



In these exceptional times, it is important to be aware that cybercriminals are seizing this opportunity to multiply their attacks. That is why we must not lower our vigilance but rather double it. As the risk is present, APRIL assists you through cyber security newsletters to inform you of the best practices to implement. In this second edition, we will focus on cell phones.

### **Wifi**

- Do not allow your device to automatically access an unknown and public network.

### **Applications**

- Install only the available applications on the official app store of your device. NEVER download them from a browser.
- More than 1000 applications with malicious functions with the keyword COVID or Coronavirus have been identified.

### **Bluetooth**

- Deactivate Bluetooth when you do not need it.

### **Smishing (message phishing)**

- Do not trust messages that try to get you to reveal personal information.

### **Browser**

- Beware of scams with links offering to help in the context of COVID-19 or even to make a donation.

### **Vishing (vocal phishing)**

- Do not respond to telephone or e-mail requests for personal information, especially if it appears to come from your bank.



Sage Advisor Resources Corp., Axis Capital and April have put together a comprehensive and affordable cyber program exclusive to the association membership. If you would like to learn more or obtain a quote, contact Sage today