10-point checklist

for choosing the right security awareness training solution

COPEAR
GLOBAL COMMUNICATIONS

Choosing the right security awareness training solution

Security Awareness Training is essential for protecting your organisation from damaging breaches. Not all SAT is alike, however.

This document will help you understand what to look for when comparing SAT software, and guide you in choosing the right provider to fit your needs.

☐ Gap analysis

Gap analysis, otherwise known as a gap questionnaire, will test your end-users for their existing knowledge in the core security areas. A gap analysis is useful for many reasons:

- Lets you know the current state of security awareness amongst your users
- Tells you which areas are in most dire need of improvement
- Allows you to compare progress later and see if your security awareness training is actually effective.

☐ Individually tailored courses

The knowledge and awareness levels of your end-users are likely to vary greatly. Making users with existing knowledge cover the basics again will not only make them less likely to engage in the future but also costs you time and money.

A smart security awareness training programme will use the results of a gap analysis questionnaire to individually tailor courses to make them as relevant as possible to each of your user's needs.

☐ Threat simulation

Threat simulation is an essential part of security awareness training as it will allow you to test your end-users in real-world scenarios. A simulated phishing tool with realistic templates can be used to see if your users are prepared to counteract phishing attempts.

Simulations are also useful for seeing how much of their training your users have internalised, as you can test them again sometime after they have started their training to know if their threat detection skills have improved.

☐ Automated course management

Wasting your time by manually enrolling users to courses is the last thing you want.

Having a security awareness program that can automatically enrol users to the courses most relevant to them will save you time and money - and make onboarding a lot faster. This is especially important if your user base is on the larger end.

☐ The right selection of courses

Even if a training provider had all the other features on this checklist, there's no point in going with them if they don't provide courses on the right topics.

We have included a list of the core cyber security topics below, but you should also consider if your organisation has any specific requirements, such as regulatory compliance training.

- Social Engineering
- Removable Media
- Working Remotely
- Physical Security
- Cloud Security
- Mobile Device Security
- Public Wi-Fi
- Secure Passwords and Authentication
- Phishing
- Social Media
- Internet and Email Use
- Patching and Updating.

☐ Concise, mobile-friendly modules

One of the best things about online security awareness training is that it doesn't bore your users in the same way as long presentations do. However, if your SAT consist of long, wordy modules, users are not going to be any more interested or engaged than they would be had you sat them in front of an hour-long PowerPoint.

Repetition is the key to memory, and short, concise material is the key to keeping users engaged. Modules should be sent out to users regularly, ideally on a monthly or weekly basis, and they should not be overwhelmed with too much material at once.

Having modules be mobile-friendly will also allow your users to be more productive by learning while away from their desk.

☐ Video & Interactive content

One of the best ways to keep end-users engaged is to provide training through video content. Videos are great at presenting information in an attention-grabbing and memorable way, and will boost user engagement with courses.

Training providers with video content are more likely to actually be invested in making high-quality learning material.

☐ Password-free access

Your end-users don't want to have yet another username and password combination to remember.

To save yourself from having to deal with forgotten usernames, lost passwords and other excuses for low course participation, you should look out for SAT providers who can offer password-free access to learning material.

This will often come in the form of direct email links to your users' email addresses, allowing them to start their courses in just one click.

☐ Tracking of course participation

There is not much use in spending money on security awareness training if your users aren't actually going through their courses. In order to know which users are doing their courses - and who aren't - you will want your SAT to include reporting on course participation.

To make your life a little bit easier, you might also want to look out for providers offering automatic reminder emails that are sent out to users who fall behind on their learning material.

☐ Custom reporting tools

In addition to keeping track of course participation, good reporting tools will also allow you to see how each user has performed on their courses, as well as create custom reports.

Custom reports could be used to find out - for example - how well your marketing team has fared on phishing questions, or whether your HR team has any general gaps in knowledge across the department.

Your 10-point checklist:

- [ ] **Gap Analysis**
- [ ] **Individually tailored courses**
- [ ] **Threat simulation**
- [ ] **Automated course enrolment**
- [ ] **The right selection of courses**
- [ ] **Concise, mobile-friendly modules**
- [ ] **Video content**
- [ ] **Password-free access**
- [ ] **Report on course participation**
- [ ] **Custom reporting tools**

Tel: +44203 4753272
Web: https://www.copear.com
Email: accounts@copear.com