → **ENROLL** 2023—**GAMIFIED** SECURITY AWARENESS TRAINING
    - NO → **ENROLL** 2023—**ALL-IN-ONE** CYBERSECURITY TRAINING

MY ORGANIZATION HANDLES PERSONALLY IDENTIFIABLE INFORMATION (PII)

- YES → **ENROLL** PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII) → GREAT START!
- NO → GREAT START!

GREAT START!

CONSIDER ENROLLING IN SHORT MINI COURSES AND/OR MINI GAMES THROUGHOUT THE YEAR TO KEEP YOUR EMPLOYEES SHARP.

MINI COURSES AND MINI GAMES CAN BE SUBSCRIBED TO FOR FREE UNDER **SCHOOL** > **CONTENT LIBRARY / STORE**.

TRAINING EMAIL CAMPAIGNS CAN ALSO BE SCHEDULED OUT TO SEND REGULARLY, FROM SEVERAL TEMPLATES OR YOUR OWN CONTENT.