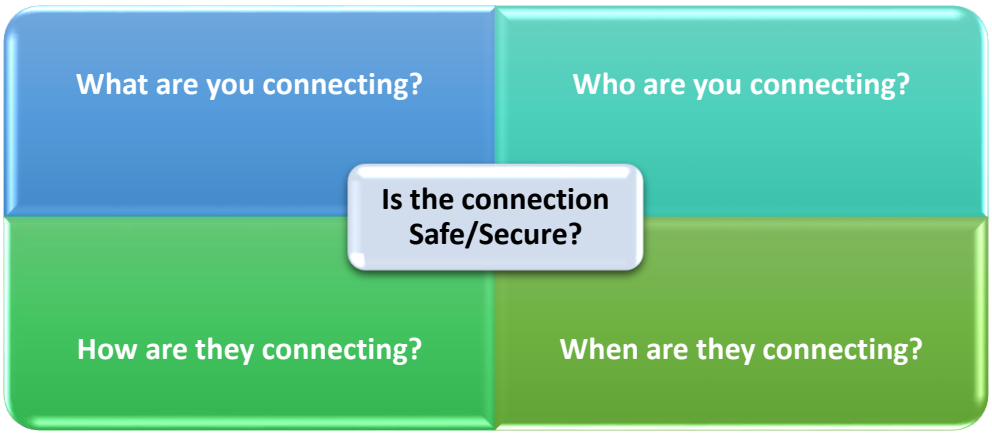
# Covid-19: Cybersecurity considerations for remote working.

As a Vistage speaker I'm currently having a lot of different types of conversation about Covid-19. One question that is increasing during my Cybersecurity masterclasses is "What things (both from a cybersecurity and a technology perspective) should we consider with staff working from home due to the Coronavirus outbreak?" and that's the purpose of this article.




The basic building blocks that you need to be thinking about are what, who and how are you connecting, when do they need to connect and is the connection safe and secure?

If you allow users to connect to your systems there is always a risk, if their machines are not secure then by default nor are yours, whatever access you're giving and however you're going to facilitate it you need to be thinking about security and your human firewall. Your human firewall is both your best line of defence and also your biggest risk.

A common issue I'm seeing is that in the past people have asked staff whether they are able to work from home (have access to a computer) and have been told yes, the nuance with the current scenario is that we need to consider what happens when an entire family is working from home. Do all your people have sole access to a machine?
For some the solution is to allow staff to take their work machines home with them (laptop users probably do this anyway), if you're doing this with a desktop you need to think about connectivity, most home networking is Wi-Fi so you'll either need a Wi-Fi dongle or consider long CAT-5e ethernet cable to run from the machine to the home router.

An increasing number of applications are now cloud based and this of course makes remote working a lot easier but for any on-premise applications you are going to need to be using a remote access tool. Which you use will probably be decided on what your IT team/provider are most proficient at using and your appetite to ease versus cost.

With increased concurrent remote users accessing an on-premise solution you may face speed issues due to the size of your connectivity pipe. Many people have a larger bearer (the pipe that carries the service) than the service they are paying for, this is a great scenario as it is quick and easy to increase the speed of connectivity for your office.

A good anti-virus product needs to be used by everyone. For many people they've got a good anti-virus policy in the office, but they have no control over what people use at home. Consider a licensing agreement whereby home users are provided for under the office license agreement, this allows you to ensure that everyone has good protection. Don't allow users to use free anti-virus software, in my opinion, you get what you pay for!

● www.ramsac.com ● rob.may@ramsac.com ● https://twitter.com/robmay70
● https://speakers.vistage.co.uk/speakers/rob-may

Now more than ever you also need good password policy and wherever available please use multi factor authentication (2FA/MFA).

Don't be fooled into thinking that having a VPN provides you all the security that you need, by themselves that is not what are VPN does. A VPN is about providing privacy and a private connection rather than a secure connection. A VPN is a private tunnel from a user to the main system and it's imperative that we take the security steps to ensure that the tunnel is secure at both ends - if not the bad guys can simply come through the tunnel and attack your systems.

It saddens me but unfortunately cybercriminals are making the most of the current environment of heightened fear and using Coronavirus to attack users and their machines. There are a lot of cyberattacks and malware problems being delivered under the guise of either Covid-19 advice or as an interactive Covid-19 Virus Outbreak Map. Please advise your users to be aware of this and not be tempted to click on social media clickbait.

Coronavirus related spam is also booming now, in addition to the usual filtering platforms I recommend you can reduce the problem by getting your mail domain and system administrator to lock down your generic email accounts.

You can help safeguard a machine by paying proper attention to the local-admin account setting. The user account that someone uses on their machine should always be set to 'standard' and not to 'local administrator'. In the office your IT team should have this in hand but at home many users have a default local administrator account. What this means is if the machine is compromised the attacker has full access to make changes and cause maximum harm. To fix this problem at home first create a new user as a local account (you do this under control panel and users). Name the account admin. Change that users account type to be a local administrator. Then select and change the normal user account type to be standard. Users should now use their standard account on an ongoing basis only switching to the admin account when they want to make changes to their machine configuration.

You must give thought as to what data remote users are generating and where it's stored as this has an implication on your GDPR responsibilities as well as prompting thought about backup needs and requirements. Where possible save to your corporate system/cloud solution and if not, you may need to consider a local backup solution such as rotating external hard drives.

As more people start to work from home, we will see more webcams being deployed, it is worth opting for a camera with a lens cover and if not supplied with one add it retrospectively (they can be obtained easily and cheaply online). Most webcams have an activity light but it's possible for malware to disable that. The internet will show you thousands of live feeds from hacked security cameras and you don't want any voyeuristic crime in your home office.

One last thought, if you are asking staff to work from home who don't normally do so, you might not have thought about insurance implications. It's also important that you ensure that staff still comply with health and safety regulations. My advice to staff is that when you're working from home, you need to make sure that you create a suitable environment that protects you from postural risks, in the same way as you would at work. Make sure you sit at table of a suitable height, using a chair that enables you comfortably use your keyboard and mouse and allows you to rest your feet on the floor. If staff need to take a monitor/keyboard home to work for long periods facilitate that and ensure that your managers are talking to their direct reports to ensure that they can work safely and securely.

I hope this is useful, if you have any questions please feel free to email me and I will respond as quickly as possible.

If you think this information might help someone else too, don't hesitate to share it.

Stay safe!

● www.ramsac.com ● rob.may@ramsac.com ● https://twitter.com/robmay70
● https://speakers.vistage.co.uk/speakers/rob-may