Preparing for security when isolating.

Prepare equipment.

Before laptops are taken home make sure the software has been updated to the latest version which includes the latest security updates. You may also want to activate automatic updating on devices to ensure they are still being updated regularly when people are working remotely. This should cover phones and tablets as well as laptops.

Make sure up-to-date security protection is installed and active on any devices that will be used for work. Make sure firewalls are enabled, anti-virus software is installed, and device encryption is in place. If this comes as standard on the hardware, make sure it is switched on. Some updates can disable security settings.

Make sure all people have password managers in place and are using them, make sure they are using strong randomly generated passwords (macOS has Keychain Access as standard). Don’t allow the reusing of passwords, every system or account should have a unique password. If an existing password has been in a data breach, hackers can find it in seconds. Make sure any default passwords on equipment has been changed. We can literally find them on Google.

People may not have taken the time to protect their home network, including Wi-Fi routers. Advice should be given to home workers on how to best do this.

If you’re sending hardware out to your staff encourage them to disinfect it. Maybe even send antibacterial wipes with it. If anyone infected had used the hardware before it was sent it could carry the virus.

Make sure networks are secure.

If there is a choice between using a free Wi-Fi network or mobile phone data, choose to use the phone data, however VPNs (Virtual Private Networks) are the best solution.

Although VPNs are now marketed as a way of hiding IP addresses or access Netflix content from another country, they are also useful for encrypting data in transit. A VPN allows companies to extend their private network over the Internet in a secure way, allowing “internal” resources to be shared with employees working from home. Companies should look to locking down access to cloud services (such as email etc.) to their internal network and give users VPN access to the network.

VPNs should be used whenever business information is being sent or received outside your company’s standard private network. This includes any public or free Wi-Fi as these are unlikely to be secure, but also home Wi-Fi as it would be difficulty to verity the security of each employees home network, or indeed any other network they might connect to such as a friend or relatives.

Smaller companies may need to set up a VPN server before they can safely introduce home working. There are lots of VPN service providers, even free ones, however these probably won’t be suitable for work users. Although they provide encryption which can be useful on an untrusted network, it can be risky not being in control of the endpoint. More importantly, you won’t be able to benefit from sharing internal company resources over the Internet with them.

Most larger companies will already have a VPN in place but should still stress test it. If it can't cope with the additional volume of traffic people can become frustrated trying to get access and may decide to bypass it. If it's struggling with the additional volume, prioritise who needs to be on it most. Have allotted windows for workers who don't need to be on it all day to sign in to access drives and send emails.

VPNs can be extended to phones and tablets too.

Keep your data safe.

Storing information locally (on a desktop or hard drive) puts it at greater risk. If the device is lost or damaged the data could be lost. If the device is compromised the data could be leaked.

Consider secure cloud services such as Office 365 or iCloud. There are some inexpensive options, and they will provide security as part of the service (just make sure the passwords are secure).

Make it a policy to backup all data to the cloud either as a default setting or at the end of the day. If you need to share large files, cloud storage and data sharing solutions are a good call. They reduce the need for external drives which can be infected with viruses (both the cyber and physical kind), or be accidentally wiped, lost or shared.Try to separate work and home.

Make it clear to employees that work equipment is for work use only. It's really tempting to stream movies on a work device, but don't take the risk. Keep work and personal use separate.

The same goes for using personal devices for work activities. It's a risk. You can't control who people might share devices with, what they access or what they connect to on their personal devices and it's not reasonable to police this unless the employee has agreed. This means personal devices will always be higher risk.

If you are asking staff to use personal devices, limit this as much as possible. For example, it's lower risk to allow emails on a phone than full system access on a personal computer.

A BYOD (bring your own device) policy is helpful if personal devices need to be used, as it sets out what is expected of personal device use and under what circumstances. Some of the guidance in this document would be relevant for securing personal devices, but you would want to add in things like a separate user accounts for work on some devices, and not sharing passwords with family or children.

Don't make security a punishment.

Security is already seen as a blocker by so many people, which is why it's so often bypassed. Involve your people in conversations about good security and how it benefits all of us. If it turns out they've been reusing using weak passwords don't shame them for it, show them how to use software to make them stronger.

As ethical hackers, Digital Interruption are committed to using our skills to help organisations become more secure. We run training and provide advice and guidance for smaller companies. For more information visit **https://www.digitalinterruption.com.**

Digital Interruption.