Cyber Security: Top Tips for members of Pension Board / Pensions Committee
V1 dated 06 07 2022

Employers generally supply training on cyber security for their employees.

This document has been prepared to summarise good cyber security practice for members of the Worcestershire Pension Fund' s Pension Board / Pensions Committee, some of whom will have received no training from their employer.

1. Make sure that all your devices are locked when you are not using them.
2. Make sure that you are not being overlooked when accessing a device.
3. Make sure that all your passwords are unique, not shared with anyone and are strong: this can include using three unrelated (to you) random words, mixing upper and lower cases / alpha characters with numeric characters, and using non-standard symbols.
4. Do not click through from links in emails or on websites to unknown websites.
5. Block pop-ups.
6. Do not reply to emails from unknown senders.
7. Beware of emails that use something personal to you that have a call to action, looking out for misspellings.
8. Apply updates to your software as soon as possible.
9. Instal anti-virus software.
10. Report any problems to IT.
11. Store passwords in your browser / in a password manager.
12. Make use of any 2-factor authentication.
13. Do not share your personal details.
14. Review your social media privacy settings.
15. Check for https:// in the url.
16. Check that the emails you are sending are all to addresses on the secure email domain list maintained by Worcestershire County Council.
17. Never ask a Pension Fund Officer for access to any Fund systems or data.
18. Use a VPN to privatise your connections.
19. Back up in the cloud / have a disaster recovery plan in place.
20. Only download apps from trusted places.
21. Avoid sensitive transactions on free wifi.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~ ENDS ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~