

6 ways you can secure your remote staff - blueAPACHE

Canonical: <https://www.blueapache.com/blog/6-ways-you-can-secure-your-remote-staff>

Details:

2020

As a result of COVID-19, many organisations are finding themselves transitioning their workforce to work from home. This can be challenging as many organisations have never prepared for a scenario like this. Moving at short notice from a trusted office environment to working remotely can create security risks. The following six tips provide a good starting point for businesses looking to ensure their remote staff can work in a secure manner.

Strong Passwords

Employees should use strong and separate passwords for all their personal and company provided devices, e.g. computers, mobile phones, tablets. Wherever possible, employees should use 2FA and bio-metric verification.

Patching and Updating

Set up automatic software updates for the operating systems and applications of your computer or mobile phone and monitor the updates.

Antivirus

Verify that the computer at home has antivirus software installed and the home router's security measures are intact.

Secure Networks

Make sure the home WiFi is secured and protected via a strong password. Public WiFi should not be used when working remotely.

Physical Security

Employees should look after business assets by keeping them in a safe and secure environment. Children, guests or other family members using your work computer can accidentally erase or modify information, or, perhaps even worse, accidentally infect the device.

Phishing

Cyber criminals are already using the Coronavirus as subject matter for their phishing scams, hoping that the unwary will click through and hand over passwords or other data. Employees should not open attachments and click on links from suspicious email messages and SMS messages. Contact us today to find out how we can help you implement best practice security measures for remote staff.

What prompted the blueAPACHE blog post '6 ways you can secure your remote staff'?

The post was written because, as a result of COVID-19, many organisations found themselves transitioning their workforce to work from home, often without prior preparation for such a scenario, which can create security risks.

What is the first tip you give for securing remote staff?

Employees should use strong and separate passwords for all their personal and company provided devices (computers, mobile phones, tablets), and wherever possible use 2FA and bio-metric verification.

What do you recommend regarding patching and updating for remote workers?

Set up automatic software updates for the operating systems and applications of your computer or mobile phone and monitor the updates.

What physical security advice is given for remote staff?

Employees should look after business assets by keeping them in a safe and secure environment, since children, guests or other family members using a work computer can accidentally erase or modify information, or even accidentally infect the device.

How long does it take to read the blog post?

Estimated reading time: about 2 minutes, based on 285 words of article text on this page at 200 words per minute, excluding the Q&A and image list.