Dear colleague,

We need you! Did you know **one Belgian enterprise out of two is confronted with cyber criminality** today?

An employee of a Belgian SME had the following painful experience: **one mouse click on an attachment infected with a virus**. His computer was completely **encrypted;** so he could not access the data of the enterprise, even not via the backup… It all went **very fast**: loss of important data, 10.000 bitcoins ransom, clients complaining. A direct real cost of 35.000 EUR due to one single click on an infected attachment

Could this happen to you? You are careful and not easy to impress? That’s what our employee thought too…

That’s why we would like to deal with the **3 most frequent and most feared attacks**:

1. **Hacking passwords:** so the security of professional and personal accounts is compromised.
2. **Phishing:**someone’s identity is abused (often by e-mail) to get access to confidential company info or bank data.
3. **Social engineering or social hacking:** abuses the confidence of staff to get important information or to realize a money transfer in a fraudulent way.

You certainly saw these forms of internet fraud on the news. Would you like to know more about them?

Let’s think together about how to:

* **Expose attacks**
* Have the **right reflexes**
* **Alarm and react fast**

The upcoming weeks you will receive **interactive information** via e-mail with online tests, videos and scenarios of real cases of cyber-attacks. Next we **share our experiences** during a participative and cosy ‘breakfast meeting’.

We **count on your active participation for the security of all of us**.

Best regards,