Covid-19 Briefing #1 – **Home working and WiFi Safety**

If your staff are using their home Wi-Fi to access your systems, consider the risk that another machine on the home WiFI network may be infected, which may lead to other computers or devices on the network being infected as well.

If that risk becomes a reality, there is a further risk that the home computer used to access your systems, even via a VPN for example, may infect all the other machines in your business as well.

It is unlikely that the security measures taken at home are anywhere near as comprehensive as in your business, so it is more likely that a family member's computer is more easily compromised.

Sharing the home WiFi network does increase the vulnerability to a work-related computer.

The following measures can mitigate the risk:

- ensure that all devices on your WiFI network have secure passwords (eg CCTV cameras may have factory settings such as 0000)

- call your internet provider and ask them to talk you through setting up a guest-WiFi at home to isolate your machine and not connect to the family WiFi (not allowing other family members or visitors to access the guest-WiFi);

- download and set-up Multi Factor Authentication on all your devices and all Apps, including Facebook, Twitter, etc, assuming you're using a password manager, otherwise hackers can monitor your log-in details including passwords… go into 'security settings' of your password manager, to ensure it alerts you for a code when a hacker is trying to gain access;

- a standard virus-checker, which release an update every 4-6 weeks, only protects you against known threats, but every second there's 4 new versions of ransomware, so consider using two or more reputable solutions to keep you safe in real-time (noting that your ISP is using standard anti-virus solutions, so may also be 4-6 weeks behind on patches); and

- consider encrypted and protected remote hosted desktops, so even if the home machine gets infected, the remote hosted desktop does not get infected (remembering that it should also be protected) – a remote desktop, instead of using the processor in your computer, is where you use your mouse and keypad, but are using the processor of another computer and using your screen instead… hosted means the security of the remote computer is not your problem.

In summary – work-related computers using home WiFi networks risk being infected over that network from other computers or devices using the same network that do not have the same level of security you would have at work. So, when subsequently connected to the work network, work-related computers also used at home may infect the rest of the machines connected via the work network. Mitigate risk to all data – commercial and personal – residing on machines that are connected, starting with the work-related computers used at home during COVID-19.

For the rest in the **Home Working** series, which includes "Using virtual meetings safely and lawfully", email info@priviness.eu

Covid-19 Briefing #2 – **Home working and using virtual meetings safely and lawfully**

Whilst working from home, no doubt you will be holding virtual meetings using various online audio and video conferencing and collaboration tools – not just to connect to colleagues, but also with friends and family. This creates a constant fluidity between your working and private lives where it is more difficult to distinguish between the two: where you would normally leave work life behind in the office at the end of the day, with its policies and practices, and leave your private life at home when you go into work, these boundaries no longer exist.

There is therefore an increased risk that you will share accessible data – commercial or personal – with your newly extended virtual community using your own device or computer at home: what you would reasonably share with colleagues at work may be shared with friends or family; and similarly, the other way around, you may share the private lives of family and friends with individuals at work.

It is one thing to moan about an episode in your work life at home or talk about an event at home in your work life, but it is entirely another matter when you use automated means to do so.

Your guard is naturally down at home where such strict work-related policies and practices are not noticeable, so it is more likely you will forget these policies and practices in a home environment.

The following measures can mitigate the risk:

- at home, use work-related computers for work purposes and home computers for your private life – this not only separates the chance for cross-sharing information between work and private lives, it also creates a discrete barrier to focus on work during a working day;

- in general, whilst working, try not to use your computer to share details relating to your private life, and refrain from going into detail about your work life with family and friends;

- do not record conversations in meetings with those involved with work unless consent is provided by each of them – remember if permitted to record them, you need their separate consent to further share the recordings – unless there is another lawful basis to do so;

- if you receive a recording from someone, ask them to confirm it was legitimate for them to record and / or share – the same applies, if you aren't sure, to any data they share with you; and

- always be mindful of what you type or share about other people, and if a recording is permitted, be careful what you say about them – you never know where it might go.

In summary – for those unused to working from home, boundaries between work and home get blurred, especially when using separate online tools on your home computer or device to connect to individuals in your working life whilst simultaneously communicating with family and friends. You risk sharing work-related data with family and friends, and risk sharing the private lives of family and friends with individuals you are connected to in a work-related capacity. Mitigate the risk to cross-sharing data, including recordings, by keeping work life at home separate from your private life.

For the rest in the **Home Working** series, which includes "Home WiFi network safety", email info@priviness.eu

Covid-19 Briefing #3 – **Home working and keeping data just as safe as at work**

With much attention on COVID-19, it is easy to take your eye off the ball whilst working from home, especially in terms of some of the general principles that are designed to keep you, your colleagues and commercial interests safe, as laid out in the policies and practices in your workplace. It is worth noting though that these can be equally applied when working from home.

At the heart of everything we do is data – commercial and personal – and BYOD (bring your own device), acceptable-use policies, information security as well as data protection documentation are important manuals that help to guide our everyday work procedures, whether in the office or at home. Being busy in our daily jobs, there is a risk that these have gathered dust, as might your normal governance protocols as you and colleagues work from home.

It is all too easy to forget in the confines of your home that treating data with respect is no less important than it is at work. You would not allow another person to share your computer at work, but you may well do at home, because you naturally have a stronger trust in your family – but this is how mistakes happen and increase the risk to data that you are responsible for.

We tend to keep to a stricter code at work (partly to ensure we keep our jobs), whilst in the more familiar setting at home, where we are more likely to speak our mind with our loved ones, the risk of careless comments increases due to our looser tongues (where you are more likely to be forgiven for speaking out of turn). Integrity and confidentiality risks need to recognised and mitigated.

The following measures can mitigate the risk:

- do not leave your laptop in your garden office whilst you disappear inside for lunch with the family;
- do be aware of prying eyes and, as the old adage goes, "*keep mum*";
- do not send work-related material to personal accounts;
- keep personal data regarding other people relating to work private when working at home; and
- take time to re-read work policies to both refresh yourself of them, as well as to consider if there are omissions or elements that are now out-of-date.

In summary – by design, home is where you are supposed to have the least amount of boundaries. What you do or say does not come under the same scrutiny as at work – at home, the consequences of your actions are not the same as they are in the office. So, when working from home, without the same general regard for tight policies at work, the risk to commercially-sensitive and personal data is heightened, not so much because family members can't be trusted, but because of the increased possibility of mistakes occurring when work-related practices and procedures are less evident. The risk increases when your home is a shared flat with strangers. Mitigate the risk of exposing data to unauthorised access or accidental loss by re-familiarising yourself with office policies.

For the rest in the **Home Working** series, which includes "Protecting privacy safely", email info@priviness.eu