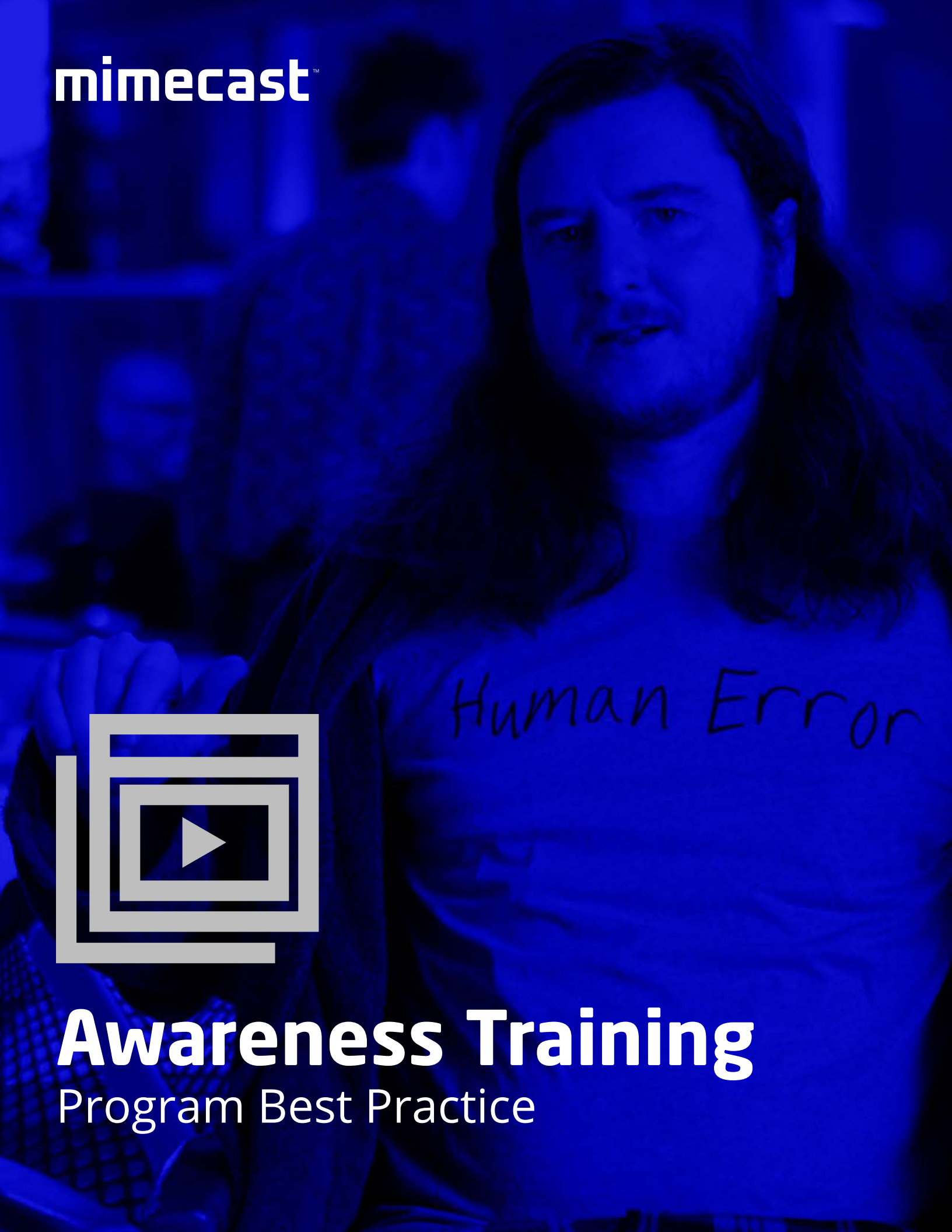
mimecast™



Awareness Training

Program Best Practice

Our Value Proposition

Research shows that 90%+ of breaches involve human error[1], and in 2018, organizations faced a 27% chance of suffering a major data breach involving 10,000 records or more[2]. Those types of massive breaches came with an average cost of four million dollars each to remediate.[3] Clearly, human error is not to be taken lightly. People are – and likely always will be – the weak link in the chain. Yet, efforts to reduce the risk they represent are failing. Organizations are pouring billions into **security awareness training**, but these investments are not translating into results. In fact, the probability that companies of all types and sizes will experience a security breach is greater today than it was yesterday. Something needs to change.

We believe harsh reprimands towards employees without context are not the way to tackle human error and change behavior. Instead, it's imperative to capture hearts and minds to change an employee's view of security from something they have to do (compliance) to something they want to do (commitment).

Our security awareness training program is designed to change behavior, improve knowledge and retention of core security issues, and ultimately lower risk. The punch line is training that takes 2 to 3 minutes a month, a tolerable ask of today's busy employee.

Implementing Mimecast Awareness Training with our recommended best practices has proven to change user behavior. Users at companies that don't have Mimecast Awareness Training are 5.2 times more likely to click on bad links.[4]

The Approach

Mimecast Awareness Training is successful for employees, the organization, and business leaders when broken down into these five stages.

This strategy can be broken down into five stages:

1. **Analyze –** Know your company's strengths, weaknesses, threats and opportunities (SWOT) for a successful security program.
2. **Create –** Create the plan and set the annual goals for your awareness training program.
3. **Implement –** Implement the plan with a detailed approach, engaging your users and stakeholders.
4. **Evaluate –** Evaluate your plan and make corrections where needed to be successful.
5. **Repeat –** Repeat step 1 – 4

---

1 Verizon Data Breach Investigations Report 2018 2-4. Mimecast 100 Days of Coronavirus Report 2020

Stage 1 - Analyze

Without analysis, it's impossible to determine what training is necessary, and how you should be testing that training on an ongoing basis.

1. What does your company do (i.e. industry, mission statement, etc.)?
2. How does your company deliver its products (i.e. distribution such as SaaS, professional services, retail, etc.)?
3. What does your supply chain look like today (i.e. outsourced, 3rd party goods, etc.)?
4. What regulatory/compliance requirements do you have meet? (SOX, ISO, NERC, etc.)?
5. How do your employees work today (i.e. 100% remote, in the office or a combination of both)?
6. What do your employees use to complete their work (i.e. mobile devices, Macs/ PC, IoT devices, etc.)?
7. How do your employees communicate daily (i.e. email, IM, social media, snail mail or all the above)?
8. How would define your leadership structure (mechanistic or organic)?

Now, shift focus to your 'threats'. Ask yourself the following:

1. What is the largest security challenge your company has faced in the last year (phishing attacks, ransomware, lost/stolen equipment, insider threat, wire fraud, etc.)?
2. Which department has the most public exposure?
3. Which department has led to the most security headaches?
4. Which medium has led to the largest number of incidents (email, USBs, social media, etc.)?

Combining information from your 'opportunities' and 'threats' helps create a solid foundation for your training program.

Take this example:

Bob works in the retail industry with a largely mechanistic leadership. Most of his employees use point of sales (POS) systems in the U.S. A number of incidents with ransomware have originated via email to the sales team.

Bob can apply that information to build a program that focuses on PCI, phishing attacks and general cyber hygiene.

Keep in mind, **security awareness training** is not complete with three modules or a one-time deployment.

Stage 2 - Create

"Now that you have completed an analysis, it is time to create the security awareness training plan. To generate a plan, you must convert the items you identified in the SWOT into a sequence of goals. Each goal should have an expected outcome that is measurable quantitatively or qualitatively.

In this context, quantitative goals refer to how much of your organization is completing the training and how quickly are they doing it. You cannot give merit to qualitative goals without achieving a higher result quantitatively. Why? Because, ultimately an attacker only needs one person to click one link to take advantage of your org. Presumably, anyone who has not taken the training is unqualified to keep your organization safe.

> *"**90% of the organization** will complete their monthly training modules by Q3 of our fiscal year"*
>
> *"**70% of employees completing their monthly training** will do it by week 2 of every month by Q4 of our fiscal year"*

Here are two quantitative goals you can set for your organization:

To achieve your quantitative goals, you will have to engage end-users in new ways (bottom-up) and obtain support from company leadership (top-down). Remember, this is a program meant to engage people and not merely an automated playlist of training videos. That means hosting town halls, sending memes and more importantly, spotlighting employees that are security champions. To gain the support of leadership, ensure you describe your program as a carrot vs. a stick meaning education vs. punishment. Dedicate time to focus on getting quantitative numbers up before you move on to qualitative goals.

When you select quantitative goals and associated metrics, plan to implement your program and evaluate it. Over time you will reach an inflection point where your qualitative goals and their metrics are representative of your security posture and user risk.

> *"**Less than 10%** of the organization will fail the awareness training by Q1 of our fiscal year"*
>
> *"**Less than 5%** of the organization will click on potentially malicious links by end of Q3 of the fiscal year"*

As we've already outlined, qualitative goals measure how secure your organization is based on employees' knowledge of the training and how they respond in practical situations. To accurately measure your qualitative goals, you need to define your company's baseline security knowledge, then continuously evaluate how you can help the organization pivot to being a security champion. Here are two examples of qualitative goals:

Now that you've identified the goals for your security awareness training plan, let's talk about your approach. We recommend continuous micro-trainings released on a monthly cadence. These micro-trainings keep your employees' attention. It also means you have a mechanism to continuously measure engagement. If the trainings are humorous and short, like Mimecast Awareness Training, a monthly cadence will have no impact on productivity or the employee's time. Ideally, you should send the trainings for one quarter before you begin your qualitative measures, such as phishing simulation.

To see maximum success, you should augment with materials that reinforce the trainings. One example is sharing memes over several communication channels at the same time. You could also put posters of the training videos up around the office, in a Slack channel or email at the beginning of the month to offer further discussion on the training.

To measure your qualitative goals we recommend launching a quarterly phishing simulation campaign. Your first campaign should be used as a baseline and not shared with the business. We recommend launching a campaign after your first three trainings, and every three months following. You should share the results not only with your leadership, but with the business to guide discussions on how various business units are performing. If you find a unit performing poorly, remember to use a carrot instead of a stick approach. Reach out to the business leader first as they could be the root of positive change.

Now it's time to lay out your security awareness training plan. Use your analysis from Stage 1 to augment this plan with **appropriate topics**. *Ideally, your first year would look something like this:*

1. **Phishing**
2. **Industry Specific Training (like PCI or HIPAA)**
3. **Threat your company has been dealing with (like ransomware)**
4. **Password Protection**
5. **Phishing (Whaling)**
6. **Information Protection (Stolen/Lost equipment)**
7. **Social Media Posting**
8. **Privileged User**
9. **Insider Threat**
10. **Shredder Usage**
11. **Unvetted App Download**
12. **Phishing (Holidays)**

Stage 3 - Implement

Now that you have a solid analysis and goals it's time to implement your plan. We recommend a time-based approach that looks something like this:

1. Set up all of the modules to be sent out over the next 12 months based on your SWOT.
2. Deploy the phishing reporting button.
3. Send an email to your leadership team to let them know you are deploying security awareness training, highlighting that training is often an industry requirement. But more importantly, convey how through the program you and your team will report on key insights into how the company is defending their IP, how it saves employees time, and guidance on how you can continue to improve.
   Clearly lay out your plan of offering one micro-training per month. Each training takes less than five minutes which equals to less than one hour of training a year. Ultimately, this offers more value than one massive training session that employees are unlikely to retain.
   Show your leaders the training modules that you're planning to release and talk about the quarterly assessment (phishing simulation) that measures how your company would fare against a phishing attack.
4. Talk with them about how their support will help improve security posture by achieving quantitative goals (getting employees to take the training quickly after they're sent).
5. Send an email to all employees to let them know about their new monthly training. Explain the process and how the organization will measure the training, including the goal of all employees completing the monthly training quickly. Also, be sure to share details about the phishing reporting button that you've deployed to their Outlook clients.
6. Send the first training followed by posting memes around the office. Remind employees the training is live via internal communication channels.
7. At the end of the first week, send a report to the company reporting how many people have taken the training.
8. At the end of the second week, create an email that another leader can send sharing how much of the organization has completed the training.
9. At the end of week three, send another update. If you can, show which departments have the highest completion rate to create friendly competition.

10. For month two, send an email providing information about new training for the month, and highlight the positive takeaways from trainings in the previous month. Share enthusiasm for successes and completion rates, and continue to send memes and post them in visible areas. Finally, keep the metrics from last month, as you will need them for trending data.

11. On month two, week two send a status update to the company to remind them to take the training, share the overall completion rate and highlight departments with high completion rates. Notify any leader directly if their department has a below-average completion rate.

12. For month three, send a note talking about the new training for the month, but also highlight the positives of how the training went the last month and the completion rate. Send the memes and post them in visible areas. Keep the metrics for last month. (You will need this for trending).

13. In the middle of month three, send your first phishing campaign. Use a phishing template that matches the threat covered in the topic for your month two training. Schedule the campaign to last the final two weeks to the close of month three.

14. For month four, send an email providing information about new training for the month, and highlight the positive takeaways from trainings in the previous month. Share enthusiasm for successes and completion rates, and continue to send memes and post them in visible areas. Finally, keep the metrics from last month, as you will need them for trending data.

15. Schedule or attend a leadership meeting to discuss your program's performance against your quantitative goals. Be sure to include requests for support from leaders whose departments could help you close gaps.

    Also, use this time to prepare your leadership for qualitative goals (click through rates). Ask them how they want to handle repeat offenders (who clicked a link in the phishing campaign). Give them the options of additional mandatory training, policy restrictions such as browser isolation, or discussions with their managers. The key here is an agreement with leadership, and that may require a follow-up meeting.

16. For month five, send an email providing information about new training for the month, and highlight the positive takeaways from trainings in the previous month. Share enthusiasm for successes and completion rates, and continue to send memes and post them in visible areas. Finally, keep the metrics from last month, as you will need them for trending data.

17. For month six, send a note talking about the new training for the month, but also highlight the positives of how the training went the last month and the completion rate.

18. In the middle of month six, send your second phishing campaign. Use a phishing template that matches the threat covered in the topic for your month five training. Time box the campaign to last the final two weeks to the close of month six.

19. For month seven, send an email providing information about new training for the month, and highlight the positive takeaways from trainings in the previous month. Share enthusiasm for successes and completion rates, and continue to send memes and post them in visible areas. Finally, keep the metrics from last month, as you will need them for trending data.

20. Schedule or attend a leadership meeting to discuss your program's performance against quantitative and qualitative goals. Discuss areas of weakness and share your recommendations on how to handle them.

21. Schedule office hours or a town hall to discuss the results of the phishing campaigns. Take time to review the templates used and share what users should have looked out for. Remind users about the phishing reporting button and highlight users who were early reporters of the phishing campaigns. Ask those users to speak about what they thought was suspicious.

22. Repeat steps 19 - 21 until the end of the program for the year. However, you can change the order of your remaining training modules, should environmental factors or geopoltical events give you just cause.

Stage 4 - Evaluate

You've done it! You've run an entire year of training, and now is the time to evaluate how you performed. First, revisit your SWOT to evaluate the 'strengths' and 'weakness' of your program. Next, review how your employees performed against your quantitative and qualitative goals. Didn't hit your goals? Don't be discouraged; a security awareness training program is about continuous improvement.

An evaluation is your opportunity to pull in input from your employees. Be sure to get feedback from superstars and those with low participation. Ask them what they liked, what they disliked, what they want you to do more of, and what they want you to stop.

This information is important as it may help identify larger issues standing in the way of hitting your goals. Some examples may include employees who didn't take the training because they cannot reach the platform given their limited computer access in their role.

Maybe your company uses a volume of contractors who sit on someone else's network. Likewise, turnover could mean that you have stale records in your active directory. Your metrics are not only meant to drive success but also identify issues that speak to broader security problems.

Stage 5 - Repeat

Now that you've completed the first year of your security awareness training program, you're probably wondering where to go from here. That's a great question! For year two (and every year following) take what you've learned so far and start back at Stage 1. You now have more details and understanding for your SWOT analysis. What's more, you have successfully established a security awareness program that has won the hearts of your employees and trust of your leadership! Go you!

Conclusion - Retain the Dazzle!

When you follow these steps your employees become more engaged and enthusiastic, and they'll become an extension of your security team. Remember, security is a team sport which requires the hearts of your employees and the minds of all. So when do you know that you're successful? One way to tell would be when your employees recognize threats, and share their knowledge - for example, not clicking on malicious items - with others in the office, creating community defense. Another way is when employees take their best practices home to train their families. More importantly, it is when your company as a whole is excited about cybersecurity!