Working remotely

INFOSEC

Working remotely is safer, right?

Working remotely means you may be working with a home setup you can control, but if you're working from someone else's Wi-Fi, it may not be secured. Physical security is a concern without the protection of the secured office.

So I need a strong Wi-Fi password, right?

Definitely! But not just that. Your router has a separate password, one that you may never have changed. Make sure your router and Wi-Fi passwords are both strong and unique.

My router, too? Is there anything else that needs a password?

Phones, tablets and smart devices all need strong passwords. It's especially important with smart devices, which often come with default passwords that are forgotten or ignored, just like routers.

This sounds like a lot of trouble. Can I just use someone else's Wi-Fi?

It's not a good idea to work remotely over someone else's network. You don't know what protections (if any) that person or business has set up. Despite this, a survey found that 81% of people still connect to unsecured public networks.

What about the home office itself?

Setting up a home office means you're in charge of physical and digital security. It's important to invest in antivirus, shred unneeded documents ASAP, follow your organization's security policies to the letter and make sure that family members and friends don't use your work computer.

What's one thing I can do to improve my remote security?

Set up a VPN. A VPN, or Virtual Private Network, establishes a secure encrypted connection, tunneling data directly from the host to its destination. This is a great way to protect information when it's traveling across an insecure network.

Sources: https://oneworldidentity.com/despite-security-risks-free-public-wi-fi-81-percent-still-connect-owi-labs-survey-finds/

© 2019 Infosec. All rights reserved.