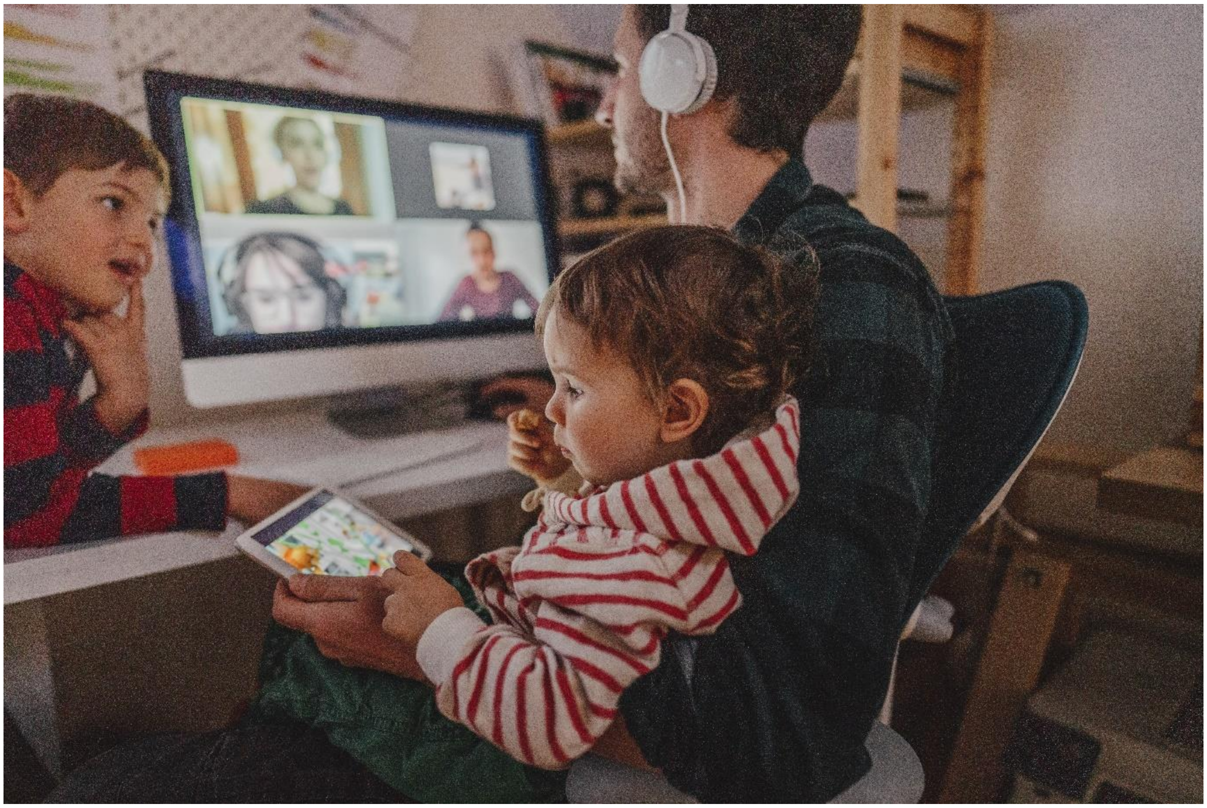

Survey Suggests the Behaviour of Remote Workers is Adding Extra Cybersecurity Risk to Their Employers' Business

AT&T research finds more than half of employees (54%) admit company devices are used for personal reasons; 35% are used to connect to smart devices in the home

LONDON, UK, March 23, 2021

What's the news? The COVID-19 generation of remote workers are admitting to playing a significant part in increasing the cybersecurity risks facing their companies. New AT&T* research shows 54% are regularly using their work device for personal purposes, including sharing work equipment with family members.

The survey, conducted by Opinium, questioned 3,000 workers in the UK and Germany who are now operating remotely because of new policies brought in to combat the global Coronavirus pandemic. More than a third of those questioned admitted to using work equipment to connect to smart home devices (35%) such as voice assistants (14%) smart speakers (14%), fitness monitors (13%), smart lighting (12%) and smart kitchen appliances (12%).

Why is this important?
The data clearly shows workers understand the problem. Two thirds (66%) said they are more aware of cyber security threats since shifting to home working. Nearly half believe they personally (49% in the UK; 38% in Germany) and their companies (52% in the UK; 42% in Germany) are at increased risk of cyberattacks. 55% have been the target of a cybersecurity threat while working remotely over the past year, and nearly a third of those surveyed (29%) said their company isn’t doing enough to protect them from cybersecurity threats.

Yet when it comes to taking responsibility, two in three remote workers (66%) say that practicing good cybersecurity at work is challenging; citing a lack of adequate training or technical support (22%), lack of prioritisation by senior management (18%) and it taking too much time/being too much hassle (16%). One in five employees (20%) say there is no way they could be encouraged to care about cybersecurity risk.

What else does the data tell us?
The results of the 2021 research correspond with a July 2020 AT&T survey of 800 EMEA cybersecurity experts, which found that 70% of large businesses with more than 5,000 employees believed widespread remote working was making their companies more vulnerable to cyberattacks. That survey identified employees (31%) as the biggest risk to implementing good cybersecurity practices. At that time, experts believed that one in three (35%) employees were using devices for both work and personal uses but the new research suggests that number is much higher.

While many businesses did introduce new cybersecurity measures to mitigate risks since the onset of COVID-19, employees indicated that many employers have not taken basic steps to improve cybersecurity. One in three (32%) say their company hasn’t implemented additional login protocols to protect from web-based threats and 50% have not required any additional cybersecurity training since shifting to remote working.

John V. Slamecka, region president EMEA & LATAM, AT&T Business
“The lines between our professional and personal lives are blurring and that includes our online behaviours. It’s clear that businesses can only protect their networks by mitigating for those behaviours. Cybercriminals are launching cyberattacks at the most vulnerable point – the remote worker. Businesses who initially compromised on cybersecurity to speed up the transition to homeworking are taking a tremendous risk. They must address cyber risks now to provide for business continuity and help protect their workforce and business for the future.

"Just as companies have introduced measures to support the physical and mental well-being of their employees, they should educate and support their employees' to help them better understand cyber safety while working outside the office. This includes steps like ensuring employees can access secure internet connectivity and web based applications, and providing enhanced cybersecurity training to help employees decrease the risk from attack surfaces should be mandatory to help protect the individual and the company now and as we move into a new hybrid working environment."

Rupesh Chokshi, VP, AT&T Cybersecurity
"With today's hyper distributed workforce, there is a need for Zero Trust. Zero Trust assumes that traditional access credentials are no longer sufficient to accurately establish trusted identities for user, device and application access. Rather, organisations should undertake continuous, risk-informed assessment and deploy granular security controls to manage, monitor, and enforce access."

About AT&T Communications

We help family, friends and neighbors connect in meaningful ways every day. From the first phone call 140+ years ago to mobile video streaming, we @ATT innovate to improve lives.

AT&T Communications is part of AT&T Inc. (NYSE:T). For more information, please visit us at att.com.

For more information, contact:

Jonathan Moore
AT&T Corporate Communications
Phone: +44 7850 071608
Email: jonathan.moore@intl.att.com