KnowBe4
Human error. Conquered.

TAPPED Out Survey Research

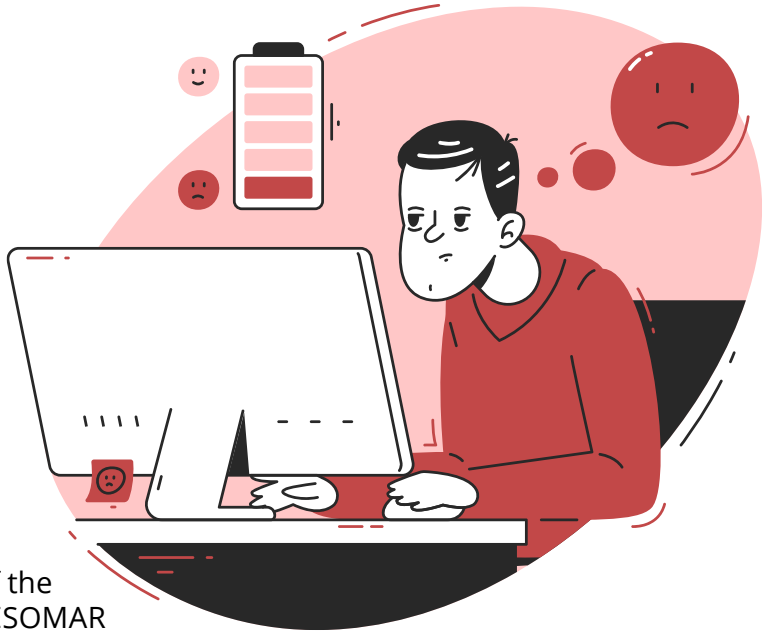
> Employers need to reduce stress and distraction as part of enabling a more security-focused workforce.

Overview

KnowBe4 conducted the TAPPED out research, which stands for Tired, Angry, Pissed, Pressed, Emotional and Distracted, among office workers (those working full-time remotely, in a hybrid way and full-time in the office) across all levels of seniority to uncover attitudes and behaviours relating to corporate cybersecurity.

This report explores the following themes specifically focussing on similarities and differences between working location (full time office, full time remote and hybrid):

- Attitudes towards company cybersecurity
- Workers' behaviour
- Key factors influencing cybersecurity behaviour
- Areas for improvement



Methodology

Censuswide surveyed 6,016 office workers in the UK: 2,007 full time working from a remote location, 2,006 full time working in a hybrid fashion, 2,003 full time working from the office between 31.08.2023 – 12.09.2023.

Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

ATTITUDES TOWARDS COMPANY CYBERSECURITY

REMOTE AND HYBRID WORKERS SURVEYED MORE LIKELY THAN IN-OFFICE WORKERS FEEL RESPONSIBLE TOWARDS THEIR COMPANY'S CYBERSECURITY (86%, 86% VS 79%)

On first inspection, there is good news for companies when it comes to surveyed workers' attitudes towards cybersecurity.

A high percentage of hybrid (86%) and remote (86%) workers surveyed say that they feel responsible towards their company's cybersecurity, this then drops slightly for those who work full-time in the office, where just under 4 in 5 (79%) feel responsible towards their company's cybersecurity. In fact, just over a fifth (21%) of full-time office workers do not feel responsible towards their company's cybersecurity, compared to 1 in 7 remote or hybrid workers (both 14%). This is perhaps good news for businesses given that remote and hybrid ways of working tend to present more of a cybersecurity challenge.

Overall, the findings indicate that a significant proportion of workers do feel responsible for their company's cybersecurity. However, further analysis of the data reveals that this is not always supported by secure behaviour.

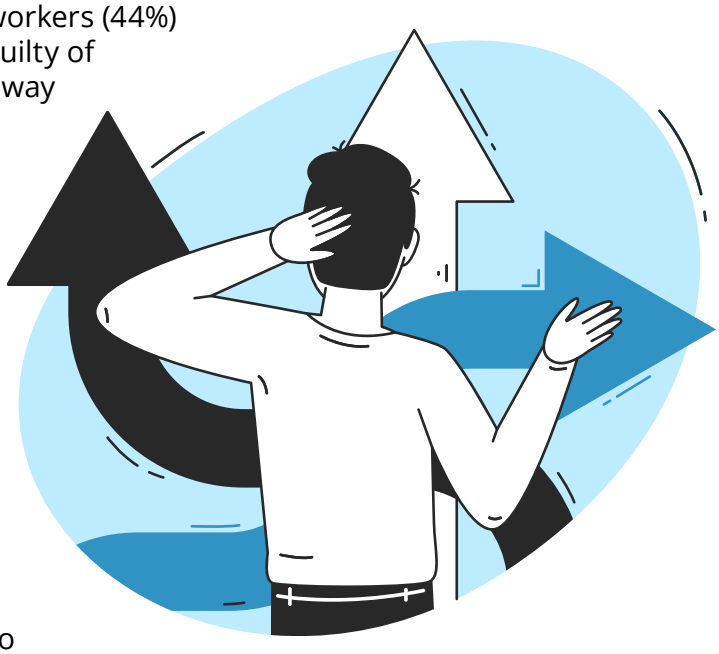
WORKER BEHAVIOUR

HYBRID AND REMOTE WORKERS MORE LIKELY THAN IN-OFFICE WORKERS TO BE CHECKING AND RESPONDING TO EMAILS WHILST HALF ASLEEP

The findings show that although many feel responsible for their company's cybersecurity, office workers surveyed are engaging in behaviour that could be putting it at risk.

For example, over 3 in 5 (62%) hybrid workers surveyed say that they have checked work emails during a meeting or while multitasking on other work activities and around half of remote (50%) or full-time office workers (49%) also say the same. Notable percentages of hybrid (58%), remote (47%) and in-office workers (45%) say the same of responding to work emails in this manner too.

Over 2 in 5 (47%) hybrid workers also say that they have checked emails first thing in the morning while still half asleep—a similar percentage of remote workers (44%) say the same, whilst fewer (37%) in-office workers are guilty of this habit. When looking at responding to emails in this way (first thing and half asleep), remote workers (36%) are most guilty of this, closely followed by hybrid workers (34%), whilst in-office workers are again the least likely of the groups to do this (28%). In a similar trend, hybrid workers were also the guiltiest of the groups to admit to checking (44%) and responding (38%) to work emails on public transport during a commute.



While on the subject of multitasking, around a fifth of hybrid (20%), in-office (20%) and remote (21%) workers say they have responded to their work emails while on the toilet but those who work remotely (8%) or in a hybrid way (7%) are slightly more likely than those who are in the office full time (5%) to have responded to work emails when tipsy/drunk/high. The report also revealed that men were twice as likely to respond to an email while tipsy, drunk or high than women at 10% and 5% respectively.

The fact that so many workers are checking and responding to emails while multitasking, half asleep or on the go makes it less surprising that a high proportion are making mistakes when doing so and again, it seems that hybrid workers are the guiltiest. Indeed, hybrid workers surveyed are most likely to say that they have sent an email too quickly and missed something (63%), while those who work full time from the office (58%) and full time remotely (54%) were less likely to have done this. This is unsurprising given that it had been noted that hybrid workers are also most likely to admit that they respond to emails during meetings or while multitasking on other work tasks.

Generally, workers were less likely to say that they have opened a file or attachment they should not have, but those who work remotely are the most likely to have done this (20%), followed by in-office workers (15%) and then hybrid workers (13%). Similarly, remote workers surveyed (17%) are also slightly more likely than in-office (15%) or hybrid (14%) workers to have clicked on a link they should not have.

KEY FACTORS INFLUENCING CYBERSECURITY BEHAVIOUR

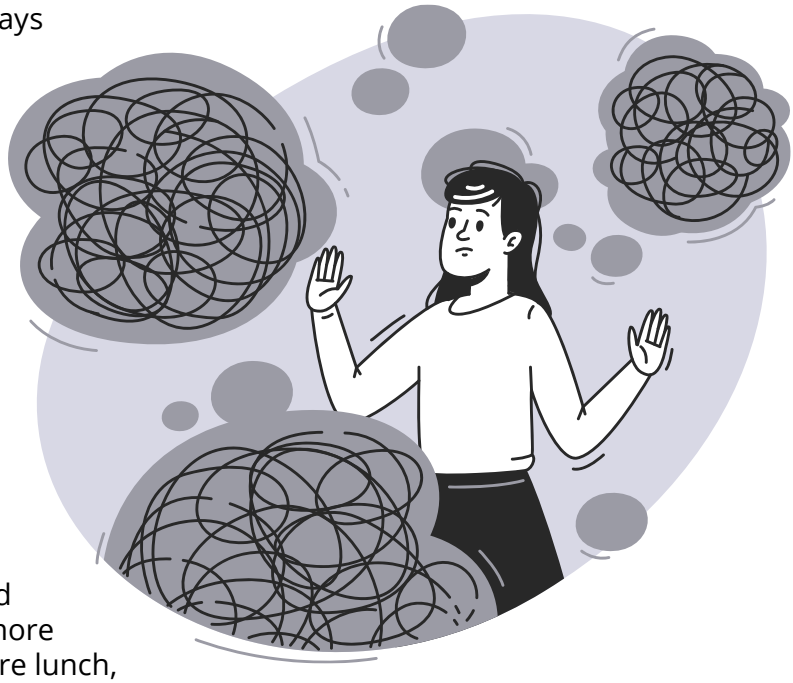
OVER 4 IN 5 HYBRID (82%), IN-OFFICE (84%) AND REMOTE (85%) WORKERS DO NOT ALWAYS MAKE SECURITY-CONSCIOUS CHOICES

The following section explores the factors that may be causing workers to behave in ways that put their company's cybersecurity at risk.

Timing

The data shows that the time of day has an impact on how likely workers are to make security-conscious decisions.

According to the findings, less than a fifth of office workers surveyed (regardless of whether they are hybrid (18%), in-office (16%) or remote (15%) say that they always make security-conscious choices.



For those who do not always make security-conscious decisions, there are specific times of day when they are/would be more likely to pay closer attention to cybersecurity. The findings indicate that whilst hybrid (21%) and in-office (24%) workers claim to be most likely to make security-conscious choices during their entire workday, those who work remotely or full time from the office are most likely to make these good choices first thing in the morning (20%).

Comparing findings from before lunch and after lunch (including after their working day and in the evening), remote (34% vs 29%), hybrid (32% vs 24%) and in-office (32% vs 21%) are all more likely to make security-conscious decisions before lunch, rather than after lunch. Further cementing the findings that good security choices are made in the morning is found in the fact that remote (17%), hybrid (17%) and in-office (15%) workers surveyed are all least likely to make security-conscious decisions in the evening. It is perhaps concerning then, that almost a third (32%) of remote workers are typically checking and responding to most of their emails after lunch, whilst just over a quarter (26%) of in-office workers do the same and over a fifth (22%) of hybrid workers, too.

These findings provide important insights as to when security awareness training administrators should be focusing their efforts to train employees or phish their users. While not meant to catch them out, it can provide crucial lessons that security should be an "always on" function of the workday.

Mental Clarity

As previously discussed, remote, hybrid and in-office workers have a tendency towards checking and responding to emails while multitasking or tired. So, it is no surprise that a considerable number have made embarrassing and sometimes unsafe mistakes.

It is also unsurprising given the manner in which many workers sort through their inbox that poor mental clarity, be it caused by stress, tiredness or distractions, is often to blame when mistakes are made, and therefore poses a threat.

According to the findings, feeling stressed or distracted seems to be the biggest drivers for mistakes made. For example, over half (52%) of in-office workers surveyed sent an email they regretted when they were stressed and a similar percentage (51%) of hybrid workers said the same. Fewer (44%) remote workers said they were most likely to be stressed at the time they sent an email they regretted; however, it was still the leading cause. For those who opened a file or attachment they should not have, regardless of whether they are remote (36%), hybrid (39%) or in-office (45%), workers were most likely to have done this when they were feeling distracted.

Meanwhile, almost 2 in 5 (39%) workers who have clicked a link they should not have also say that they were distracted at the time, while over a third (35%) say that they were feeling stressed. In addition, 2 in 5 (40%) workers who have opened a file or attachment they should not have also say they were distracted at the time, while over a third (35%) of workers say they were feeling stressed.

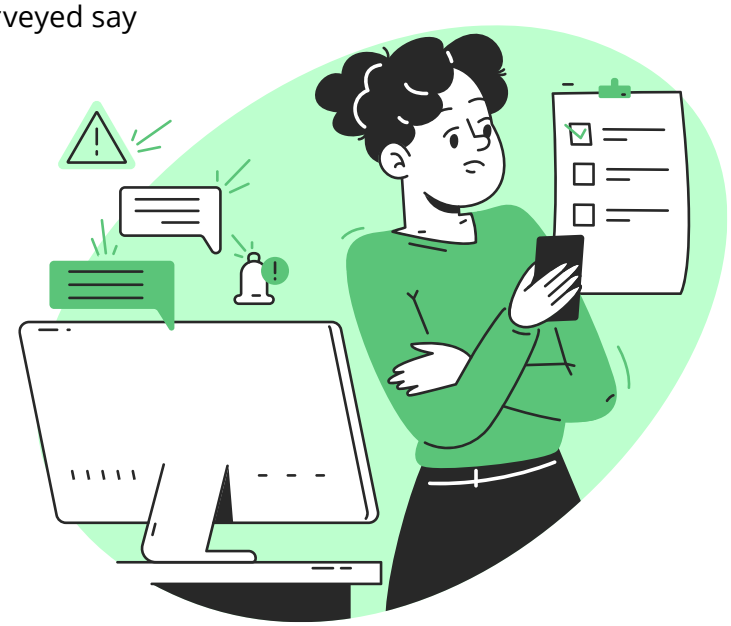
It is evident then, that employers need to reduce stress and distraction as part of enabling a more security-focused workforce.

Distractions

As noted, the findings clearly indicate that distractions play a big role in causing workers to engage in risky behaviour that could put their company's cybersecurity at risk.

The top five things that full-time remote workers surveyed say distract them during a regular working day are:

- Phone notifications/calls (39%)
- Hunger/snacks (32%)
- Housemates/family members/children or colleagues (29%)
- Deliveries (28%) / Unnecessary meetings (28%)



Meanwhile, the top five things that full-time hybrid workers surveyed say distract them during a regular working day are:

- Phone notifications/calls (45%)
- Unnecessary meetings (43%)
- Hunger/snacks (36%)
- Housemates/family members/children or colleagues (28%)
- Deliveries (26%) / Need to do chores (26%)

Lastly, the top five things that full-time office workers surveyed say distract them during a regular working day are:

- Phone notifications/calls (45%)
- Hunger/snacks (34%)
- Unnecessary meetings (33%)
- Housemates/family members/children or colleagues (22%)
- Entertainment (TV, social media, radio etc.) (15%) / Deliveries (15%)

Each group of workers tends to experience similar distractions. It is clear for example, that wherever workers are based, there is simply no escaping the distractions caused by their phone. In fact, remote, hybrid and office workers were all most likely to say that phone notifications/calls distract them during their regular working day. Hunger/snacks also rank highly for each group, as do unnecessary meetings.

However, there are some notable differences in how likely each group of workers is to experience various distractions throughout their working day.

For example, unnecessary meetings are a particular problem for hybrid workers. Over 2 in 5 (43%) full-time hybrid workers surveyed say these distract them during a regular working day, while under 3 in 10 (28%) of those who work remotely full time say the same.

As one might expect, deliveries tend to create more of a distraction for workers who spend time working from home. Almost 3 in 10 (28%) full-time remote workers surveyed, and just over a quarter (26%) of full-time hybrid workers surveyed say they are distracted by deliveries in their regular working day, while just 15% of those working from the office full time say the same.

Similarly, just over a quarter (26%) of full-time remote workers and the same percentage of full-time hybrid workers (26%) say that the need to do chores distracts them. This is compared to just 14% of those working full time from the office who say the same.

Other people are also a source of distraction, especially for full-time remote (29%) and hybrid (28%) workers who are slightly more likely than full-time office workers (22%) surveyed to say that they are distracted by housemates/family members/children or colleagues during their regular working day. The same can be said for pets, as a quarter (25%) of full-time remote workers say that they distract them during their regular working day, while just under 1 in 10 (9%) of those working from the office full time say the same.

On top of these distractions, many workers are also dividing their time and attention between multiple income streams.

It is perhaps unsurprising that workers working remotely full time are most likely to have a side hustle or another job. Almost half (49%) of these workers say they have a side hustle or another job, while less than 2 in 5 (38%) of those working from the office full-time say the same.

Not only does this increase companies' cybersecurity risk factor because those with a side hustle or another job are perhaps more likely to be distracted and therefore in a frame of mind to make

errors, but the research also shows that many workers with a second source of income are posing a threat to their primary companies' cybersecurity by using the same resources for multiple jobs. In fact, over 9 in 10 (94%) full-time remote, 9 in 10 (90%) full-time hybrid and 9 in 10 (90%) full-time office workers surveyed say they use the same resources for both their jobs/side hustles.

For example, very similar percentages of full-time remote (43%), hybrid (45%) and office (45%) workers surveyed said they use the same laptop/computer for multiple income streams. Meanwhile, 36% of full-time remote workers, a third (33%) of full-time hybrid workers and just over 3 in 10 (31%) full-time office workers surveyed said that they use the same web browser logins (i.e. saving passwords and credentials to Chrome) when working on their different sources of income.

AREAS FOR IMPROVEMENT

ALMOST A THIRD (32%) OF FULL-TIME REMOTE WORKERS THINK THEY NEED HEALTH AND WELL-BEING INITIATIVES TO ENCOURAGE MINDFULNESS WHEN WORKING

The data shows that businesses are doing reasonably well at equipping their employees with the tools, policies, and education they need to work securely. In fact, high percentages of full-time hybrid (88%), remote (87%) and office (87%) workers surveyed said they feel they have been given the necessary tools, policies and education to work securely.

However, there is plenty of room for improvement as demonstrated by the fact that almost half (47%) of full-time hybrid workers, over 2 in 5 (43%) full-time office workers and over 2 in 5 (42%) full-time remote workers said they are only somewhat equipped by their company to work securely. Meanwhile, 1 in 9 (11%) full-time remote, hybrid and office workers said they do not feel they have been given the necessary tools, policies and education to work securely.

Businesses' shortcomings in this area might explain why many workers behave in a way that could be putting their company's cybersecurity at risk. This behaviour is not necessarily intentional and can be influenced by factors that workers may not even be aware have an impact on their decisions when it comes to cybersecurity. However, it can also come as the result of more deliberate actions such as using the same resources to work on multiple income streams.

When it comes to the areas in which workers could benefit from support to help improve their cybersecurity at work, full-time remote (34%), hybrid (33%) and office (32%) workers were all most likely to say that they think they need cybersecurity awareness training to improve their cybersecurity at work.

That said, the findings indicate that there is a clear link between workers' mental states and behaviours that could pose a risk to cybersecurity. With this in mind, companies would do well to recognise the impact their workforce's mindset has on cybersecurity and include health and well-being initiatives to encourage mindfulness when working as part of their plans to improve this area of their operation. In fact, almost a third (32%) of full-time remote workers, 3 in 10 (30%) full-time hybrid workers and almost 3 in 10 (29%) full-time office workers surveyed state that they think they need this to improve their cybersecurity at work, and would no doubt support this type of initiative.

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 organisations 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 recognised 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 organisations rely on KnowBe4 to mobilise their end users as their last line of defence 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

02D10K01