Security Awareness Training For Large Enterprises

- Six common pitfalls to avoid when delivering Security Awareness Training to thousands of employees
- Six best practices in successful enterprise-level Security Awareness Training

MetaCompliance®

Six common pitfalls to avoid when delivering Security Awareness Training to thousands of employees

MetaCompliance®

1 Same old, same old for everyone

Not all phishing campaigns are created equal; role-based phishing is used in spear phishing and sophisticated social engineering scams. Demarcation of roles in larger organisations means that Security Awareness Training should also have a **role-based focus**. By tailoring security awareness and phishing simulation exercises to fit the types of attacks that focus on specific roles, such as CEOs and Accounts Payable, you are more likely to keep the training relevant and focused. When it comes to awareness training, a one-size-fits-all approach is likely to leave numerous vulnerabilities across the company.

A vital aspect of any training, including role-based, is to provide contextual material after a simulated phishing campaign. Training is most effective when people understand the whys and wherefores of an education event. Provide supplementary training to ensure the outcome of a simulated phishing exercise is understood.

2 Boring security training modules and inconsistent Security Awareness Training

Make the training engaging and less of a chore. Any program of education, including security awareness, is more likely to be a success if the trainees are interested in the materials on offer and those materials are relevant.

Make training modules **fun and entertaining** by using a variety of content. Interesting and engaging video games are winners amongst employees. You can use spoofs of well-known shows to create *Line of Duty*-style video series that go through security scenarios to add interest and engage learners. Cyber Security Awareness Month runs throughout October each year.[1] Some companies like to create special Security Awareness Training videos and **posters** that coincide with that year's theme, e.g. in 2021, the theme was 'Think Before U Click'.

Furthermore, consistency is an important aspect of human behaviour; consistency helps to form bonds and build trust; and consistency provides a way for humans to build mental models that they can rely on. Therefore, regular training that follows recognisable and engaging modules is more likely to succeed.[2]

3 Unrelatable training material and language issues

Successful Security Awareness Training is an interactive experience. The use of point-of-need learning experiences ensures that employees are given instructions on where they went wrong, and how to rectify it at the point of a dangerous interaction with a phishing message or other simulated attack.

Another important aspect of creating relatable awareness materials is to connect training to current events. For example, during the height of the COVID-19 pandemic, large phishing email campaigns were created that mimicked World Health Organization (WHO) emails, using the brand to trick the public. More recently, the war in Ukraine has been used in a similar way, with cybercriminals creating Ukraine fundraising scams. [3]

For multinationals with hubs, operations or offices all over the globe, a key challenge is to provide campaigns in the user's native language. Too often, vendors rely on poorly translated content, using automated tools that do not consider subtle differences in the local culture. If an employee doesn't wholeheartedly understand the training, they can't be expected to follow it.

4 Stuck in the same cyber attack pattern

The cyber security attack landscape is never static. Cybercriminals are always changing techniques and tactics to make their cyber attacks successful. Using the same thinking, do not be afraid to adjust things as the cyber-threat landscape changes. Adjust your simulated phishing campaigns; add new cyber attack tactics into the training; and ensure that the education fits the types of attacks being used against larger organisations.

5 Who is responsible for the training?

This is a challenge that can cause internal debate. Who should be running the training? IT or HR? Security Awareness Training is not a one-stop program. It needs to be carried out on a regular basis; analysis of results must be carried out; and support of employees and 'repeat offenders' who struggle to take the training on board must be offered. Co-operation in designing and managing Security Awareness Training may be the right answer for your organisation. The use of specialist third parties can be of benefit in handling the training and providing the know-how to make sure it is a success.

6 Closing the door to Incident Reporting

Employees must feel confident enough to report a security incident. Larger organisations need to work on this and encourage incident reporting to ensure that IT teams have the time and the appropriate details to respond to a threat.

Six best practices in successful enterprise-level Security Awareness Training

What if you are a larger organisation with multiple employees, across multiple branches and departments, with many employees working remotely, travelling or working in home offices? Just how do you train your staff at scale to be secure?

Add to this mix a large supply chain ecosystem, as both a supplier and a consumer of supplies, and you have a perfect storm for a cybercriminal to exploit. The way forward in successful Security Awareness Training at scale is to use the following six best practice principles.

MetaCompliance®

1 Localise training across departments and branches

Build Security Awareness Training programs that map to your own company structure. Plan your awareness campaigns to reach every position in your organisational chart. Design these programs to reflect the roles of the departments that are at risk, and target bespoke training around these risks.

To localise training, MetaCompliance offers training in 35 different languages, with support for even more languages coming soon. These additional language versions are all created by native speakers to ensure that the translation is correct. Across all supported languages, MetaCompliance offers all of our eLearning content with linguistically accurate audio and subtitles.

2 Make it personal and make it stick

Personalised Security Awareness Training more closely mimics the real-world use of spear phishing. Personalised training programs can be configured using advanced security training platforms. These systems create tailored **phishing simulations** and other security training modules that closely reflect the personal situation of a given employee. In addition, be sure to personalise and brand the training as your own. If staff can see that the training has been issued by the company they work for, they are more likely to be receptive to it.

3 Short blasts of education

Regular training, with a bite-sized approach to delivery of material and modules, is a successful strategy to adopt in Security Awareness Training. The short, sharp blast of training prevents training fatigue. Again, having these short-burst modules in a variety of languages is ideal for large corporations that may have many multilingual speakers around the globe.

4 Automate Security Awareness Training with detailed reporting

By automating your **Security Awareness Training** program, you create a more effective training process while freeing up a substantial amount of your time. Benefits of automated Security Awareness Training include being able to quickly scale your training without additional resources and allowing you to schedule an annual campaign to ensure continuous learning, all year round. Plus, with the detailed and sophisticated reporting that accompanies an automated platform, you can prove a high level of engagement amongst employees.

5 Make Security Awareness Training consistent and regular

Many organisations fail to deliver regular Security Awareness Training throughout the year. Automated Security Awareness Training creates an engaging learning experience for employees, all year round to ensure cyber security threats stay top of mind. Using a "set it and forget it" approach, automated security training helps to save time and resources. This is a proactive and organised way of carrying out effective training programs, as opposed to hoping that an ad-hoc approach to training will be enough.

6 Give your Board a 'Return on Investment' (ROI)

The measurement of a program's success is crucial to determine its success or failure, yet security and risk management leaders often struggle to justify their organisation's investment. Budgets are tight, and it is important to prove that Security Awareness Training works. By using a platform with a reporting suite that captures data from the thousands of employees who are carrying out the training, you can prove compliance obligations have been met, demonstrate improvements in cyber security-related behaviours and, most importantly, provide an ROI to your Board.

Conclusion

A final statement from an **(ISC)² report** sums up the situation regarding Security Awareness Training:[4]

> ...the lack of security awareness and skills among all employees remains the **number one security challenge for organisations**. To alleviate this shortage, cyber security professionals agree that **6 out of 10 employees** would **benefit** from **security training** and/or **certification** for their jobs.

Going a step further, it is important to give employees the tools to protect themselves and their company, but this must be done to maximise success. Security Awareness Training at scale is no mean feat in itself. En masse training of employees in any area is complex, but cyber security can be a dry and boring subject that can easily lose the audience if done badly. By following the six best practices here, and avoiding the pitfalls of poor Security Awareness Training, even the largest and most dispersed organisations can slam the corporate doors shut on cyber crime.

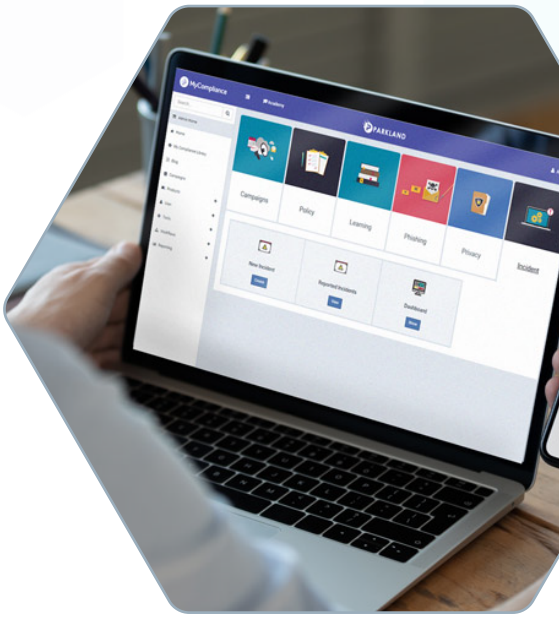
Out of pitfalls come best practices! Here are six important things to do to ensure your Security Awareness Training at scale works.

In Summary – Checklist

- ✓ Save time and enhance organisational resilience by engaging employees with automated cyber security training, all year round.
- ✓ Personalise Security Awareness Training and incorporate a variety of styles and formats to capture the attention of end-users.
- ✓ Create tailored and targeted cyber security training courses that are specific to your organisation's needs and culture.
- ✓ Deliver digestible bites of cyber security training in short bursts to avoid user fatigue.
- ✓ Use reporting to demonstrate regulatory requirements have been met and prove that the security awareness program is improving end-user behaviours.
- ✓ Increase employee engagement, completion rates and retention, with localised content.

With over 15 years' experience, and with corporate, household-name clients all over the world, MetaCompliance are specialists when it comes to providing cyber Security Awareness Training at an enterprise level. We know what it takes to provide effective training to thousands or even tens of thousands of employees.

Put us to the test and see for yourself – **request a demo today**.



info@metacompliance.com

www.metacompliance.com

Source references

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month
[2] https://www.routledge.com/Consistency-in-Cognitive-Social-Behaviour-An-Introduction-to-Social-Psychology/White/p/book/9781138851214
[3] https://www.bbc.co.uk/news/technology-60836962
[4] https://www.isc2.org/Research/Workforce-Study