COVID-19 and how to securely work from home – key recommendations

The current COVID-19 crisis has led to an exponential increase in the numbers of WFH – people working from home – to safeguard public health. At the same time, there is an increased risk in terms of Cybersecurity. This is predominantly caused by two factors:

- The re-distribution of workplaces away from the office and the spike in using virtual collaboration platforms has substantially widened the attack surface. This can threaten the digital infrastructure we now rely on more than ever for business continuity. It could even threaten critical infrastructure and provision of critical services, if not addressed pro-actively.
- The COVID-19 crisis provides adversaries with new opportunities for targeted attacks, whether these are phishing emails or targeted scams. These tactics are intended to take advantage of citizens who are naturally concerned about their health and safety and are particularly vulnerable.

Hence, it starts with you: stay safe and stay secure. To do so, follow these eight tips for cybersecurity in the home office:

Bring home only the devices and information that are absolutely necessary

The best way to protect information or devices against loss is by not removing them from their accustomed company environment in the first place. This way, they won't get lost in transit or in your home. So, make sure you take home only the devices and information that you really need.

Safeguard your home network and communicate via secure connections

Because you'll be using your private network at home, you'll have to protect it accordingly, with strong WLAN encryption, a unique and complex password, and regular updates. Always work via a secure connection established by VPN, especially if you're also exchanging sensitive information or are accessing the Intranet.

Keep the software on all your devices up to date

Working from home, company and personal devices use the same network. Data traffic passes through that same router that's connected many other devices including various smart home appliances which, in the worst case, may not have any up-to-date protection. All these are potential gateways for hackers, which is why it's recommended that you allow all your devices, whether company or personal, to update automatically.

Switch off voice-controlled smart devices at your home workstation and cover the webcam when you're not using it

Voice assistants listen to what's being said in the room and transmit it to the provider. The possibility of these recordings falling into the wrong hands can't be ruled out. So, such devices have no business being in rooms where you discuss important matters or should at least be switched off. And be sure to cover the

webcam on your PC when you're not using it and be careful what you share via the video function.

Don't mix personal and business use of devices

Make a clear distinction between devices and information for business and personal use, and don't transfer any work data to personal devices. This will prevent any unintended outflow of information. As a side effect, it also helps to psychologically separate the time you are "at work" from the time you are "at home".

Proactively identify all participants in online meetings

Teleconferences and video conferencing tools are an excellent substitute for in-person meetings. At the same time, however, it's more difficult to verify whether everyone on the line has actually been invited. It's especially easy for unauthorized persons who have acquired the dial-in data to sneak into large online meetings with lots of participants. That's why everyone displayed in the meeting software needs to briefly identify themselves, particularly if you're discussing sensitive topics and sharing presentations on the screen.

Log off when you stop using your devices and store them securely

Even if you're only taking a short break, lock the screen of your PC and mobile devices just as you would at work so that they aren't accessible during your absence. And, of course, you also need to safeguard the devices themselves against unauthorized use or even theft when they're in your home.

Be extremely wary of suspicious e-mails or attachments, particularly if you don't know the sender

Especially in the familiar environment of your home office, you need to be wary of suspicious e-mails. Studies show that the likelihood of falling victim to malicious intentions is particularly high at home. In addition, do not be pressured by emails asking for immediate action or referring for example to the current COVID-19 crisis. Take your time and examine each e-mail thoroughly before you open it. For more information on phishing e-mails, and COVID-19 scams, for example visit:

https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

https://www.who.int/about/communications/cyber-security

Overall, with business continuity increasingly based on digital infrastructure, it is more important than ever to revisit organizational measures for more effective Cybersecurity to manage these risks. Key recommendations to do so, especially for Small and Medium Enterprises, are summarized in the booklet "Seeing Cybersecurity as an Opportunity" (https://www.charteroftrust.com/topic/seeing-cybersecurity-as-an-opportunity/).

You may find further resources here: https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics