Beaming

Business guide to:

Securing Remote Workers

Navigating the complexities of a modern, flexible business model means finding the right balance between productivity and security. With employees working from home, a local café, or even abroad, your organisation's network perimeter has expanded far beyond the walls of the office. This shift introduces new security challenges that demand a strategic and comprehensive response.

Our guide will walk you through the essential security measures needed to protect your organisation and empower your remote team to work securely from anywhere. We'll explore a layered approach that combines robust technology with clear policy and employee education, providing you with a complete framework to defend against today's evolving cyber threats.

Guide to the security measures organisations need to consider when enabling remote work:

1. Enforce Strong Authentication

Require multi-factor authentication (MFA) for all remote access.

Without MFA, a cybercriminal who gets a user's password can gain full access to the network. With MFA, the stolen password is useless without the second factor.

Enforce use of password managers.

A password manager provides users with an easy and secure tool that makes it simple to follow the best practices of using strong and unique passwords for all their accounts.

Each user should have their own secure login credentials.

This prevents unauthorised access and makes it possible to quickly identify and respond to any suspicious activity on the network.

2. Secure all Endpoints

Deploy endpoint protection software (antivirus, anti-malware).

As devices such as laptops, desktop computers, and are often the points of for most cyberattacks, Endpoint software will protect them from a range of digital threats.

Enable full disk encryption (e.g. BitLocker)

This will protect all the data on a computer's hard drive by encoding it. This makes the data unreadable to anyone who doesn't have the correct decryption key.

Configure automatic screen locking after inactivity.

This helps prevent accidental data exposure in shared spaces.

Ensure updates are applied regularly on all software and operating systems.

This is essential when some devices are outside the protection of a corporate network, making them more susceptible to attack if left unpatched.

3. Harden Home Networks

Educate employees on changing default router passwords.

Leaving the default password unchanged makes it simple for attackers to gain access to the router, allowing them to monitor or redirect the user's traffic and potentially compromise sensitive data.

Require WPA2 or WPA3 encryption on Wi-Fi.

These are the most secure Wi-Fi encryption protocols, protecting all data transmitted wirelessly from a device to the router. Requiring this ensures a remote worker's data cannot be easily intercepted by unauthorised parties on the same Wi-Fi network, preventing data theft.

Encourage use of personal firewalls and secure Domain Name System (DNS) settings.

Personal firewalls and secure DNS settings provide an essential extra layer of security for remote workers who are outside the protection of a corporate network. They help to block malicious connections and prevent attackers from monitoring internet traffic or redirecting users to fake websites.

4. Use a Secure VPN or Zero Trust Access

Provide a corporate VPN with strong encryption.

Leaving the default password unchanged makes it simple for attackers to gain access to the router, allowing them to monitor or redirect the user's traffic and potentially compromise sensitive data.

Consider Zero Trust Network Access (ZTNA) for granular control.

This provides more granular, application-specific access beyond the traditional VPN model. This reduces the network's attack surface by only granting users access to the specific resources they need, rather than the entire network.

Monitor VPN usage and enforce session timeouts.

Prevent a prolonged, unmonitored connection that could be exploited by an attacker. This practice enhances security by ensuring active connections are legitimate and by automatically disconnecting unattended sessions.

5. Protect Data Everywhere

Use Data Loss Prevention (DLP) tools to monitor sensitive data.

These tools monitor data as it is used and shared, blocking unauthorised transfers to protect against data breaches.

Store files in secure cloud platforms (e.g. SharePoint, OneDrive).

Storing files in secure cloud platforms is crucial as it protects company data from being lost if a remote worker's device is lost, stolen, or fails. It also provides centralised control and ensures all data is backed up and securely accessible for collaboration.

Avoid local storage or USB drives for company data.

These methods introduce a high risk of data loss or theft. Data stored on a local device or an easily-lost USB stick is vulnerable if the device is compromised or misplaced.

6. Defend Against Phishing and Social Engineering

Train employees to spot phishing emails and suspicious links.

Empower remote workers to identify and avoid malicious links or attachments that could lead to a system compromise.

Simulate phishing attacks to reinforce awareness.

Reinforce security awareness and test the effectiveness of employee training in a safe environment. It helps to keep cybersecurity front-of-mind and provides actionable data on where further education is needed.

Provide a clear process for reporting suspicious activity.

Enable fast identification and containment of potential threats across the organisation, allowing the security team to act quickly on suspicious activity.

7. Monitor and Respond

Use security monitoring tools to detect anomalies.

Tools can spot things humans can miss and allows the security team to identify and investigate potential breaches in real-time, even when devices are off-site

Enable remote wipe capabilities for lost or stolen devices.

This feature allows the security team to remotely erase all data on the device, preventing an unauthorised party from accessing it, critical for protecting sensitive company data if a remote worker's device is lost or stolen.

Have an incident response plan tailored for remote scenarios.

Provide a clear, pre-defined procedure to follow during a security incident. This ensures the team can respond quickly and effectively to contain a breach on an off-site device, minimising damage and data loss.

In Summary

Securing employees who work from anywhere requires a comprehensive, layered approach that combines robust technology with user education. The most effective defence is maintaining the best tools, supported by well-informed employees, trained to spot and report phishing and other social engineering threats.

Beaming can support you to keep your remote teams as secure as possible. Get in touch to find out more.

We are Beaming, an internet service provider for businesses. Since 2004, we have been providing companies across the UK with dependable voice and data connectivity.

We understand that every business is different, so we make an effort to get to know you and your needs. We can work with you to help store data safely, run applications smoothly, and keep your business online.

Our goal is to be a helpful advisor to you and your team. We're always here to answer your questions and help you solve any problems to keep your network running smoothly.

If you need a new connectivity partner for your business, we'd love to have a conversation.

Get in touch

Speak to our experts: Call 0800 082 2868
Or email hello@beaming.co.uk
Or visit www.beaming.co.uk

Certificate Number 9849
ISO 9001, ISO 27001