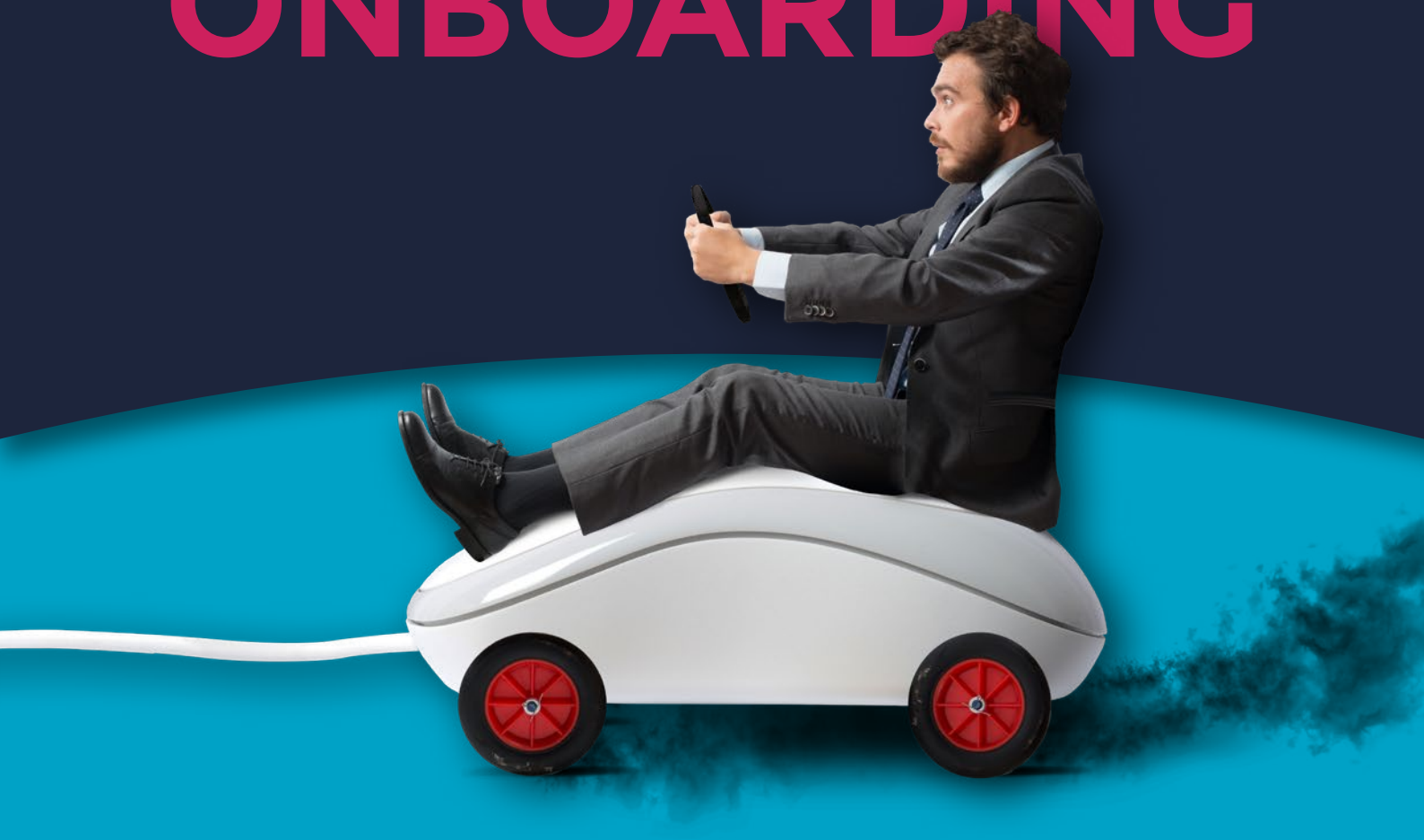
Bob's Business

THE ULTIMATE GUIDE TO CYBERSECURITY ONBOARDING



So your exciting new addition has signed on the dotted line and becomes the latest hire at your company - congratulations!

Taking on new staff is an exciting time for any business, and the new ideas and perspectives they bring can help drive success across your organisation.

But whilst the future might be rosy, there's a period of adjustment to get through first. Yes, we're talking about the onboarding process.

Onboarding new members of your team can be tough. From new processes to follow to adjusting to dynamics within the company, it can be just as hard for an organisation to adapt to a new team member as it is for that team member to adjust to the organisation.

Whilst onboarding varies from organisation to organisation, cybersecurity training is one thing that no onboarding process can skip. In this guide, we're going to share why cybersecurity training should form part of your onboarding processes, how to get started, and share ten essential first steps for any new hire to take to boost their cybersecurity.

Let's get started

Contents

Why is cybersecurity an onboarding essential?

Onboarding can feel like a delicate balancing act. Overloading a new staff member with rules, procedures, and cultures can stop anything from going in. Nevertheless, locking in behaviours whilst a new hire settles in is the most surefire method for improvement.

So why introduce cybersecurity training into the mix? An astonishing 90% of breaches occur due to simple human error. Though the number of organisations training their teams to spot and stop threats is growing, it remains the case that assuming a good level of cybersecurity knowledge is a fast track to failure.

Not only does proper cybersecurity training help protect sensitive customer data, it helps new employees understand their role in protecting the organisation's sensitive information and systems.

By providing cybersecurity training during the onboarding process, organisations can ensure that all employees have the necessary knowledge and skills to protect themselves and the organisation from cyberattacks.

How to embed cybersecurity in your onboarding

Assign a course as part of your welcome pack.

Incorporating an entry-level cybersecurity module into your onboarding documentation is a valuable step towards ensuring your organisation is well-protected against common threats an employee will face.

This module should provide information on the most common cybersecurity threats, such as phishing, malware, and ransomware. Additionally, it should include best practices to protect data, such as avoiding clicking on suspicious links, using strong passwords alongside two-factor authentication, and regularly updating software.

It is also important to educate employees on the importance of protecting their data and the organisation's data, as well as ensuring any data shared externally is done so securely.

By taking these steps, your organisation can ensure it is well-protected against cyber threats.

Take the time to explain why cybersecurity training is important

The first step in any successful cybersecurity awareness training programme is ensuring that every single person in your business understands why they are a crucial part of the company's security.

Start by highlighting the risks associated with not having a good understanding of cybersecurity, such as data breaches and the potential damage they can cause. Afterwards, explain the benefits of cybersecurity training, such as improved security and protection of sensitive data.

Finally, demonstrate the value of their training by setting clear expectations about what the training will cover and the skills the employees will learn. Encourage employees to ask questions and support them during the training process. By taking these steps, you can ensure that your employees are well-informed and engaged in their cybersecurity training.

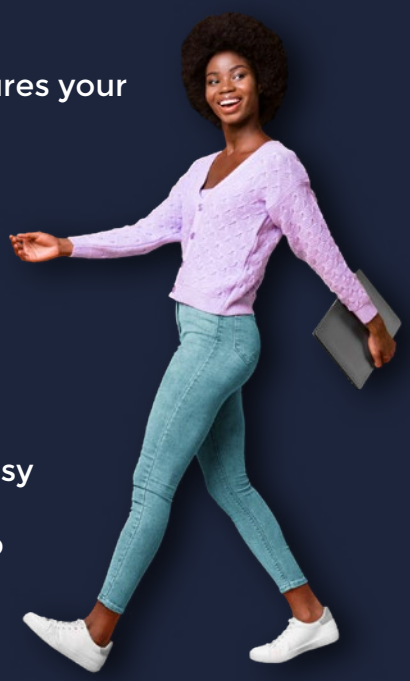
Creating an environment of excitement and enthusiasm for cybersecurity training can be challenging, but it is certainly achievable.

Here are a few tips to make your employees more engaged and enthusiastic about cybersecurity training:

Focus on the importance of cybersecurity training:

Make sure your employees understand the importance of cybersecurity training and the many ways it can help protect their personal information, your business's data, and the viability of your organisation.

Explain the value of cybersecurity training, and highlight the measures your organisation is taking to ensure its safety.



Offer incentives and rewards:

Incentives and rewards can be a great way to encourage your employees to engage in cybersecurity training. Offer rewards for completing courses or for taking on additional training.

Make the training fun and engaging:

With so many online training materials and courses available, it's easy to make cybersecurity training more interactive and engaging. Incorporate quizzes, videos, and other interactive elements to keep your employees engaged and interested in the material.

Get creative:

Consider offering different types of training activities that encourage creative thinking. Team building exercises and games can be fun to engage employees in cybersecurity training.

By focusing on the importance of cybersecurity training while making the training interactive and fun, offering incentives and rewards, and getting creative, you can easily excite your employees about cybersecurity training. With these tips, you can ensure that your employees are well informed and up-to-date on the latest security best practices.

Set employee cybersecurity expectations

Setting employee cybersecurity expectations is important in keeping your team on board with training and your organisation safe. The good news is that onboarding is the perfect opportunity to set those expectations.

Although your stated expectations will vary, we recommend the following as a starting point:

- You are expected to complete any and all training courses you are assigned.
- You are expected to report any suspicious activity, phishing emails or suspected malware.
- You will never be punished for making a mistake that leads to a breach.

The last point is crucial to building a positive cybersecurity culture. People are people, although training regularly reduces the potential of mistakes, when they do occur, employees need to know that you won't punish them for those errors.

By destigmatising cybersecurity mistakes, you encourage employees to come forward and reduce the impact of a breach by catching it early and securing your systems.

Ten 'quick cybersecurity wins' for your new team member

1 Use strong and unique passwords

Using strong and unique passwords is one of the most basic yet essential cybersecurity practices you can adopt. You would be surprised how many employees' passwords are 'password'. Is this you? If it is, then here are some tips on creating strong passwords.

A strong password should:

- Be at least 12 characters long
- Include a combination of letters, numbers, and special characters
- Avoid using easily guessable information, such as your name, birthdate, or common words.
- Avoid using the same password for multiple accounts too, as a data breach on one site could lead to a domino effect across all your accounts.

2 Keep your software and devices up to date

Software and device updates often include security patches to fix known vulnerabilities. If a security vulnerability is discovered, hackers will often try to exploit it before a patch is released. By keeping your software and devices up to date, you can ensure that these vulnerabilities are fixed, and your devices are protected.

3 Be cautious when opening attachments or clicking on links in emails

Phishing scams often use emails to trick people into providing sensitive information or downloading malware. Always be cautious when opening attachments or clicking on links in emails, especially if they are from unknown senders.

4 Use a VPN when working remotely or accessing company resources from a public network

A VPN encrypts your internet connection and helps protect your data from hackers. Public Wi-Fi networks are often not secure and can be easily hacked, so using a VPN when working remotely or accessing company resources from a public network is essential.

5 Avoid using public Wi-Fi networks

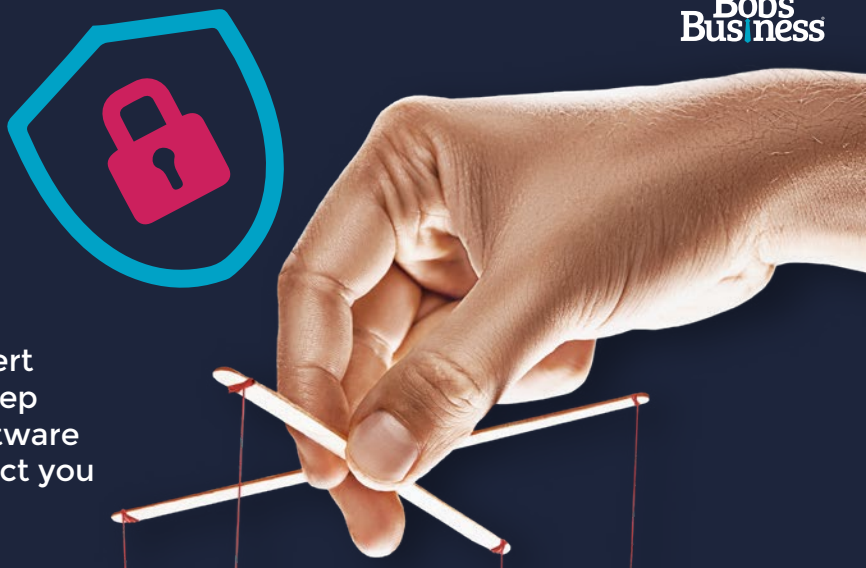
Public Wi-Fi networks are often not secure and can be easily hacked. If you need to access company resources or sensitive information while on a public network, use a VPN to encrypt your connection and protect your data.

6 Use two-factor authentication whenever possible

Two-factor authentication adds an extra layer of security to your accounts by requiring a second form of identification, such as a fingerprint or a code sent to your phone. This makes it much more difficult for hackers to gain access to your account, even if they have your password.

7 Be mindful of your online presence

Be careful about what you post on social media and be aware of your privacy settings. Hackers can gather information about you from your online presence. Be mindful of the information you share online and use privacy settings to control who can see your posts.



8 Use anti-virus and anti-malware software

These programs help protect your computer from malware and other malicious software. They scan your computer for known malware and alert you if it finds anything suspicious. Keep your anti-virus and anti-malware software up to date to ensure that it can protect you from the latest threats.

9 Be aware of social engineering tactics

Cybercriminals often use tactics such as phishing and pretexting to trick people into providing sensitive information. Be aware of these tactics and be cautious when providing personal information, especially over the phone or online.

10 Report any suspicious activity or breaches immediately

If you suspect your computer or network has been compromised, report it to your IT department immediately. Time is of the essence when it comes to cybersecurity breaches; the faster they are detected and dealt with, the less damage they can cause.

Download your free quick-wins checklist here!

How Bob's Business makes onboarding easy

Full access to a diverse training catalogue

No matter what your new employee's role is, our course catalogue has something to suit. Whether that's GDPR training, anti-bullying, fire safety, phishing awareness or any other topic you might require, there's no stone left unturned.

Whether it's our NCSC-certified GDPR and cybersecurity awareness training to any of our other uniquely engaging and effective courses, our training packages offer full access to our catalogue at an affordable price.

Included LMS for all your onboarding needs

Bob's Culture and Bob's Compliance include access to your own customisable organisational Learning Management System (LMS), branded to match your organisation.

It's where your team will access their courses, but that's not the only feature, because your LMS is the ultimate onboarding tool for your team. With features including custom course uploads, user group functionality and more, you'll be amazed at how easy our LMS makes onboarding.

Policy document tracking and attestation

With Bob's Culture and Bob's Compliance, we make it simple to ensure complete compliance with your organisation's policies. Simply upload your policy documents and assign them to your team.

Built-in attestation tracking functionality means that you can see who has - and hasn't - accepted your organisational policies too, to make onboarding a cinch.

Why choose Bob's Business?

At Bob's Business, we make reducing your risk easy, measurable and engaging.

Working closely with your key stakeholders, we create a bespoke package tailored to your business needs, eliminating the necessity and high costs of employing extra staff to deliver effective training solutions.

Changing behaviour and creating a positive security culture takes time and consistency, which is why we stay with you from start to finish, providing regular metrics, support and reinforcement materials to ensure that lessons learned are not lost.

We believe in quality over quantity, and with engagement rates of over 90%, you can be sure your staff are getting a premium solution that relies on science and psychology to implement measurable and long-lasting behavioural change.

Trusted by:

Hotel Chocolat · Charlotte Tilbury · Helly Hansen · mfg motor fuel group · East of England Co-op

About Bob's Business

Founded in 2007 by Melanie Oldham OBE, Bob's Business was created to mitigate the risk which makes all organisations susceptible to cybersecurity breaches - their workforce.

Today, Bob's Business is a leading provider of scientifically-informed cybersecurity awareness training and phishing simulation, working with organisations across the private and public sector to educate staff, transform cultures and deliver meaningful change.

Get in Touch

Visit us online:
www.bobsbusiness.co.uk

Call us:
01226 337335

Email us:
info@bobsbusiness.co.uk

Book a Demo