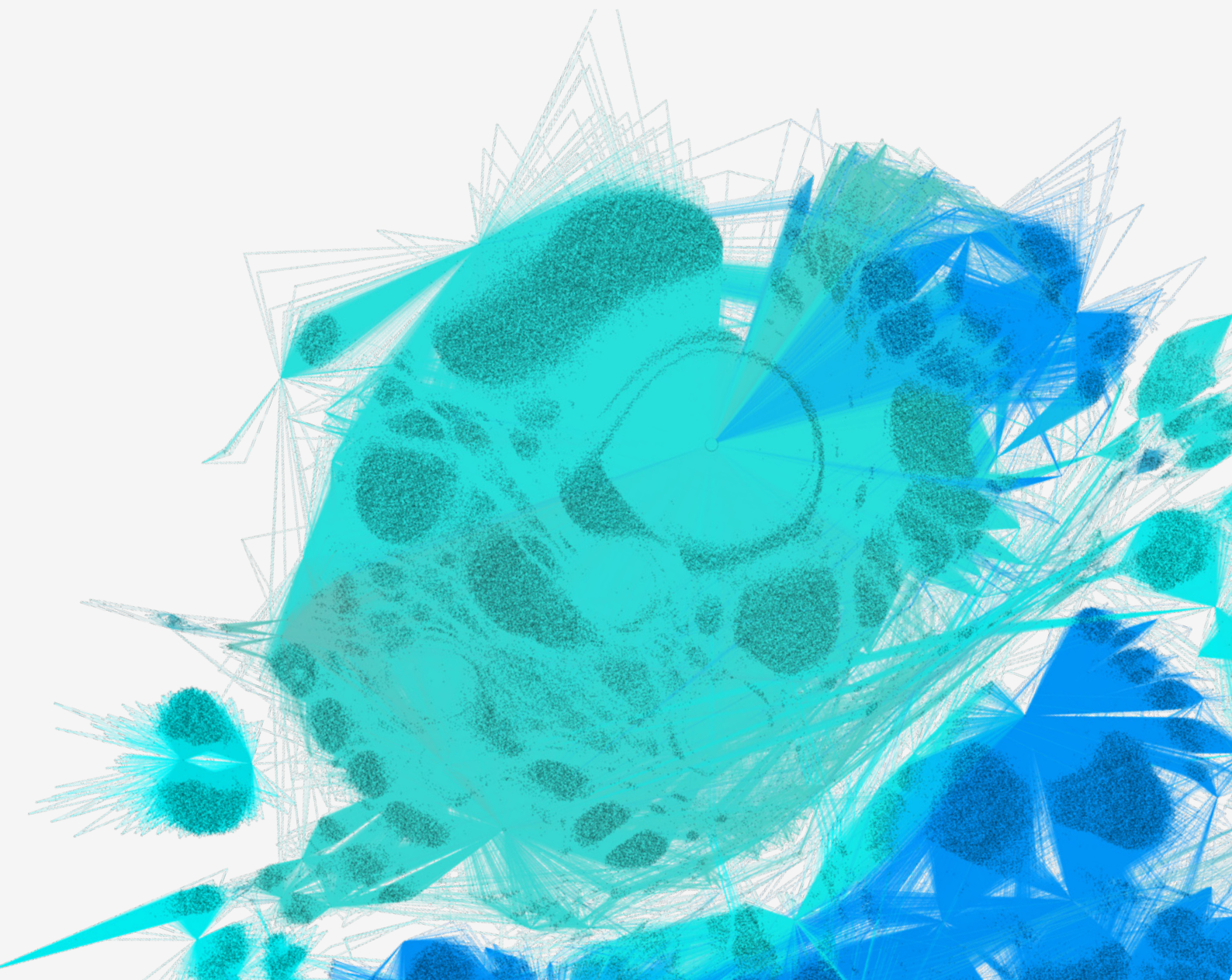


Head in the Clouds:

How remote working behaviours are exposing organisations to cyber risks



13,000
remote workers

27
countries

Introduction

It's often said that employees are the weakest link in the corporate cybersecurity chain. This would certainly explain why phishing attacks have become the number one threat vector for cyber-attacks. Trend Micro detected a 100%+ increase in the volume of Office 365 phishing URLs between 2018 and 2019, for example. During the COVID-19 crisis, organisations have arguably become more exposed than ever to the potentially insecure user behaviour of their remote workers.

This is partly because, given the large numbers of home workers involved, many may not have the luxury of using a corporate laptop. Personal equipment could be less well secured, while the home environment may feature more distractions than the office. What's more, stretched IT teams and budgets mean those that do have a security-related problem may not get the support they would normally. This is a concern.

So how concerned do we need to be about our employees? To find out more, Trend Micro commissioned a major new piece of research themed 'Head in the Clouds', based on the responses of over 13,000 remote workers in 27 countries. It highlights where best practice is occurring, and where things may be going wrong. With over three-quarters (78%) of respondents working more from home during the pandemic, IT and business leaders need to know where the risks are, so they can take concrete steps to address it.

In doing so, they must also remember that no two employees are the same. Trend Micro worked closely with cyberpsychology expert Dr Linda K. Kaye on this research, who explains that there are actually **four distinct personas** in every organisation. Understanding these will help to inform more effective staff training and awareness, although technology controls are also an essential part of any security strategy.

Methodology

Trend Micro commissioned independent market research firm Sapio Research to interview 13,214 remote working knowledge workers in 27 countries. They hailed from a range of ages, industries, different sized companies and job functions.

Four cloud security personas



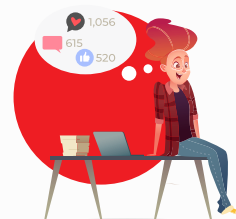
Fearful



Conscientious



Ignorant



Daredevil



85%

agree they have an
important responsibility
to keep the organisation
secure

Good practice is surprisingly common

The first bit of good news is that, despite working in physical isolation from colleagues and managers, an overwhelming number of employees (72%) said they have become more security conscious during lockdown, with only 4% claiming to be less so. What does this mean in practice?

It means understanding that approved corporate platforms should be used to send files, and recognising that using a non-work application for company business is a security risk. It's also about taking instructions from the IT team seriously, as 85% said they do, and agreeing that they have an important responsibility to keep the organisation secure (81%, rising to 86% in larger organisations).

It's also about understanding that it's risky to click on unsolicited emails (68%), even ones promising attractive offers like free cloud storage or faster internet speeds. And knowing definitely not to click if using a corporate laptop.

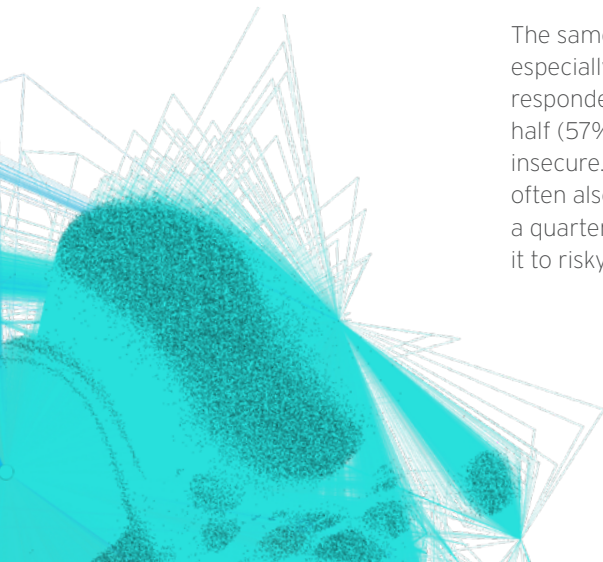
But there's still a long way to go

Unfortunately, that's where most of the good news ends. We also found a large amount of poor security practice which could expose organisations to serious cyber-related risks. These included:

WiFi and remote working issues: Nearly two-fifths of respondents said they always or often use public WiFi without using the company VPN, potentially exposing their browsing and passwords to eavesdroppers. A third have even worked on sensitive documents in view of members of the public without using any privacy screen shield, rising to 44% for contractors, 48% for those working in legal roles and 47% for HR professionals.

Exposing work laptops to online threats: Only 20% said they never use their work laptops for personal ends. Over a third do so freely and a further 45% only during business trips. Such activity could mean exposing corporate data to malware found in torrent sites, non-approved app stores, adult content sites, and more. The good news is that 81% understand that there's a limit to what they should be browsing for on work laptops, although a significant 19% browse freely with no reservations. Their accessing of online games (19%), porn (8%) and dark web sites (7%) should raise serious security red flags as this often violates corporate usage policy of company assets.

The same is true of non-work applications, which could be pre-loaded with malware, especially if they are downloaded from a non-reputable app store. A fifth (20%) of respondents said they see no issue with downloading this software to their work laptop. Over half (57%) of those who have, connect them to smart home endpoints, which are notoriously insecure. A further 70% said they connect these machines to the home network, which are often also home not just to IoT gadgets but insecure personal devices and laptops. Just over a quarter (28%) allow an unsupervised third party to use their work device, further exposing it to risky behaviour.





Personal devices used to access work data: Cyber risk is also multiplied the other way around: if remote workers use potentially less well protected personal devices to access corporate systems. Two-fifths (39%) of respondents said they often or always do so.

Shadow IT and non-work apps: Perhaps even more concerning is the fact that two-fifths (38%) of remote workers have uploaded corporate data to a non-work app – rising even higher for contractors (44%), younger respondents and those in legal (53%) and HR (51%). Although these may be legitimate applications, the fact they are non-sanctioned by IT compounds the challenges of visibility and control associated with shadow IT.

Contractors, youngsters and legal workers: As we have seen, these groups of employees are far more prone to make risky decisions than the average. Contractors are more likely to use public Wi-Fi when out and about and work on sensitive materials in full view of the public. Perhaps unsurprisingly they are less likely to feel responsible for their decisions to the company they're working for. Nearly half (47%) of 18-24-year-olds access corporate data from non-work devices and are less likely to restrict the content they view on a work device. Employees working in legal are surprisingly less likely to take the IT team seriously or agree that non-work apps pose a risk.

Recommendations

38%

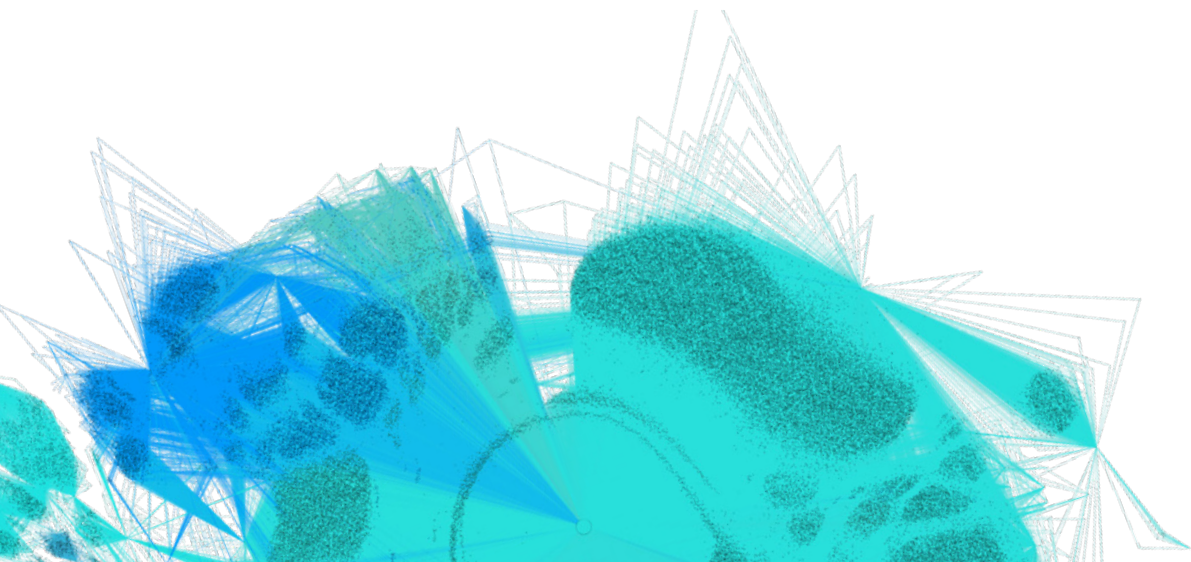
use Multi-factor authentication (MFA)

On the positive side, nearly two-thirds of respondents said they already protect their main personal device with a password, although it's unclear how strong the password is. Multi-factor authentication (MFA) is better, although used by only 38%, while disappointingly less than half (46%) have security software installed.

Fortunately, there's plenty that organisations can do to mitigate risky employee behaviour, even in the context of mass remote working.

IT security managers must combine strict policies on acceptable usage (ie banning use of personal devices for work account access or uploading corporate data to non-work apps) with enhanced education and awareness training. The latter should focus on best practice security including how to spot phishing attacks, using practical tasks and real-world simulations to drive behavioural changes.

Remote working is set to become the norm long after the current pandemic has receded. Now that the initial rush to support the distributed workforce has subsided, it makes sense to start planning in earnest to mitigate the risks highlighted in this report.





72%

have connected their work laptop to the home network, where it shares a connection with potentially insecure personal devices

In-depth: Focus on the UK

In the UK, over three-quarters of users said they have been working from home more than usual during the pandemic, around the global average. Overall, they appear to have a good grasp of cybersecurity best practice and the dangers of phishing. Some 72% said they would not click on a link in an unsolicited email, more than the global average of 68%, and two-thirds (66%) said that home working has made them more security conscious. Over 80% of respondents said they take IT instructions seriously (81%) and think cybersecurity is partly their responsibility (83%).

Overall, this translates into good security-aware behaviour from UK remote workers. Some 70% said they don't allow unsupervised access to their work device, and 64% believe using an unsanctioned app for work is a security risk. Just 25% have uploaded corporate data to such an app, much lower than the global average of 38%. Although a third (32%) said they use their work laptop for personal browsing, 83% restrict the sites they use on it.

However, there are concerns. Over a third (36%) said they use non-work devices to access corporate data, and 72% have connected their work laptop to the home network, where it shares a connection with potentially insecure personal devices (66%) and smart home devices (58%). What's more, although 62% said they protect their personal devices with a password, less than half (43%) have security software installed and only 35% protect accounts with MFA.

In general, therefore, UK remote workers are more responsible than the global average, but still prone to some behaviour which could expose their employer to cyber threats.