# Top 10 Cyber Security Tips for Homeworking

The COVID-19 outbreak has turned many regular office goers and commuters into home workers. They have been thrust into an environment that is both familiar and strange that can pose novel risks for both staff and their employers. These Information Security Forum top tips can make your experience more safe and secure:

## About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its members. Find out more at **www.securityforum.org**

in Information Security Forum
@SecurityForum
+44 (0)20 3875 6868

**1. CHOOSE THE RIGHT ENVIRONMENT**

Try to work from the same room or location every day. Picking one spot has a number of benefits. It'll come to feel like your workplace helping you get into that working mindset. More importantly, it'll mean you only have to keep one place secure. If you spread yourself around your home you are likely to forget key steps that keep you, company data and equipment safe.

**2. PROTECT YOUR WIFI**

Change the default password on your home router if you've not already done it.

**3. GENERATE SENSIBLE PASSWORDS**

Home working is likely to mean you have to generate a few new passwords. Be sensible about these – use a short phrase or a mix of letters, numbers and symbols. As you are at home you are probably safe to write them down but keep the list away from other family members.

**4. KEEP WORK AND HOME SEPARATE**

Especially when it comes to communications and sharing files and documents. Don't send company information across personal email or social network accounts – no matter how tempting that might be.

**5. AVOID CROSS-CONTAMINATION**

Don't use work equipment to log into your personal accounts on social networks and email systems.

**6. DON'T OPEN SUSPICIOUS CONTENT**

Be more vigilant about scam messages and emails, do not click on suspicious attachments or links. Con-artists will seek to piggy-back on the changes the outbreak has ushered in. If you are suspicious follow up with a phone call or a message sent via other means.

**7. AVOID COVID-19 HOAX MESSAGES**

Lots of messages about the spread of Covid-19 are being used to spread malware. Be wary of updates and warnings that arrive in your inbox but are not from your employer. If you do click where you shouldn't, call the appropriate IT support immediately.

**8. KEEP CALLS PRIVATE**

Make calls, via phone or video, from a private room at home. Don't do it in the local coffee shop.

**9. HIDE YOUR WEBCAM**

Put tape across the camera lens on your laptop. Before making a video call, look around to make sure no sensitive information is exposed. Look at what is on the wall behind you.

**10. SECURE YOUR DEVICES WHEN YOU FINISH WORK**

Shut down laptops and phones and keep them, as well as documents and devices, locked away when you are done for the day.

## FIND OUT MORE

Discover more useful resources at securityforum.org/covid-19