The Worshipful Company of Information Technologists

ADVICE TO SMALL BUSINESSES AND CHARITIES 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 short document which we hope will help keep us all, and our places of work more secure and a touch safer. Charities communicating with volunteers to organise Covid-19 support services are peculiarly vulnerable. Others with more experience of advising them might like to bear this in mind.

1. USE SECURE COMMUNICATIONS WHERE POSSIBLE

Consider whether your staff have all the equipment they need to work effectively and securely at home. If you have the necessary infrastructure, it is much better for staff without corporate laptops or other dedicated equipment to work over secure communications channels such as VPNs to remotely access machines at work, rather than relying on using their personal machines.

2. ESTABLISH A WORK ROUTINE

You should consider Display Screen Equipment issues and put in place measures/ encouragement to limit the amount of time people 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. Consider staff who may have children at home or who are sharing desk and/or equipment and may need to establish a shift pattern.

3. CONSIDER YOUR INSURANCE SITUATION

You may well have business continuity or cyber insurance, but it's worth being certain what cover this provides, and in particular if there are any exclusions relating to home working.

4. EVALUATE RISK & BENEFIT HOLISTICALLY

It's clearly vital for many firms to find a way in which those away from their place of work can continue to produce. But the consequences of a serious data breach or loss, whether accidental or the result of criminal activity, can be an existential threat to many. Don't panic but think through the risks and benefits together.

5. CHOOSE VIDEO AND AUDIO-CONFERENCING TOOLS WISELY & PROVIDE CLEAR GUIDANCE TO YOUR STAFF

It can be very tempting to jump on the latest bandwagon and choose a tool for communication based on the latest consumer trends, but there may be more secure options, and you may well already have them, or the right to use them for free, during the current emergency. You don't want hidden eavesdroppers.

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. TALK ABOUT CONTINUITY IF HOME-WORKING STAFF FALL SICK

It's all too possible that a key home worker could fall sick quickly. Before you know it, they're incommunicado in hospital and no-one has access to their password protected material.

7. ENSURE STAFF KNOW HOW TO AUTHENTICATE MATERIAL FROM OTHER PARTS OF THE ORGANISATION

Fraudsters are using e-mails from "personnel" or "procurement" which require the recipient to click on a link and/or submit personal details (including passwords) to access information on new home-working support process. Avoid sending such communications other than from addresses already known to the recipient and ensure they have access to contacts and/or websites they can use to check that intra-company communications are genuine.

8. IF AN INCIDENT OCCURS, MAKE SURE YOUR STAFF AND CUSTOMERS KNOW WHAT TO DO TO SUPPORT IT

Whether it's a personal attack on an individual, a phishing attack to which someone falls victim, or something directly affecting your corporate network, make sure people know how to report it to the organisation, and if appropriate, to 'actionfraud' (https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime).

9. PROVIDE YOUR STAFF WITH OUR ADVICE FOR HOME WORKERS

If your corporate setup makes some of that advice inappropriate, flag it as such, and explain the reasons. We know that a single document can't fit every possible situation, but some good clear advice is better than an information vacuum. Consider setting up a 'go-to-for-help' colleague, perhaps one of the younger members of staff or who is a wizard with IT. Specialist and scarce IT support may not always be necessary or available.

10. BE CAREFUL HOW YOUR STAFF USE EMAIL SENT OUTSIDE YOUR ORGANISATION

If your staff have work email accounts, ensure that they do not use personal email for work business. Emails can get lost or misdirected. So, if your staff have to send confidential information outside your corporate email network, get your staff to password protect or encrypt it, and send the intended recipient the password by some other means, like a text message. Generally, you should balance the needs of security against the needs for staff to do their job effectively and efficiently. If IT becomes too hard to use, they won't be as productive or staff will find more insecure work arounds.

11. PLAN HOW YOUR STAFF ARE TO SHARE FILES AND COLLABORATE

Plan with care how your staff are to share large files too large to be sent via email. File sharing sites which many organisations use to send large amounts of data between staff should be selected with care. The sending of hard copy or use of portable media may not be possible now and working collaboratively on a single document may be difficult. A number of collaborative sites and applications are available, select the most appropriate for your requirements and consider the security they offer.

Advice like this can only be generic in nature & style, and is not possible to cover every single scenario that charities and small businesses 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.