IT and Data Protection

With the increase in the number of staff working from home and using new software, there are many new risks to the security of the LOROS network, and people will undoubtedly be making the most of the COVID virus to try and send phishing emails or infiltrate networks.

This guide will try to explain any risks, link you to any useful guidance or tools that can be used, and be updated regularly with any new information, warnings, or guidance.

LATEST NEWS AND ADVICE

Zoom faces privacy questions over data sharing and ability for Zoombombers to crash people's calls

LOROS does not advocate the use of Zoom and would recommend you use Microsoft Teams when video conferencing. However, for those of you that use it on a personal level, you may wish to see our recent guidance document, Data protection and Zoom

Zoom have implemented additional security measures that help to prevent 'Zoombombing', but there are still concerns around its security. The guidance document gives you further information.

Added 01/04/20:

Criminals are exploiting the corona virus online by sending phishing e mails that try and trick users into clicking on a bad link.

If clicked, these links could lead to malware infection and loss of data like passwords. The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

Like many phishing scams, these emails are preying on real-world concerns to try and trick people into doing the wrong thing. Please refer to the NCSC guidance on dealing with suspicious emails to learn more about spotting and dealing with phishing emails.

What to do if you have already clicked?
The most important thing to do is not to panic. There are number of practical steps you can take:
*Open your antivirus (AV) software if installed, and run a full scan. Follow any instructions given.
*If you've been tricked into providing your password, you should change your passwords on all your other accounts.
*If you're using a work device, contact your IT department and let them know.
*Report the incident on Sentinel
*If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

USEFUL GUIDANCE AND ADVICE:

A really good resource for everyone to use and to learn more is this online short training package for staying safe online (from the NCSC) National Cyber Security Centre:

The Stay Safe Online: Top Tips for Staff page, hosted on the NCSC website. The package is free to use, and includes a short quiz at the end, with links to further reading. No login is required - just click on the link and start learning.

The Little Leaflet of Cyber Mistakes

This document is a very short but useful guide to point to the most common mistakes people make, and how to avoid them. We would recommend sharing and/or printing for you and your staff:

https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/the-little-leaflet-of-cyber-advice.pdf