KnowBe4
Human error. Conquered.

WHITEPAPER

Furloughed Workers: A Second Wave, a Second Look

A Study of 1,000 Furloughed Employees in the UK&I

Table of Contents

INTRODUCTION

Earlier in 2020, we undertook a survey of 1,000 UK&I-based furloughed professionals with respect to their attitudes towards email and phishing.

Since then, some employees have returned to work, others haven't and some have been to work and sent back home yet again.

While many repeatedly refer to our current status as the 'new normal', it is anything but normal for employees bouncing back and forth.

This report sets out to understand, from a human perspective, what extended furlough and transitions in and out of employment have meant to employees. It also explores where their loyalties lie and if anyone actually cares about security during this turbulent time.

Key Findings

- Only a quarter of respondents reported that their employers had added additional security measures to secure remote working.
- Nearly 28% of employees said they felt less loyal to their employers after furlough, and of those, 70% claimed they either did not feel supported, had little to no information or did not have regular communication with their employers.
- Only 37% of respondents stated they had received any form of security awareness training in the last year.

Methodology and Scope

This report is derived from a survey of 1,000 UK employees who have been on furlough at some point in the last six months and use emails for their roles.

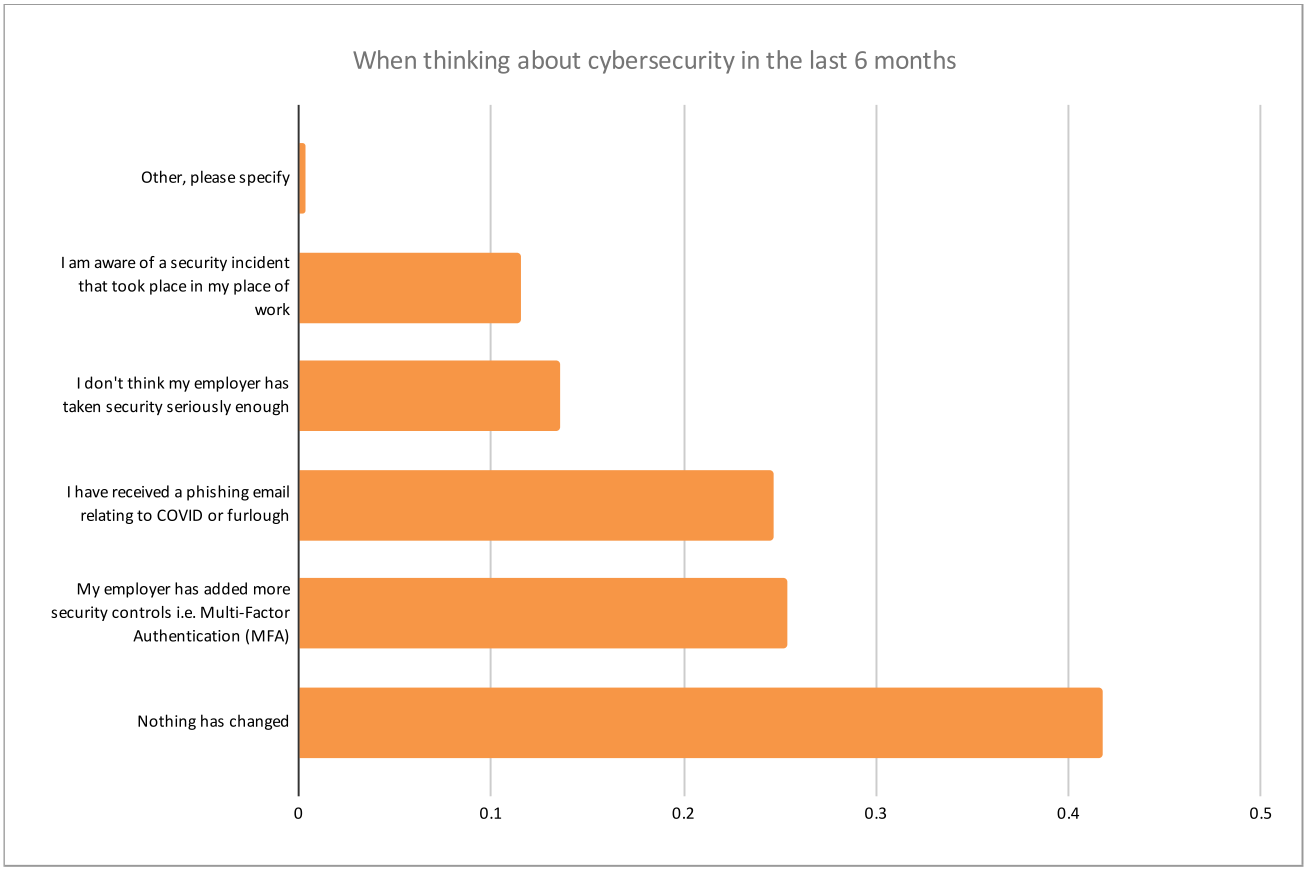
PART 1: CYBERSECURITY CONTROLS, EMAILS AND MEETINGS

It's been a tough year for many organisations. Having to move most, if not all staff to remote working in short order, furloughing some staff, and even cutting back on security controls.

However, criminal activities have spiked during COVID-19 and more organisations and individuals have been attacked during this time. So, it's important that organisations not only implement the right security controls to accommodate a flexible workforce, but also provide the right training to its staff.

Some interesting observations from the survey relating to cybersecurity controls were:

Twenty-five percent of respondents said in the last six months, their employer has added more security controls such as Multi-Factor Authentication (MFA). This is an encouraging response, although there is room for improvement. It's still clear that cybersecurity is enough of a concern that a quarter of organisations took steps to implement better controls.

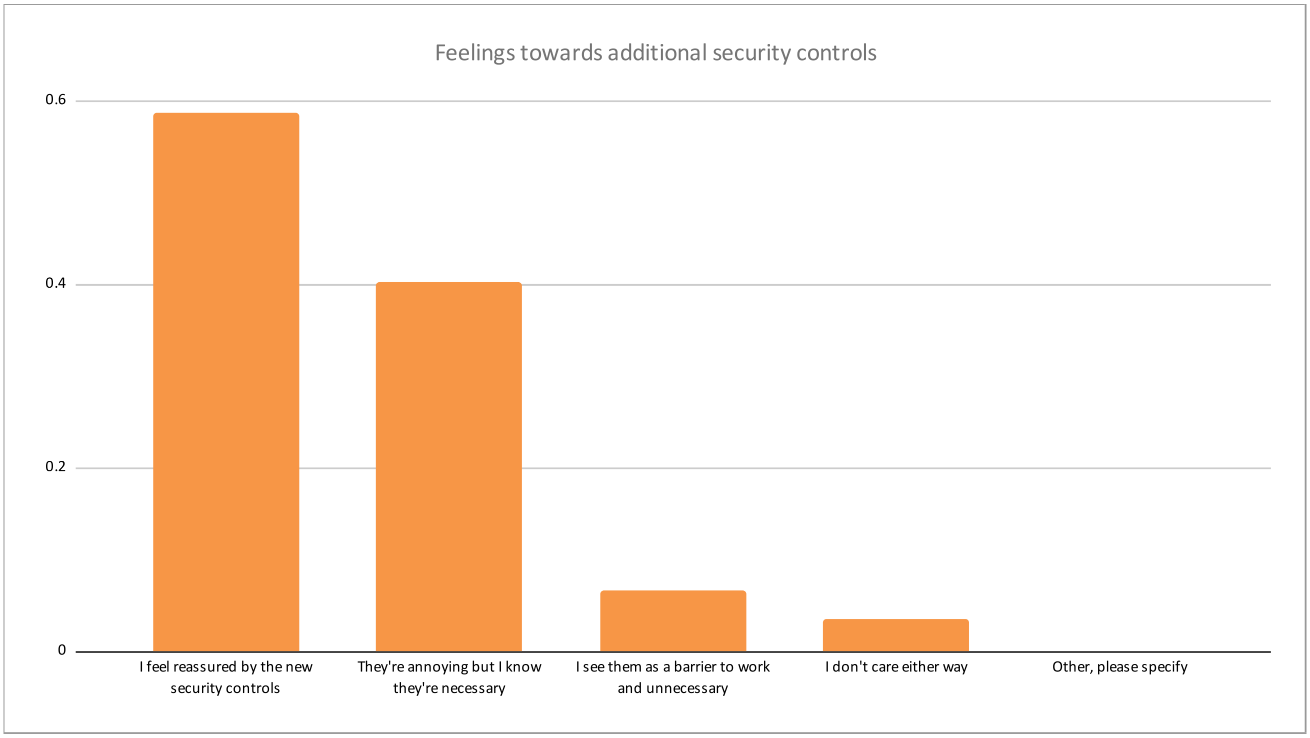


The increase in security controls is not unwarranted, as 25% of respondents said in the last six months, they have received a phishing email relating to COVID-19 or furlough.

Fourteen percent of respondents said that they didn't think their employer had taken security seriously enough. This is somewhat concerning considering that 12% of respondents stated that they were aware of a security incident that has occured in their place of work in the last six months.

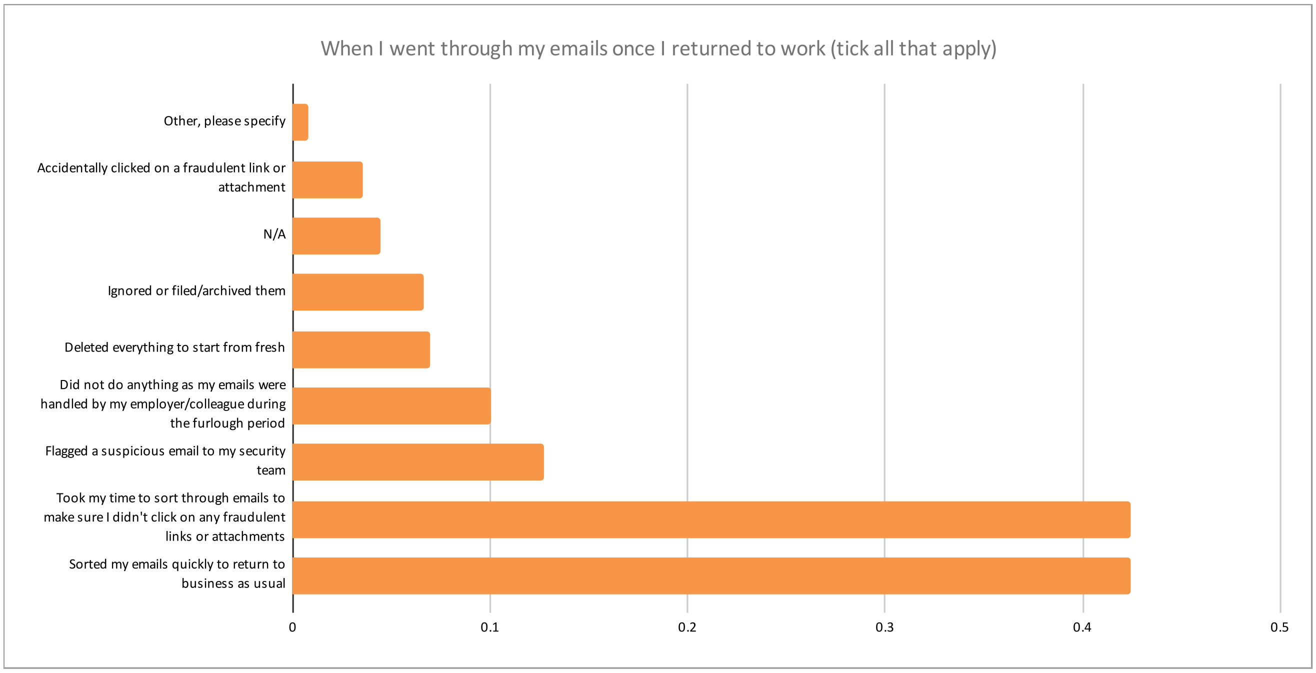
So, while some organisations have made some progress towards increasing cybersecurity controls, the overall sentiment is that more could be done. We wanted to understand how the respondents perceived the added security controls, so we asked those respondents who said their employer had implemented new controls for their opinion.

Fifty-nine percent of respondents felt reassured by the new security controls, whereas 40% said that while they understood the controls were necessary, they were annoying. Only 7% of respondents stated that they viewed the additional security controls as a barrier to work and unnecessary.



Interestingly, employees aged between 35-44 were most likely to view the new controls as a barrier to work and unnecessary at 35%.

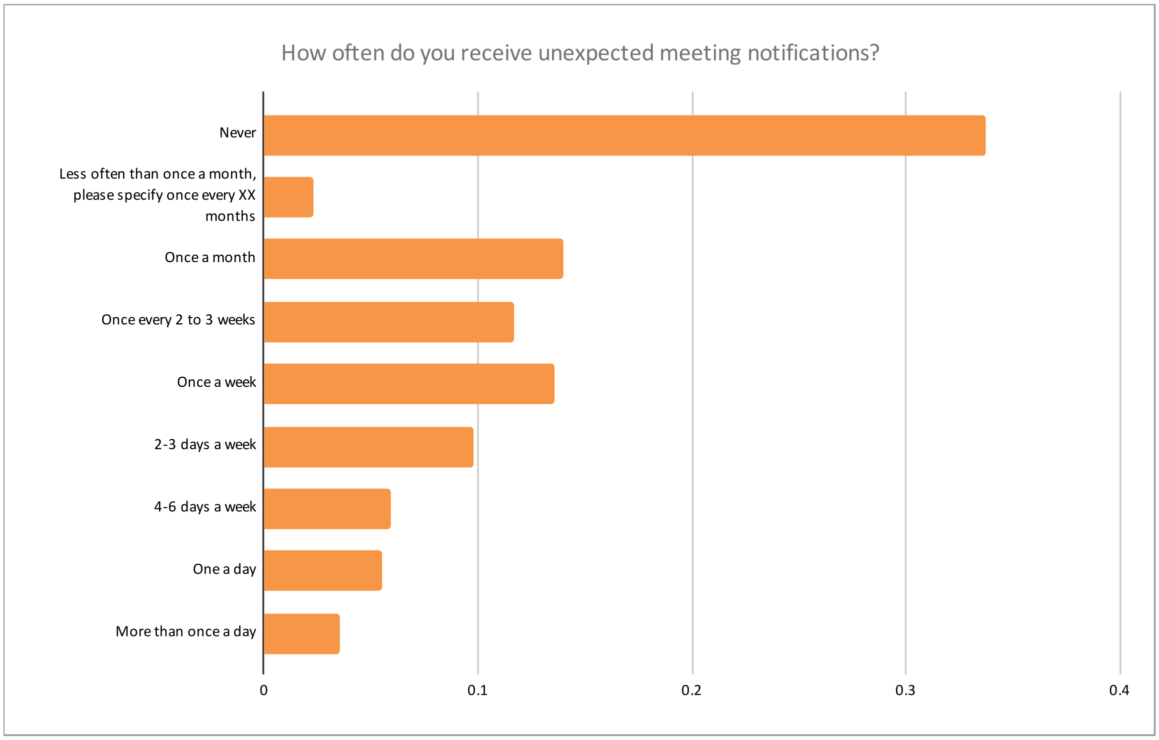
We also wanted to understand how inboxes were handled upon returning to work.



Most employees stated that they either quickly went through their emails and returned to business as usual or took their time to sort through emails to ensure they didn't click on any fraudulent emails or attachments.

Encouragingly, nearly 13% reported that upon returning, they had flagged a suspicious email to their security team. About 10% did not have to do anything, as their emails were handled by their employer or colleagues while they were off and nearly 14% opted for some kind of 'nuclear' option whereby they deleted or archived all emails and started fresh. Nearly 4% admitted that upon returning to work, they accidentally clicked on a fraudulent link or attachment.

But emails aren't the only thing landing in people's inboxes. With so many people working remotely, chatting with a colleague is not as simple as walking over to their desk. So meeting invites flow fast and furious as people try to book out the best time to speak with colleagues, partners and customers. Amongst all the meeting invites, we were curious to find out how many people had unexpected meeting notifications pop up during the course of the day.



A third of respondents said that they never had unexpected meeting notifications appear. But on average, respondents received unexpected meeting notifications two times per week.

A fifth (20%) of respondents in the Architecture, Engineering & Building industry sector receive unexpected meeting notifications once a month, whereas 10% respondents in the Education industry sector said the same.

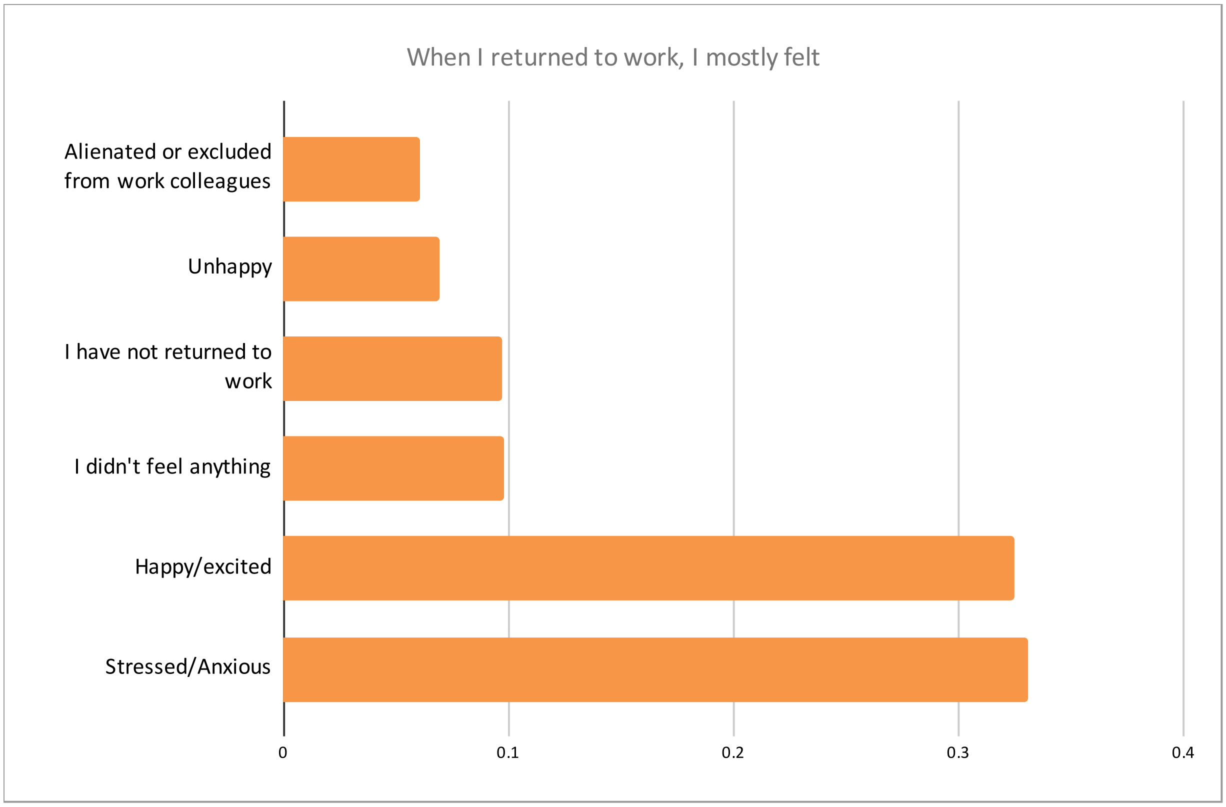
This is interesting from a social engineering perspective. As people have moved to more remote working, we've seen an increase in phishing emails disguised as meeting invites. Recently, a hedge fund in Australia was forced to close after one of its execs clicked on a link in what appeared to be a Zoom meeting. As a result, criminals gained access to the executive's email account and were able to siphon off millions. And while much of the money was recovered, the reputation was damaged to the point where major clients pulled out their money, forcing the fund to close.

So, a cautionary tale for organisations just getting back on their feet to pay close attention to the types of attacks that are heading their way and to ensure employees receive appropriate and timely security awareness training, and have easy access to raise any issues.

PART 2: HUMAN FEELINGS

Stress, Anxiety and Support

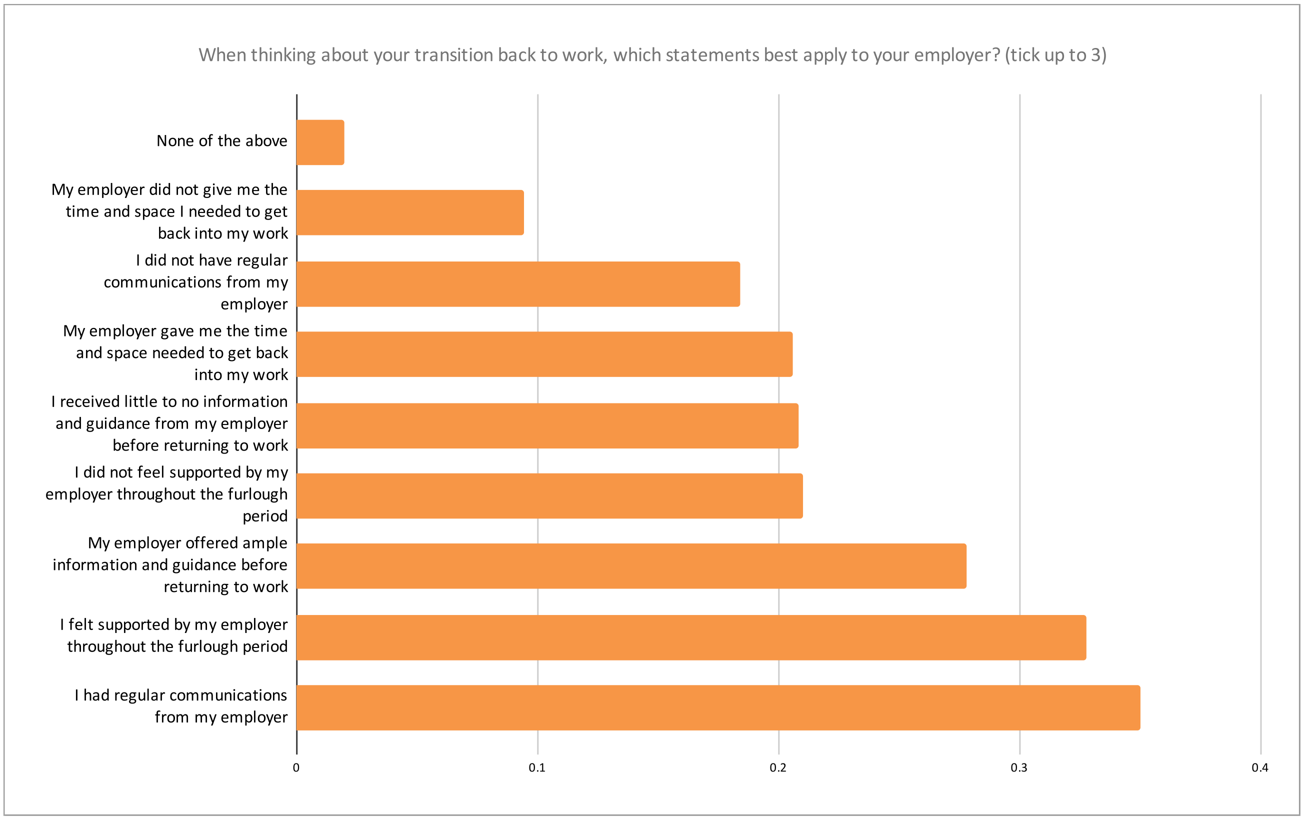
Returning to work can be a daunting prospect for many, especially after a significant amount of time away from the office. Yet, it seems as though some respondents had a tougher time adjusting upon returning to work, with a third (33%) mostly feeling stressed or anxious when they came back after furlough.



It is normal and natural to feel this way. Some may feel disengaged and happy to remain on furlough, while others may be anxious about going into the office and leaving the comfort of their own home. Others may begin to stress about believing they won't be able to perform as well as they did before lockdown.

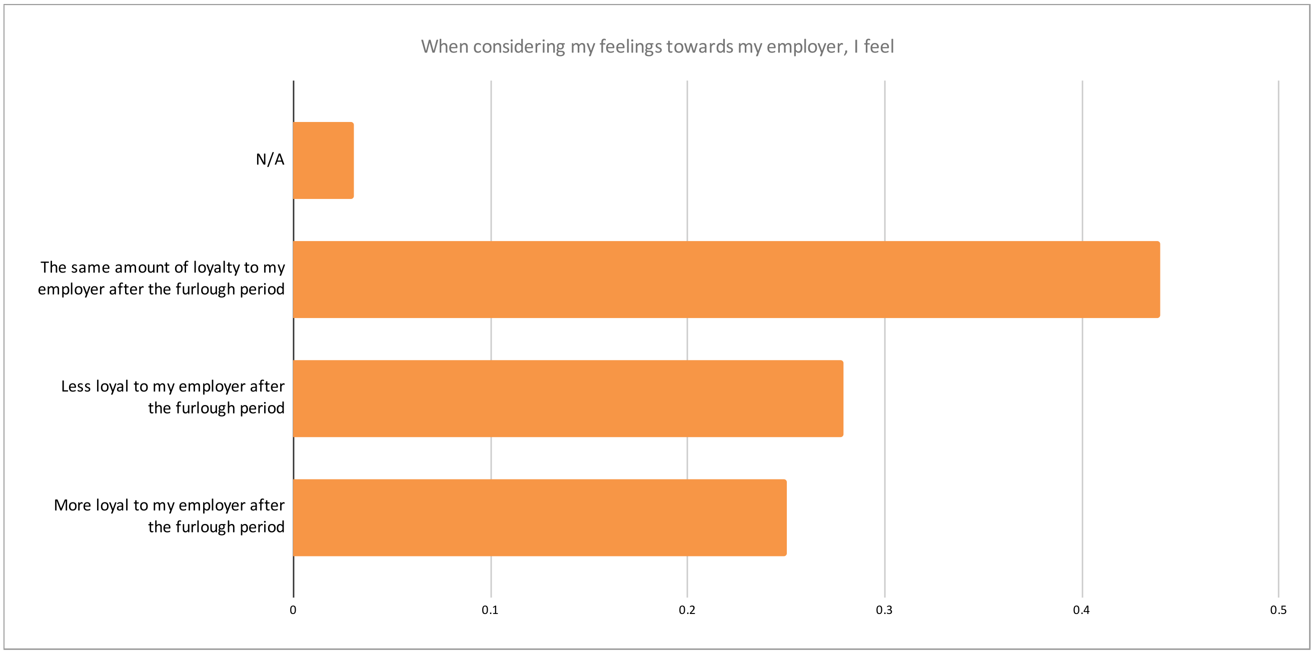
Breaking this down further, two in five (40%) workers in the Education industry sector mostly felt stressed or anxious when they returned to work. With many schools closed during this period because of the high risks of infection, many within this sector were experiencing high levels of stress and anxiety due to the uncertainty of the circumstances.

On the other hand, there was still a third (33%) that felt happy or excited to get back to work. With the well-being of employees a priority for many businesses, any negative emotions may have been subdued or alleviated depending on whether employers were supportive of their staff throughout the furlough period. This of course would make the transition back to work easier and more relaxed. In fact, over a third (35%) of respondents said when thinking about their shift back to work, the statement 'I had regular communications from my employer' best applied to their employer, while a third (33%) stated they felt supported by their employer throughout the furlough period'.



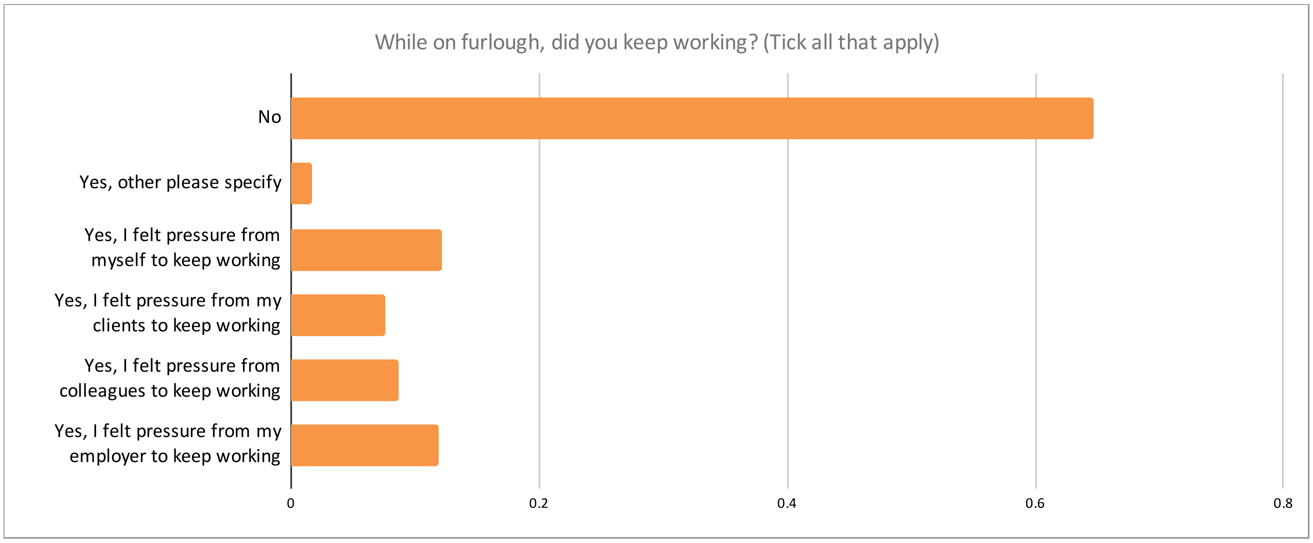
For most, the furlough period was an unfamiliar situation, but it may have brought out an air of fear, frustration or resentment towards employers. This is where company loyalty will be tested and be either strengthened or broken.

When analysing the stats, it's interesting to see three in five (44%) respondents actually felt indifferent towards their employer after the furlough period, while almost 28% stated they were less loyal.



Seven out of ten (70%) of those who felt less loyal claimed they either did not feel supported, had little to no information or did not have regular communications with their employers.

For an employer, keeping an honest open line of communication with staff members to ensure inclusivity could go a long way in preventing employees from feeling frustrated or worried about the future.



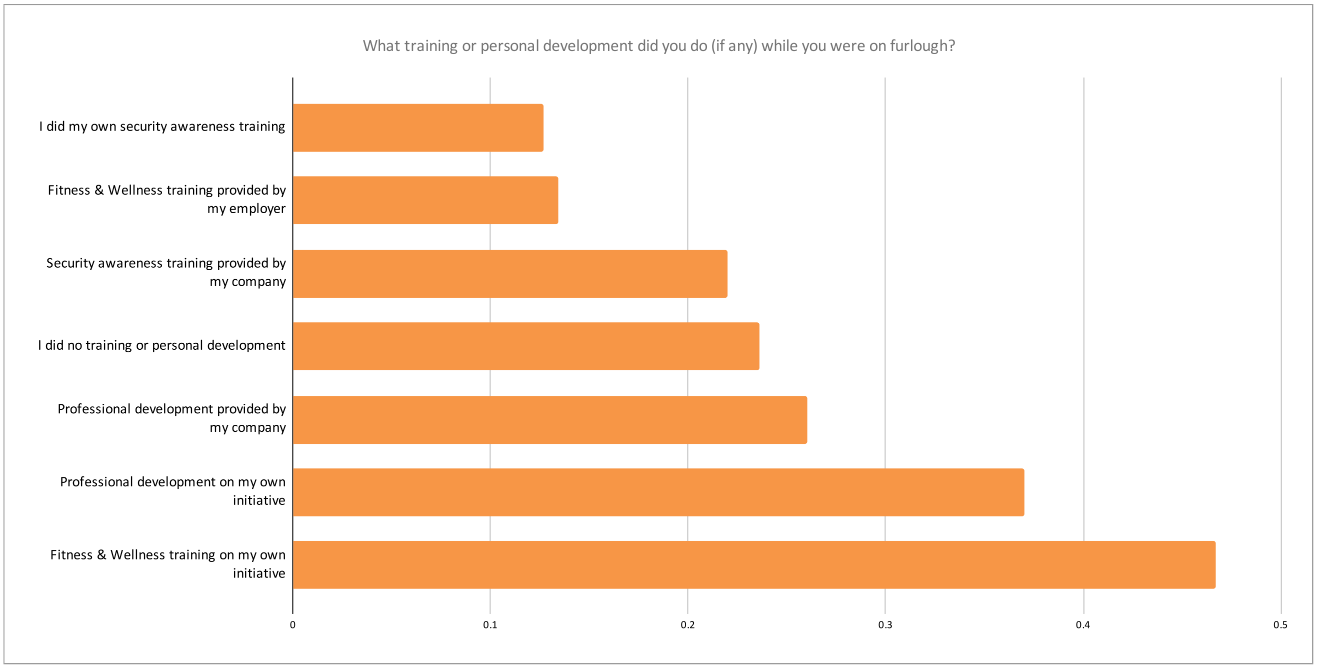
Furthermore, some may have been asked to continue working, which of course, was against the furlough schemes requirements. As we can see, the majority (65%) kept to the rules and stated they did not work. However, there were still some who felt compelled to keep working. This pressure came from either their company, clients, colleagues or themselves. And of those who kept working, just over half (57%) operated solely from home, while 29% continued from the office and 10% split time between both.

PART 3: KNOWLEDGE IS POWER

In the world of cybersecurity, social engineering is the most popular and most effective attack method for attackers. While technical controls have a place, they cannot be completely effective. Particularly where emails don't contain any links or attachments, or the attack comes in via a phone call or an SMS message. Therefore, it's important that the people piece of the puzzle is also beefed up in order to reduce the risk of organisations being breached.

However, security awareness training is not a one-time deal; nor is it something that can be rolled out on an annual basis with the expectation that it will be sufficient. Rather, security awareness training is an ongoing process, where alongside formal training, non-mandatory education, nudges and reminders are needed to keep people mindful.

With the plethora of information available, we were keen to understand what training or personal development people undertook while on furlough. Particularly as employees on furlough were still allowed to partake in any training offered by their employers.



At 47%, nearly half of respondents did fitness and wellness training on their own while they were on furlough. Just over a third, at 37%, undertook professional development on their own, and only 13% undertook their own security awareness training.

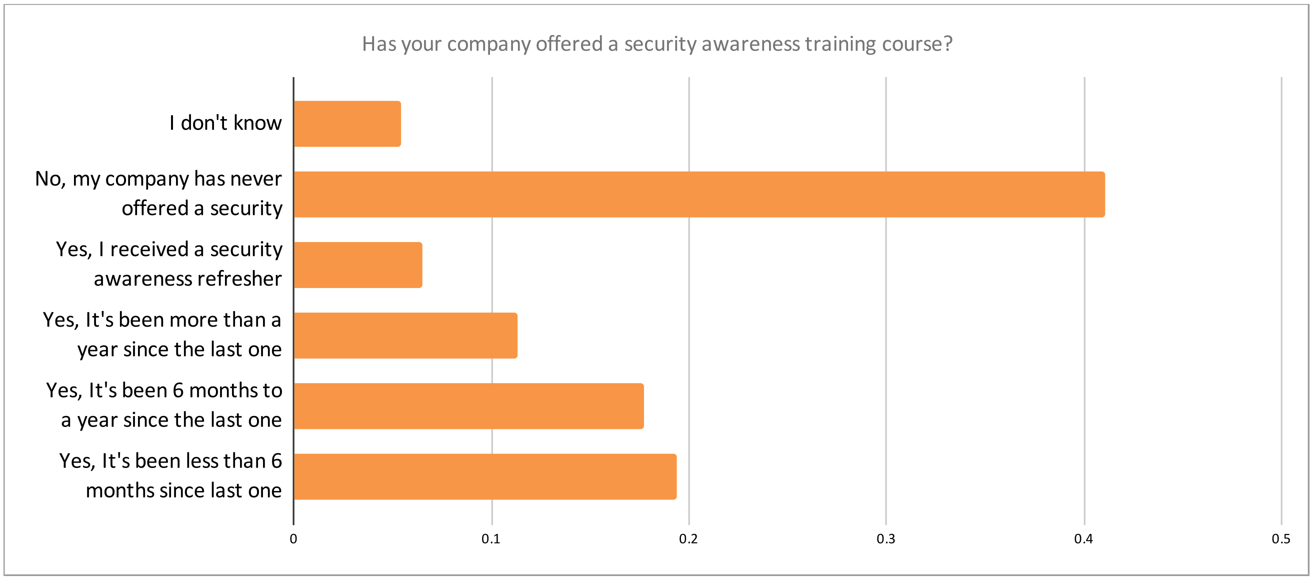
When it came to training provided by their employer, 26% of respondents undertook professional development provided by their employer and more encouragingly, 22% received security awareness training. When it came to fitness and wellness, organisations seemed less concerned and only 13% of respondents said their employer provided any such training.

Of all the respondents, 24% stated that they did not receive any training nor did they undertake any training on their own.

Over half (55%) of respondents aged 25-34 did fitness and wellness training on their own while they were on furlough, compared to three in 10 (30%) respondents aged 55+ who said the same.

Thirty-eight percent of respondents in the Finance industry sector did professional development provided by their company while they were on furlough, whilst just 17% of respondents in the Manufacturing & Utilities industry sector said the same.

Focusing more specifically on security awareness training, we asked the respondents if their organisation had offered a security awareness training course.

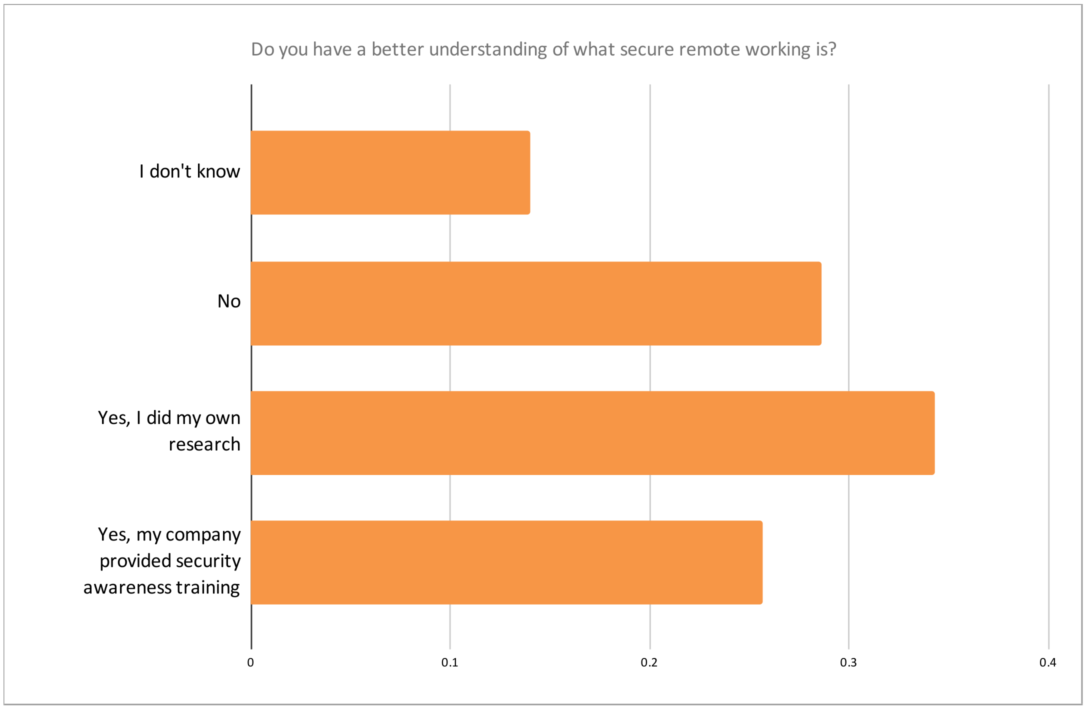


Unfortunately, 41% of respondents stated that their company has never offered a security awareness training course.

While a distant second at 19%, it was encouraging to see that those organisations had provided some training within the last six months. A further 18% stated that they last received training between six to 12 months ago. Combined, it means that around 37% of respondents have received some form of security awareness training within the last year.

From an industry perspective, almost half (49%) of respondents in the Retail, Catering & Leisure industry sector said 'No, my company has never offered a security awareness training course', whereas a quarter (25%) of respondents in the IT & Telecoms industry said the same.

Finally, we wanted to get a sense of how much people's understanding of secure remote working has increased over the lockdown period.



Just over a quarter, 26%, said that their employer had provided security awareness training with regards to secure remote working. However, 34% said that they did their own research to come up to speed on how to be more secure when working remotely.

Twenty-nine percent said that they do not have a better understanding of what secure remote working is. Of those who did their own research, 43% were aged between 16 and 24, whereas only 29% of those aged 45-54 said the same.

From an industry perspective, 45% respondents in the Finance industry sector said 'Yes, my company provided security awareness training', whereas only 17% respondents in the Retail, Catering & Leisure industry sector said the same.

CONCLUSIONS

The pandemic and furlough is very much a human problem. It brings uncertainty, which raises stress, anxiety and burnout. Criminals are all too happy to take advantage of this situation and prey on people's insecurities and distractions for their own benefit.

Organisations need to recognise the trifecta of threats which arise as a result of these circumstances. First, there is the case of the stressed, distracted and maybe even disloyal employee who is apathetic towards the organisation. The second is the criminals who are increasing the frequency and targeting of attacks. Third is the technical challenges that have come about due to remote working and having to adopt new technologies and processes.

For many organisations, these changes mean a complete shift in the risk posture and appetite. So, it's imperative that they review the technical controls for adequacy during these transitional phases and ensure that they are fit for purpose.

Security awareness training is also essential. And not just as an exercise to be carried out once a year, but as a way to build a culture of security that enables employees to make better risk decisions every day in every environment they are in.

Finally, it is important not to lose sight of the fact that employees are all human, and they are undergoing a stressful period. Mistakes will be made, attention will be diverted and performance may suffer. However, this only makes it more important for organisations to have open and direct communication channels with their employees and offer support and guidance to empower them to perform better as opposed to penalising them.

Find out what percentage of employees are Phish-prone™ with the free KnowBe4 Phishing Security Test.

Additional Resources

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

Automated Security Awareness Program
Create a customised Security Awareness Program for your organisation

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 is the world's largest integrated Security Awareness Training and Simulated Phishing platform. Realising that the human element of security was being seriously neglected, KnowBe4 was created to help organisations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organisation with security top of mind.

Tens of thousands of organisations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilise their end users as a last line of defence and enable them to make better security decisions.

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

KnowBe4 UK, Ltd. | Osprey and Kestrel, The Hawkhills Estate, Easingwold, York YO61 3FE | +44 (0) 1347 487512

V121120