The Business Owner's Guide

To A Secure Remote Workforce

SECURA
Private & Secure Digital Life

Introduction

“We're being forced into the world's largest work from home experiment and it hasn't been easy.”

– Saikat Chatterjee (Gartner)

The Pandemic has caused businesses across the global to quick transfer into a remote working state. With the Coronavirus still lingering, many have experienced highs and lows in remote working.

However, 99% of people surveyed in a research by Buffer would choose to work remotely at least part time, or for the rest of their careers. However, during this lockdown period, many have witnessed security challenges, and cyber threats. Business owners now need to re-evaluate their current situation for a safer and secure remote workforce in the future.

This guide has been written to give business owners key information to make their remote workers safe and their business data secure.

How Can Business Owners Maintain Security When Employees Are Working Remotely?

Whether you are working with 10% or 100% staff working from home, your cyber security should not be scarified. By understanding the threats and by understanding the threats and implementing correct technology and training your staff, you can keep your business and workforce safe. Cyber-attacks can be very disruptive to working life, and can be even more alarming if they happen to an employee working remotely. Did you know every third business has suffered from a data breach?

Training

99% of data breaches occur as a result of human error. Cyber criminals are playing with the weakest link i.e. your employees.

From time to time, employees do click on phishing emails or forget best practices.

But you can eliminate the risks by introducing regular training and updating your staff with the latest trends to look out for.

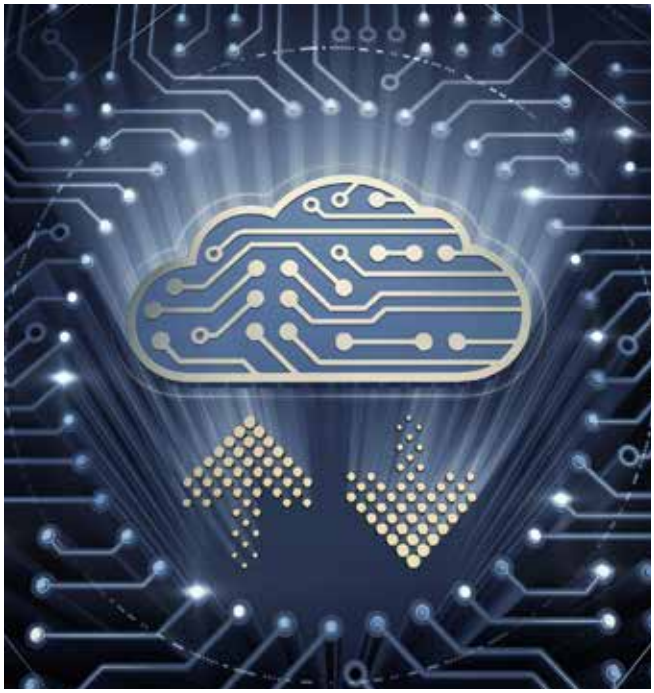
Invest In Endpoint Protection

Investing in security is costly but trusts us it's the best investment your business can make. With remote workers, the endpoint physical assets (e.g. laptop or desktop computer) aren't within your office. So you need the best security software installed and updated on these devices. End point services may include antivirus, email filtering, web filtering, and firewall services.

Consider A VPN Or Cloud Services

To improve security, a VPN (Virtual Private Network) allows you to have an encrypted connection over the internet. It's separate to public networks, so there's less exposure. Accessing systems through a VPN can be a bit frustrating for users, so cloud-based services are another option.

Your network is managed by a remote provider who protects all your data and employees can access files wherever.



Restrict Or Re-evaluate Employee Access To Data

Identifying users and restricting access is good practice for all businesses.The more access, the more risk, only share permissions according to job roles.

By doing this you can restrict access to the most sensitive business data by avoiding accidental and malicious incidences.

*"Overly Complex Access Permissions Are A **Gift To A Hacker**"*

Use A Password Manager

Passwords are the biggest gateway to accessing information, and if that is weak, then can is easy for anyone to get inside. No-one can remember loads of complicated passwords, and that's why most people use the same password for all accounts. But password managers can keep all your online accounts secure by storing encrypted passwords. These can then be easily shared by different remote employees.

Work from home can be beneficial for both employers and employees. With 74% of businesses intending to shift some employees to permanent remote working roles, these employees will typically safe $4,000 a year. However, by adopting certain security practices and introducing a blend of technology, policies and cyber security training, you can keep your business protected in the long term.


SECURA
Private & Secure Digital Life