PERSONAL DATA PROTECTION OFFICE

Good practices that help keep data secure during online lessons

20 security principles that should be kept in mind by school controllers as well as teachers and students when preparing for online lessons to protect their data

1. Keep your operating systems updated.
2. Regularly update anti-virus, anti-malware and anti-spyware software.
3. Regularly scan workstations with anti-virus, anti-malware and anti-spyware software.
4. Download software only from manufacturers' websites.
5. Do not open attachments sent by email from unknown sources.
6. Do not save passwords in web applications.
7. Do not write down your passwords.
8. Do not use the same passwords in different IT systems.
9. Secure servers or other network resources.
10. Secure wireless networks - Access Point.
11. Adjust the complexity of passwords adequately to the threats.
12. Avoid accessing unknown or contingent websites.
13. Do not log in to IT systems from random places using untrusted devices or public unsecured Wi-Fi networks.
14. Perform regular backups.
15. Use proven software to encrypt emails or storage devices.
16. Encrypt data sent by email.
17. Encrypt hard drives in portable computers.
18. For remote work, use an encrypted VPN connection.
19. When leaving the computer, log out from your device.
20. Do not use random USB storage devices: they may contain malware.

Source: www.uodo.gov.pl