KnowBe4

# UK Cybersecurity Practices at Work Report

# INTRODUCTION

This report provides an analysis of the survey data on cybersecurity practices at work. The data, gathered by OnePoll, includes responses from 2,000 participants who use a computer for work in the UK. The survey explores various aspects of cybersecurity awareness and behaviours among employees in the workplace.

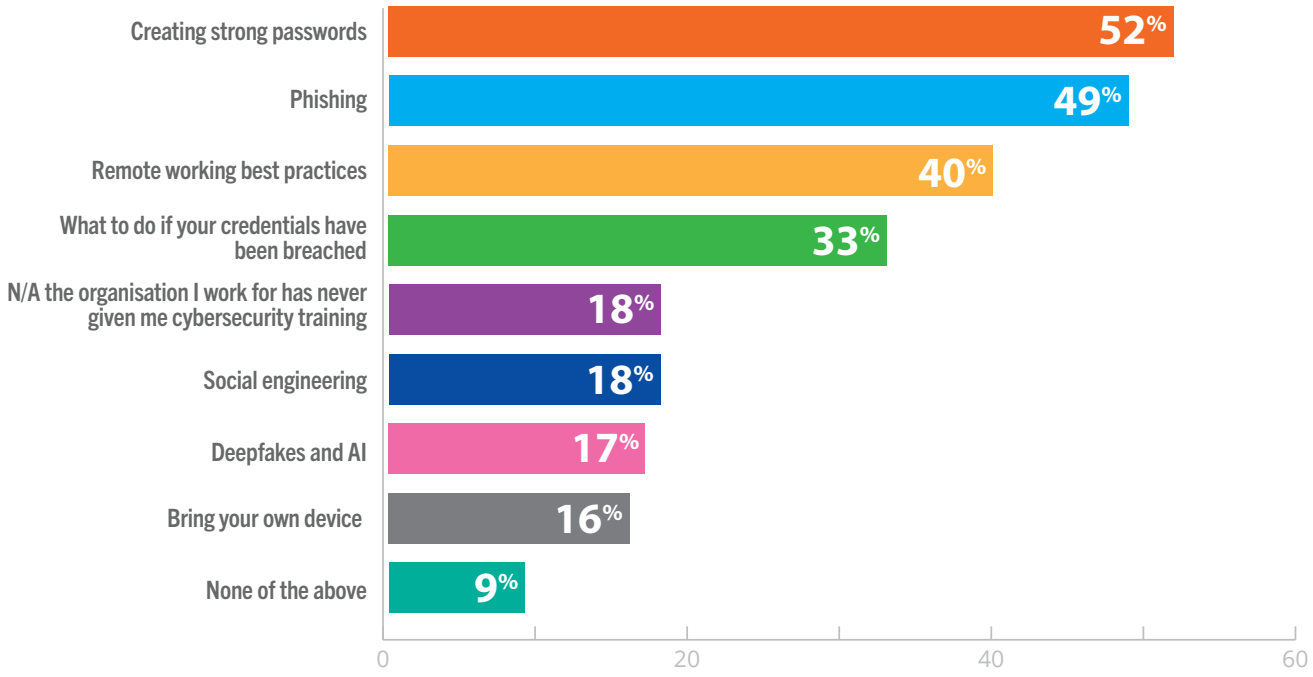
# KEY FINDINGS

## Cybersecurity best practices training

To better understand the cybersecurity awareness levels of respondents, KnowBe4 asked which kinds of cybersecurity training they receive from their organisation. Only just over half (52%) receive training on creating strong passwords, 49% on how to spot phishing, 40% on remote working best practices and one-third (33%) on what to do if their credentials have been breached.

Lower down on the list were training about social engineering (18%), deepfakes and AI (17%) and "bring your own device" (BYOD) at 16%". Alarmingly, almost one in five (18%) said that their organisations had never provided cybersecurity training and for nearly one in ten, they were not given any form of training on these core cybersecurity practices.

**Has the organisation you work for ever given you cybersecurity training on the following?**

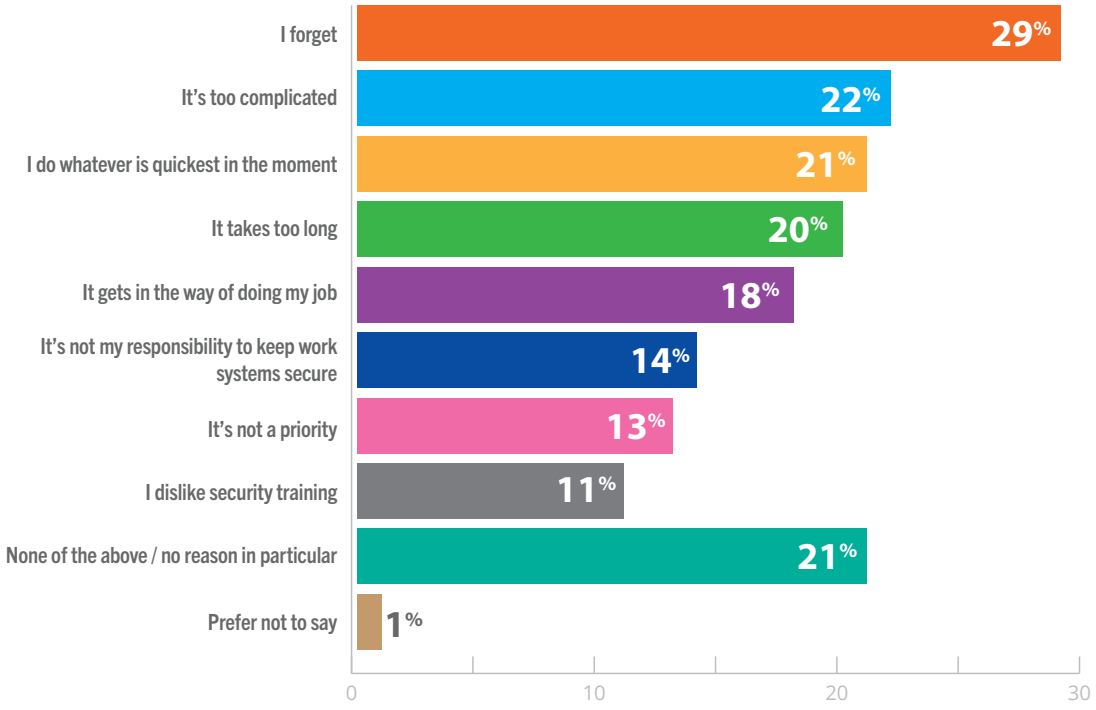



While 42% of respondents said they had read and signed their workplace's cybersecurity policies, almost one in five (17%) said they had read them but did not sign them, 8% said they had not read them but signed them anyway and a further 8% did not read or sign them. Surprisingly, one in ten (9%) did not know if they had ever read them and 15% claim that their organisation does not have a cybersecurity policy altogether.

## Following Cybersecurity Advice

While nearly three-quarters of employees that had been given cybersecurity training noted that they always or often follow security advice, it still leaves room for improvement for one in four workers who claim that they sometimes, rarely or never follow it.

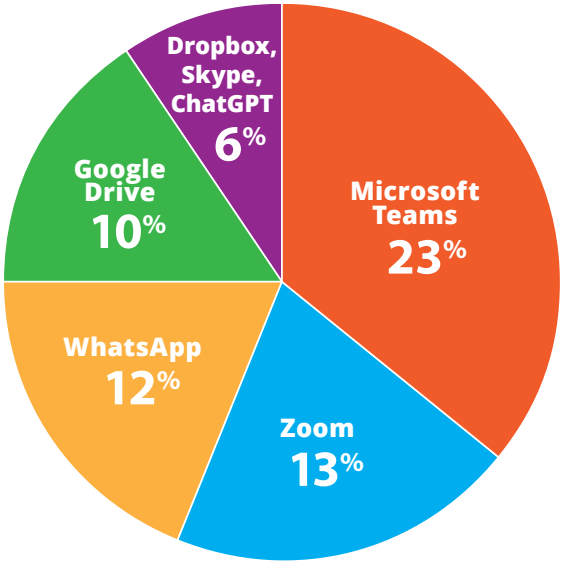
**If you don't always follow cybersecurity advice, why is this?**




The common reasons given for not following security advice include "I forget" (29%), "It's too complicated" (22%) and for more than one in five (21%) "I do whatever is quickest in the moment". Additionally, one in ten (11%) claimed to outright "dislike security training".

A third (31%) of respondents admitted that they or a colleague have bypassed a cybersecurity prompt / best practice / protocol to get their job done quicker and more than one in four (27%) admitted that either themselves or a colleague use apps which are not approved by their organisation, to carry out work tasks.

### The top apps used for work purposes were:




With so many third-party apps in use in the workplace, having clear policies when it comes to cybersecurity and acceptable use are imperative to protecting an organisation's data.

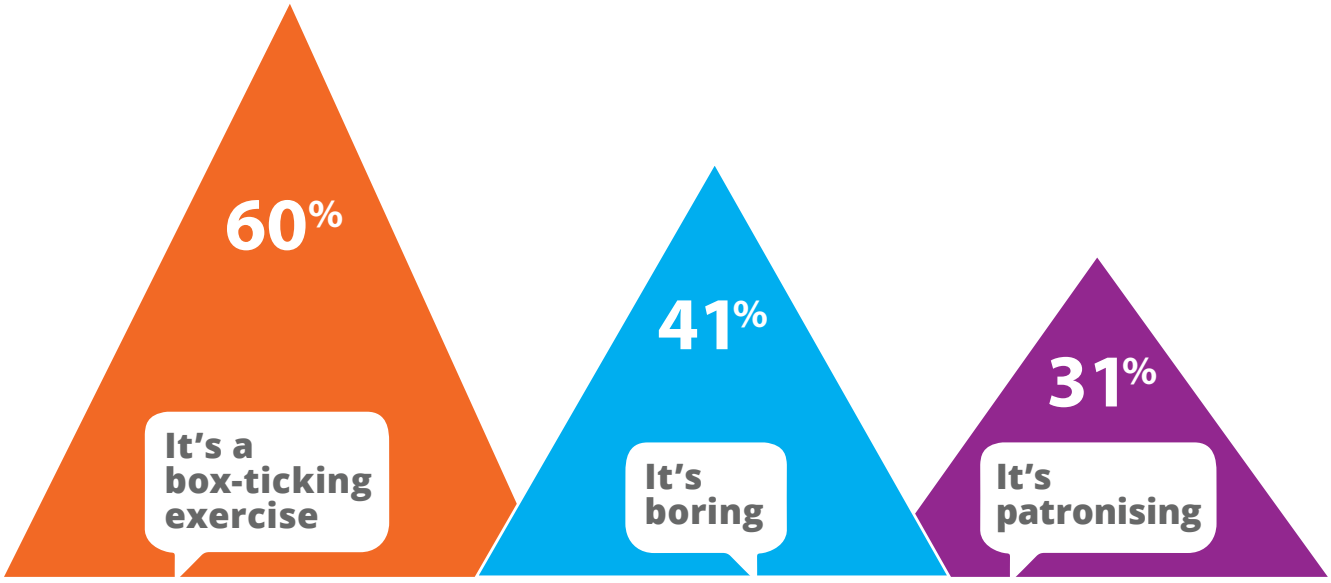
## Risky Cybersecurity Behaviours at Work

Password reuse continues to be a common problem, as well as witnessing their colleagues participating in this risky behaviour at work. The top five risky behaviours were:


## Perceptions of Cybersecurity Training

Encouragingly, those who did receive cybersecurity training from their organisations viewed it in a very positive (35%) or fairly positive (43%) light, with just over one in five having a neutral (19%) or negative perception of cybersecurity training (2%).

For those with a negative opinion of cybersecurity training, the top reasons given were:




Only 37% of UK employees responded that they strongly agreed with the statement "I know what my organisation expects from me when it comes to cybersecurity best practices at work, and I act accordingly".

When it comes to how UK employees would prefer to get cybersecurity advice at work, just over one in four (26%) favour a group training or classroom setting, while just under one in four (24%) would prefer to do it in their own time. For more than one in five (22%), short, sharp training in the moment is preferable and 13% prefer one-to-one training. This dichotomy is indicative of the need for flexible security awareness training options.

# SUMMARY AND RECOMMENDATIONS

The KnowBe4 Cybersecurity Practices at Work Report, based on a survey of 2,000 UK employees, reveals critical insights into workplace cybersecurity awareness and behaviours. Over half of the respondents receive training on creating strong passwords and spotting phishing but less on social engineering and deepfakes. Alarmingly, almost one in five receive no cybersecurity training at all.

Despite training, a quarter of employees do not consistently follow security advice due to forgetfulness, complexity and inconvenience. Risky behaviours, including password reuse, sharing login details, and using public Wi-Fi, remain prevalent. A third bypass cybersecurity protocols for efficiency, and a quarter use unapproved apps for work.

Training is viewed positively by most, yet those who don't have a good experience find it a box-ticking exercise. With preferences for training formats varying, it's crucial for organisations to provide methods that meet people where they're at and offer an array of content to improve security culture.

## Recommendations:

**Enhanced Training Coverage:** Expand training topics to include social engineering, deepfakes, and BYOD policies.

**Regular Refresher Courses:** Provide more frequent, bite-sized training and simulated phishing to reinforce best practices and keep security top of mind.

**Simplify Security Procedures:** Ensure that security protocols are user-friendly to reduce non-compliance due to complexity.

**Promote Positive Security Culture:** Address perceptions of training as a box-ticking exercise by making it engaging and relevant.

**Flexible Training Options:** Offer varied training formats to accommodate different learning preferences.

**Clear Policies on Third-Party Apps:** Establish and communicate clear guidelines on the use of third-party applications to safeguard data.

## Additional Resources

**Free Phishing Security Test**
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

**Free Automated Security Awareness Program**
Create a customized Security Awareness Program for your organization

**Free Phish Alert Button**
Your employees now have a safe way to report phishing attacks with one click

**Free Email Exposure Check**
Find out which of your users emails are exposed before the bad guys do

**Free Domain Spoof Test**
Find out if hackers can spoof an email address of your own domain


## About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

**For more information, please visit www.KnowBe4.com**

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com



01E07K01