

4 Ways To Protect Your Employee's Devices

TechRounder PDF Edition

Live article: <https://www.techrounder.com/security/4-ways-to-protect-your-employees-devices/>

By Vipin PG | Published February 6, 2020 | Updated September 26, 2022 | Format: Analysis | 3 min read

In brief

In a time where more and more employees are using their own devices for work-related purposes, it has never been more important for business owners to consider cybersecurity and how they can protect these devices (which have access to sensitive company data).

In a time where more and more employees are using their own devices for work-related purposes, it has never been more important for business owners to consider cybersecurity and how they can protect these devices (which have access to sensitive company data). This is particularly true when you consider the fact that cybercrime is a growing problem with advanced new threats constantly being developed. It is important that you find ways to protect these devices so that you can protect the company, staff and customer data while keeping the operation running smoothly and efficiently. Here are a few tips which will allow you to do this.

1. Staff Training

Perhaps the most important step to take is staff training as employee negligence is often what leads to a breach. You need to take time to educate staff on how they can use their devices safely and safeguard sensitive data - this will include tips such as:

- Using complex passwords
- Using two-factor authentication
- Never opening attachments from unsolicited emails
- Teaching them about common scams
- Being careful when connected to public Wi-Fi
- Making regular backups to an external device
- Deleting data when it is no longer required on the device

2. Create A BYOD & Cybersecurity Policy

Following this, a BYOD policy also needs to be in place. This will outline the rules for how staff can use their own devices and what level of support you will offer as a company. A cybersecurity policy should also be drafted which outlines the rules for safe usage of devices - both of these policies should provide protection while also helping staff to understand what is and what is not allowed.

3. Endpoint Security Solutions

In a time where there will be many devices connected to the corporate network, it is important that an endpoint security solution is in place from a specialist like McAfee. This provides robust protection for every endpoint connected to the network and will allow you to safeguard the corporate network as well as protect every device from the latest cyberthreats. This usually includes valuable features such as antivirus software, a firewall and a VPN for safe usage of devices.

4. Data Encryption

Data encryption is an intelligent way to protect the data on employee devices and prevent unauthorized access. One of the biggest concerns when it comes to BYOD is what would happen if an employee device was lost or stolen because it could provide easy access to sensitive data, but when this data is encrypted and the IT department have control of the encryption keys it can help to keep important data safe.

These are the best ways to protect employee devices, which can allow staff to use their devices with confidence while also providing protection to the entire company and sensitive data. There are many perks to BYOD and it is certainly worth implementing, but it can also pose a threat. Therefore, you will need to make cybersecurity a priority so that you can protect the device and business from the latest digital threats.

You may also read

- These Trends Are Driving the Growth of the Cyber Security Industry in 2020
- Choosing A Cyber Security Firm For Your Business
- Quick Overview of Mi MJSXJO2CM 360 1080P WiFi Home Security Camera

References

1. theverge.com - 2017 / 6 -
<https://www.theverge.com/2017/6/17/15772142/how-to-set-up-two-factor-authentication>
2. mcafee.com - enterprise / en-us -
<https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint.html>
3. whatismyip.com - what-is-a-vpn - <https://www.whatismyip.com/what-is-a-vpn/>