The Worshipful Company of Information Technologists

ADVICE TO HOME WORKERS DURING THE COVID-19 CRISIS

During the current emergency, many organisations and individuals find themselves using technology in ways they may not previously have been familiar with. Inevitably, there are people who see this as an opportunity to perpetrate criminal acts such as fraud, but even without active malice, mistakes happen, and things break down.

There is plenty of advice available, but most of it is not specific to the current crisis or too technical to be useful to many. The Security Panel of the Worshipful Company of Information Technologists has therefore produced the following guidance which we hope will help keep us all, and our places of work more secure and a touch safer.

1. USE WORK-SUPPLIED EQUIPMENT AND/OR PROCESSES WHERE POSSIBLE

Many organisations, even quite small ones, are able to offer their workers secure remote access into corporate machines. If you are lucky enough to be in that situation, follow your employer's guidance and don't ever do personal stuff on work machines, however tempting or convenient it may be.

2. ESTABLISH A WORK ROUTINE

You should consider Display Screen Equipment issues and take care to limit the amount of time you are working. With no commute and not a lot to do in a day the temptation is to carry on working too long and/or without breaks. Consider time differences if needing to work internationally and set working hours accordingly.

3. MAKE SURE YOUR PASSWORDS ARE IN GOOD SHAPE AND USE MULTI-FACTOR AUTHENTICATION WHERE POSSIBLE.

No identification system is 100% fool proof, but most successful ways of compromising accounts are still remarkably low-tech. If a service, particularly one involving money or online shopping, offers you an additional level of security, such as a code sent to a phone, or a smart authentication app, use it. Never use the same password for different services, otherwise you may find that your bank account has been emptied because someone hacked into that gaming site you last used a year ago.

4. BE ESPECIALLY VIGILANT ABOUT SCAM MESSAGES

There has been a significant increase in scams. Don't trust anything you receive by email, SMS, or phone call and which asks you to provide any personal information, go to a website, return a text message, or call a phone number. If it seems to be from an organisation or individual you trust, contact them directly by other means such as their published website or phone number in order to confirm its legitimacy. If someone calls you and asks you to call back, put the phone down and wait at least 3-4 minutes. Verify the phone number independently, and then call back.

5. WORK IN AS SECURE AN ENVIRONMENT AS YOU ARE ABLE TO ESTABLISH

Even at home, there may be unexpected risks. Can others eavesdrop unwittingly on your conversations? Are you sharing a house/flat with, or live next door to, people who work for competitors or whom you would otherwise not wish to share information with? Do you remember to lock screens when you leave your PC? Does your loud voice reveal your corporate secrets through the wall or window, or over the garden fence or out on the street? Does your webcam broadcast confidential information on a whiteboard or another screen visible to others in the house/flat or even outside? Are you having to share a computer with another family member or flat mate, or a desk? Does it matter that they may have access to your information?

About the Worshipful Company of Technologists

The Worshipful Company of Information Technologists is the 100th livery company of the City of London, combining centuries-old tradition with a modern focus, energy and innovation. The WCIT Information Security Panel, provides a global hub for leadership and co-operation in dealing with matters relating to 'Information Security'.

6. USE WIRED NETWORKS IF POSSIBLE AND SECURE WIFI AND ROUTERS AS BEST YOU ARE ABLE

WiFi is very convenient and may be your only way of accessing the Internet. But it is much less reliable than a cable plugged into a PC and much easier to attack, so use a physical connection if possible. In any event, make sure that all the equipment you are using (WIFI access points, routers), whether supplied by your ISP or bought separately, have good passwords and appropriate security settings. Don't assume that just because it worked out of the box that it's as safe as it should be.

7. USE AUDIO/VIDEOCONFERENCING WITH CARE AND FOLLOW CORPORATE ADVICE IF GIVEN

Not all consumer videoconferencing solutions meet corporate standards, and depending on whom you work for, there may be specific rules about whether, when, and how to use computers to communicate with others. Otherwise, work on the assumption that everything you say online might end up on YouTube.

8. ONLY TURN ON WEBCAMS AND MICROPHONES WHEN THEY ARE NEEDED

Consider unplugging them or covering them up when not in use. This includes equipment used by others in the household if it's close by. Consider meeting etiquette where video and audio are only active when you wish to speak; this will improve bandwidth and be less taxing on device resources. Remember, those convenient voice-operated systems like Alexa or Google Assistant may be transmitting what you say out of the house. If you have a cover for your inbuilt webcam, use it whenever you are not using your webcam.

9. KEEP YOUR PERSONAL MACHINES UP TO DATE WITH SECURITY UPDATES FROM TRUSTED SOURCES

If you receive official updates from sources you trust, take the time to apply them. Conversely, don't ever download a 'security patch' you receive unexpectedly.

10. BACKUP YOUR WORK REGULARLY

Remember that things break down. Make sure that the stuff you're working on is backed up, preferably on a corporate network if you are able to do that. Otherwise, it can be a good idea to email yourself (from your work email to your work email) important work in progress if it isn't too big. If possible, maintain separate offline backups of any information you hold particularly dear, in case you are a victim of ransomware or suffer an equipment failure.

11. REMEMBER THAT MEDIA CAN GET LOST

If you do have to keep business-confidential data in a portable format, such as a laptop, USB stick or removable drive, encrypt it where possible. Also remember to look after the physical objects even at home, as well as if you are one of those who still have to travel. Don't forget paper! Anything you print needs to be properly secured and eventually disposed of.

Advice like this can only be generic in nature & style, and is not possible to cover every single scenario that home workers may find themselves in. If you have a specific question or problem that you need help with, please contact a member of the WCIT Information Security Panel who will do their best to assist.

Designed by BluCreative Design Ltd.