ESSENTIAL VPN FACTS FOR WORKING FROM HOME

neoRhino
IT SOLUTIONS

BEING SECURE FROM HOME SHOULD NEVER BE OVERLOOKED.

Protecting your data and securely accessing your business' internal resources goes beyond having an anti-virus program and firewall. Having a VPN is just as important.

Anti-virus programs and firewalls mainly protect your endpoints. VPNs provide access to and protect your network data while you access it over the internet. VPNs need to be implemented now more than ever as we are adapting to working from home during this current health crisis.

1

EQUIP YOUR ENDPOINTS WITH A VPN

Ensure that all endpoints that access your internal network are equipped with a VPN. This includes work-issued mobile devices such as smart phones and tablets.

2

HAVE A VPN POLICY IN PLACE

For business owners implementing a VPN, ensure that you have a solid policy in place for your employees. Keeping logs of your network activity helps protect your resources and to evaluate the endpoints that are connecting. Also, have a protocol to execute if a potential data breach occurs.

3

VPN ISN'T FOOL-PROOF

VPNs are not guaranteed or perfect. Continue to follow cybersecurity practices such as avoiding public Wi-Fi, watching out for phishing attacks, and fully knowing who you are sharing files with.

YOU CAN NEVER BE TOO SAFE.

When you are working remotely, having the extra protection and access that a VPN provides is crucial. If your organization does not currently have a VPN implemented, then you should contact your IT provider as soon as possible. There are several options and neoRhino can determine what your best option would be for enterprise VPN implementation.