Member News

HOMESCHOOLING: BEST CYBERSECURITY PRACTISES

With the closure of schools, homework has become the rule for all students in the Grand Duchy of Luxembourg. Everyone must adapt to new tools and working methods. In this context, cybersecurity must not be forgotten, so that the educational experience does not turn into a nightmare.

There are mainly three points that need to be monitored:
a. Equipment (computer, tablets, etc.)
b. Applications
c. Connection

Equipment

1. Regularly update the material used for online courses.
2. Use a computer dedicated to school work. If this is impossible, set up separate accounts for family members.
3. Avoid connecting interfaces (USB keys, memory cards or other) with uncertain origin.
4. Install antivirus software and update it regularly.
5. Make sure your computer is locked and stored carefully when not in use.

Applications

1. Use only the software and platforms made available by the Ministry of Education for school work.
2. Be sure to update all software and applications installed on your computer.
3. Teachers: make sure your students use their personal access properly.
4. Students and Parents: use your personal access, making sure to change the initial password provided to you.
5. Change the default password you received to access this account. Use a strong password consisting of lowercase letters, capitals, numbers, and special characters.
6. Data transfer: use only the sharing functions of the application made available by the Ministry of Education, and do not transfer services to the public cloud.
7. Use only your school email address to exchange messages.

Connection

• Do not connect to any public, unknown or insecure network.
• Securely connect to your Wi-Fi at home (the network must be encrypted and accessible only with a password).
• Connect to 3G or 4G networks if you do not have access to a secure Wi-Fi connection.

Right Box

Be careful when checking your emails and social networks. Many misleading messages
relating to Covid-19 are circulating. These include:
• Fake news. To stay informed on news related to Covid-19, opt instead for official
government websites or recognised media;
• Phishing emails that contain links to fake websites which ask for your access codes;
• Scam messages which offer you, for example, to buy protective masks or remedies
against Coronavirus;

Finally, a piece of advice: think before you click.

Communicated by SECURITYMADEIN.LU