

Global Information Security Society for Professionals of Pakistan

Work from Home (WFH) Best Practices



Content

1. [Cyber Hygiene while Working From Home](#)
2. [Keeping Up with Your Self during work from home](#)
3. [Recommendations for Employers](#)

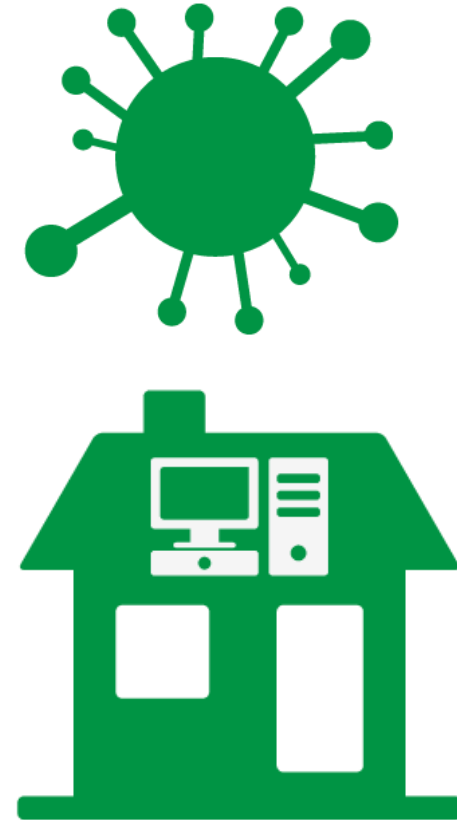
Stay Home Stay Safe



A public service message from GISPP

Cyber Hygiene while Working From Home

- Due to the on-going situations and happening because of the COVID-19 outbreak worldwide, Social distancing is strongly suggested and enforced as one of the major preventive measures against COVID-19 spread. Maintaining social distancing and adhering to state orders, most of GISPP members are **working from home (WFH)**. Earlier it was a common thought that things will become better and start getting back to normal in a week or so. However, it seems that most of us might be working from home for the entire month of April or later.
- With the latest technologies and technological workarounds, we can certainly continue our professional duties virtually. **Work From Home (WFH)** is all together is different from working in our offices as we require to adapt to our surroundings and situations. However, with an exponential increase in the number of people working from home, it is very important to take care of our **Cyber Hygiene**.



Cyber Hygiene while Working From Home

- GISPP gathered excerpt and listed out some best practices in the context of Information Security, to be adopted while working from home.
 - Allocate a workspace in your house, where you should be able to do video calls without any disturbance.
 - It is strongly recommended to avoid using personal devices for official work. On such devices, the level of risk is exponentially higher and there are more chances your machine may be compromised.
 - Your work machine (laptop/desktop) should be separate from the machine that will be used by your family especially children.
 - Your machines (laptop/ desktop) for work and family use, should be updated with the latest security patches and OS updates.



Cyber Hygiene while Working From Home

- Use licensed and updated anti-virus solutions on your machines.
- Make sure that your work machines are not used to download torrents or for visiting any suspicious or malicious sites.
- Always use the official VPN solution to connect to your office network and systems, which are authenticated using strong passwords and 2-factor authentications (2FA).
- Make sure to use strong passwords or keep changing them.



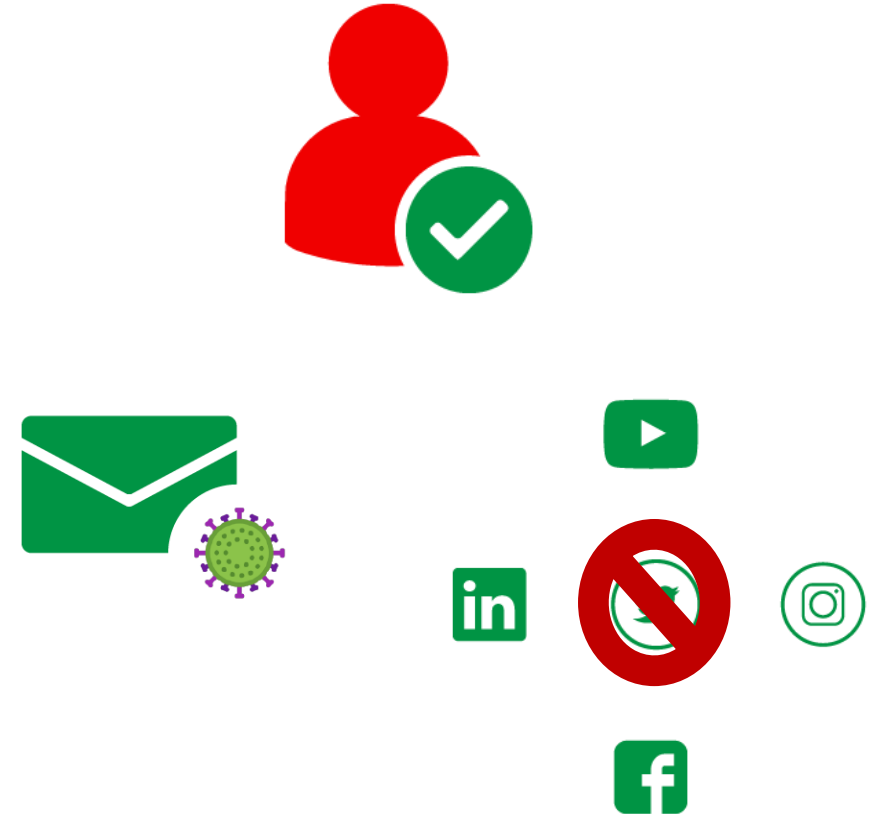
Cyber Hygiene while Working From Home

- If you receive any emails from an unknown source, always verify that the sender is legitimate / trusted and that the email is not containing basic phishing email attributes such as misspelt ID or words, grammar issues, etc.
- In the ongoing situations, be suspicious of any emails asking you to check or renew your personal or financial credentials; even if it seems to come from a trusted source. Always verify the authenticity of the request through other means (calling the source) and
- Never click on links or open/download any attachments in the emails, which seems suspicious.
- Emails that create an image of urgency or severe consequences are key candidates for phishing - in these cases always verify via an external channel before complying.



Cyber Hygiene while Working From Home

- Emails sent from people you know, but asking for unusual things are also suspect - verify by phone, if possible.
- Always report your IT Service Desk or Information Security Team, if you receive a suspicious email from an unknown source at your official email address.
- During the present days, If you receive a social media connection request (even on LinkedIn), verify the legitimacy of the account and delete the request if you do not know the person or connection requests seems inappropriate.
- Be particularly careful with any emails referencing the coronavirus in email ID, subjects or body; as these may be phishing attempts or scams.
- Do not disclose any of your activities or work-related matters on social media. Remember less is more.



Cyber Hygiene while Working From Home

- Use your company's official applications for online meetings and do not install any unauthorized applications on our work machine (laptop/desktop).
- Ensure that every online meeting is secured with a strong password and have a meeting ID to connect.
- Do not share the virtual meeting URLs on social media or other public channels. Unauthorized 3rd parties could access private meetings in this way.
- Disable the option of file transfer while in remote meetings, when not required.
- We should avoid logging into our official emails from personal devices. If these devices must be used, ensure that they are updated and protected (such as with antivirus software, defenders, firewalls, etc.).



Cyber Hygiene while Working From Home

- Consider using a spyware scanner from the list below:
 - Panda Free Antivirus (Panda Dome Free)
 - AVG Free Antivirus
 - SUPERAntiSpyware
 - Adaware Antivirus Free
 - Comodo Free Anti-Malware BOClean
 - Spybot Search and Destroy
 - Free Fixer
 - Norton Power Eraser
 - Malwarebytes Adwcleaner
 - Malwarebytes Anti-Rootkit



Keeping Up with Your Self during Work From Home

- Since social distancing, isolation or work from home is a new concept for most of us, so we have to make sure that getting distracted of our normal routines should not be burning us out and we make the best use of our time.
- We gathered a few social tips so that you can keep up with your selves while working from home.
 - Try to keep yourself organized and motivated.
 - While working from home, do not change your habits. Wake up at the same time, do the same things you would do when you use to go to work, and take regular and frequent breaks.



Keeping Up with Your Self during Work From Home

- Do not stay awake till late nights as you are expected to work from home in the morning, as official working hours remains the same.
- Do not keep checking news channel for Corona related updates. Too much exposure to news and information may have a bad effect on your mental state.
- Try to start your day early, possibly after Fajar prayer. Children will be asleep and you will be able to concentrate well and do work peacefully for a long period.
- Use a time management app like “Clockify” to keep track of the time and tasks.
- Use planner apps such as a planner by Microsoft. Add plan, add the task, add start and end date and follow it to deliver your office work.
- Take daily backups of your important and work-related data.
- Make sure that you make time for your family and not work continuously or even after work hours.



Planner

Recommendations for Employers

- If you are an employer, make your employees aware of recent security threats and ways to avoid and mitigate such kind of threats.
- Ensure that the corporate VPN solution is scalable and able to sustain a large number of simultaneous connections.
- Provide secure video conferencing for your corporate clients and teams (both audio/video capabilities).
- If you are an employer, set some core hours for which everyone has to be present. You can make the rest of the hours flexible.
- All the corporate business applications must be accessible only via encrypted communication channels (SSL VPN, IPSec VPN).



Recommendations for Employers

- Access to application portals should be safeguarded using multifactor authentication mechanisms.
- Prevent the direct Internet exposure of remote system access interfaces (e.g. RDP).
- Provide where possible corporate computers/devices to staff while they are working from home. Please ensure that these computers/devices have up-to-date security software and security patch levels and that employees are regularly reminded to check updates. A replacement scheme for failing devices should be also in place.
- Ensure that adequate IT resources are in place to support staff in case of technical issues while working remotely; provide relevant information, e.g. on contact points, to staff.
- Ensure policies for responding to security incidents and personal data breaches are in place and that staff is appropriately informed of them.



Reference: ENISA Europe Guidelines (<https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home>)

Contributors

- Shahzad Subhani (<https://bit.ly/SSubhani>)
- Amir Jamil (<https://bit.ly/AmirJamil>)
- Suman Siddiqui (<https://bit.ly/SumanSid/>)

Special Thanks to those members who provided their feedback in our WhatsApp groups .

