
PC Matic
COVID-19
CYBERSECURITY IN THE REMOTE WORKFORCE

TABLE OF CONTENTS

03 Introduction

04 Methodology

05 The Virtual Workforce

06 Corporate Issued Devices

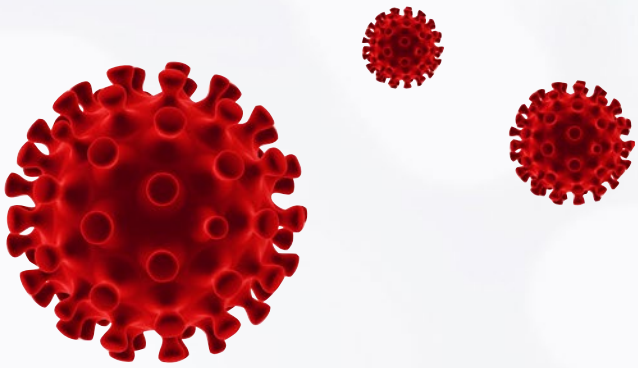
07 Security Holes and Transparency

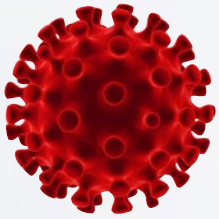
08 Best Practices At Home

09 IT Support Then to Now

10 Conclusion

11 About PC Matic





INTRODUCTION

A year into the pandemic and the face of American business has changed. Remote work is, in some respects at least, here to stay for many companies who didn't use it as an option previously. What does that look for cybersecurity? With employees working remotely, and ransomware attacks on the rise, cybersecurity is a critical component of remote work.

PC Matic conducted a survey in early 2020 to see what the initial habits were of those moving to a remote working environment. Nearly a year later, in 2021, we asked the same questions to the same number of respondents. We wanted to see what, if any, differences there were after a year of remote work.

METHODOLOGY

The information gathered within this report was obtained by surveying over 5,800 individuals in February 2021 regarding their current work from home situation, specifically related to the COVID-19 outbreak. The respondents included both male and female adults located throughout the United States.

The goal of the survey was to understand the current security practices used by individuals and businesses throughout the nation while working from home compared to the same practices used last year at the start of the pandemic. PC Matic was able to establish this baseline with the data provided by survey respondents.

THE VIRTUAL WORKFORCE

According to an article published by Forbes in November 2020, an estimated five percent of full-time employment in the United States was remote pre-COVID. The post-COVID number settled between 20%-30% of full-time workers. This means four to five times more people are now employed at home rather than in an office.

This massive shift created challenges across the board. Some companies were better equipped to handle the change while others are still struggling to adapt their IT strategies. Last year's survey data indicated 42% of those surveyed were working remotely while 36% of this year's respondents indicated they have continued to work remotely.

As some states open businesses and schools, the numbers we see from respondents this year indicate that remote work is still a reality for many companies. Because of that, we now have a more in-depth understanding of cybersecurity trends from last year to this year.

Have you been working from home as a result of COVID-19?

YES – 36%

NO – 64%

CORPORATE ISSUED DEVICES

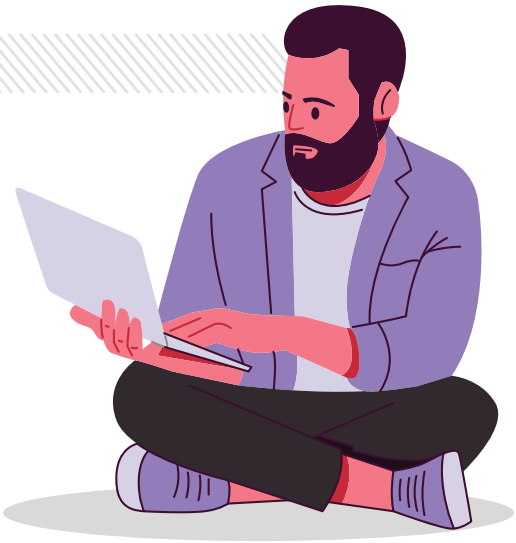
In the early months of the pandemic, work-issued devices weren't always available. Tech retailers reported increased demand and decreased supply. Schools and corporations scrambled to purchase needed hardware to provide to those who moved into their home environments.

The lack of machines led to many being forced to use their personal devices for remote work. At the time of polling last year, only 39% of employees were issued company devices. When we asked now nearly a year later, that number was almost the same.

Did your employer issue a device for work purposes?

YES – 38.5%

NO – 61.5%



SECURITY HOLES & TRANSPARENCY

There's a danger in using a machine for both work and personal use. A skilled cybercriminal could take advantage of the lax security we tend to have with personal devices. Once in, they have much easier access to company information on a shared device.

With the increase in ransomware attacks in the past year, it's likely that the shared use of devices has led to some of those attacks. Unfortunately, the lack of transparency after a cybersecurity breach doesn't allow us enough data to make definitive conclusions.

Adding insult to injury, a staggering 91% of respondents reported this year still not being provided with any type of antivirus solution to use on their device. This is down slightly from the 93% reporting last year, but it's not a significant decrease. Ransomware attacks are reported to only continue to rise. Under utilizing available security technologies adds to the likelihood of an attack.

Did your employer provide you with an antivirus solution to install on your personal device being used for work purposes?

YES – 9%

NO – 91%

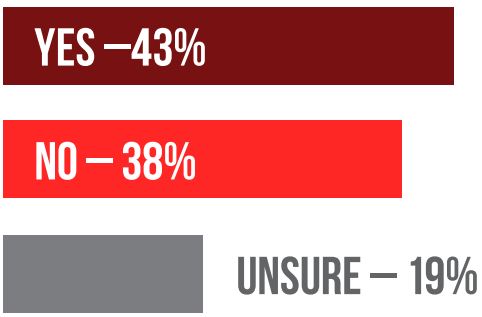
BEST PRACTICES AT HOME

The use of a Virtual Private Network (VPN) is strongly recommended when remote employees are connecting to the network from outside. While it's not essential to use a VPN during personal use, having one on a shared device may help with the security holes present with this setup. Adding security is never a bad thing.

VPN usage is up from approximately 40% of respondents to approximately 43%, which isn't a large jump. Not knowing if a VPN is present jumped from 14% to 19% from 2020 to 2021. Again, this is a number that should be decreasing as security measures increase. Instead, we've seen a 5% rise.

The VPN data seems to indicate that a large number of remote workers are still relatively uneducated about security best practices.

While working from home, are you using a virtual private network (VPN)?

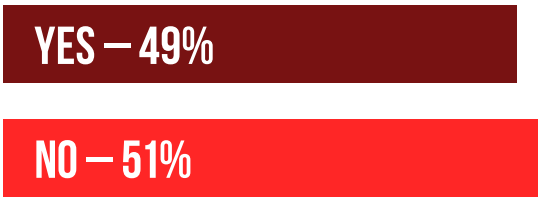


IT SUPPORT THEN TO NOW

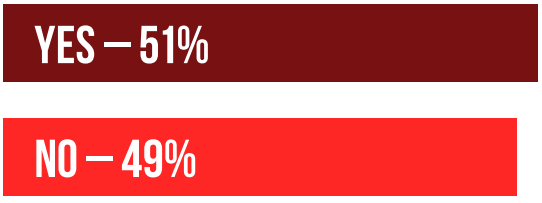
IT support for remote workers is an essential part of a healthy security plan. We know that in the early parts of the pandemic, 51% of respondents reported their company provided support while transitioning to remote work. Compared to this year's data, 49% of respondents reported, a year later, that they received IT support while transitioning. Given the 2% difference, the data appears consistent.

We then asked respondents if they have continued to receive support through the duration of their work from home experience. Nearly half of respondents, 49%, reported they have not received continued support. Again, this leaves plenty of room for cybersecurity breaches throughout various organizations.

Did your employer provide IT support services while employees transitioned to remote workstations?



Did your employer provide IT support services throughout the duration of your work-from-home experience?



CONCLUSION

It's unfortunate to see that the data has remained consistent over the course of the last year. In the best-case scenario, we would have seen security increase and many of these numbers go down. Without transparency, however, it's impossible to determine if the more than 350% increase in ransomware attacks in the last year was due to lax security measures.

As we continue forward, we note that most companies understand remote work is a permanent part of their future. FinancesOnline reports, "According to OWL Labs' State of Remote Work for 2020, 80% of full-time employees expect to work remotely even as the COVID-19 guidelines are lifted (OWL Labs). In fact, as many as 77% say having this option post-pandemic will make them happier with their career. Among their reasons for this include less stress when working from home (74%), better work-life balance (72%), and increased work productivity (70%)."

Their security plans have yet to catch up to that reality. A healthy security plan would include the supply of company devices that do not allow personal use, a mixture of security software including a VPN that is mandatory when accessing company information and continued IT support for remote employees.

Often in house IT Staff is not within the budget for a small business. For companies unable to provide their own continued IT support, managed service providers offer affordable solutions. Managed service providers range in size and expertise, many specializing in certain business types. Their services provide affordable opportunities for small businesses to secure remote workforces.

The likelihood of a ransomware attack can be greatly reduced with a healthy security plan. Since remote work is here to stay, it's time to be proactive about how to protect those workers.

ABOUT PC MATIC

PC Matic Inc., founded in 1999, is a 100% work from home organization that is based in the United States. PC Matic's products provide our customers with essential security that enhances the zero-trust model and fills potential gaps left by other traditional endpoint security software. With a foundation in application whitelisting, PC Matic uses a default-deny approach that prevents all known bad and unknown applications from executing. Our patent-pending globally automated whitelist provides a backbone of millions of known good applications to remove the headaches that come with traditional application whitelisting solutions by drastically reducing false positives during and after implementation. This NIST recommended approach combined with a globally automated whitelist lowers the burden on IT and lowers the barrier to entry for most companies to obtain and implement a zero-trust layer in their endpoint security stack.

Rob Cheng
PC Matic CEO and Founder