Loss Prevention

Take a proactive approach to loss prevention!

Data Breach

Preventing data breaches during a pandemic

In the current situation, here are some reminders of the best prevention practices to follow in order to avoid being a victim of a data breach.

A **data breach** can be voluntary, accidental or even be caused inadvertently. Below are some tips to reduce the risks associated with privacy.

- Do not leave equipment and documents in a vehicle unattended. Even making a run very quickly gives a thief ample time to steal a device or document left in a parked car.
- The same security measures should be followed for equipment brought into the home. Logout of systems when you leave, even for a few minutes. Make sure the equipment is stored out of sight when not in use. This is not only true for laptops and tablets, but also for external hard drives and even home servers, which are often much smaller and easier to steal.
- Ensure a backup of all company data and keep at least one copy outside the premises (Cloud computing, external hard drive, etc.). Backup data at least once a day. A person should be assigned to the proper functioning of this operation. Make sure a procedure is in place to ensure the recovery of data in the event of an incident. Use data encryption to adequately protect confidential business data and information.
- Having data circulate in the digital universe, from a computer to a mobile phone for example, is inevitable. Encrypt data using a virtual private network (VPN) to prevent data from being intercepted. Avoid connections to unsecured public networks.
- Evaluate user access levels internally and remove unnecessary permissions. Confirm that the firewall and other technologies (which often allow suspicious email to be intercepted before it enters your network) have the latest security patches and are installed on all devices. Keep the

intact INSURANCE

company's operating systems and software up to date.

- The use of personal email and social media accounts can increase the risk of corporate network security breaches. Therefore, the equipment provided by the company to employees (computers, telephones, etc.) should not be used for personal use.

Fraud and breach of data

Unfortunately, fraudsters are using the current health crisis to deceive individuals in order to extort them. Beware of fraud attempts involving money transfers, requests for personal information, or downloading files.

What is social engineering?

In the context of information security, social engineering involves deception in order to induce people, by manipulating them, to disclose personal or confidential information, which can be used for the purpose of identity fraud, illegal access to a network, or stealing money. Phishing is a very common social engineering technique, but fraud can also be perpetrated via phone, text, etc.

Watch out for calls, texts and emails that include the following information:

- Sense of urgency to act, threats and consequences in case of inaction
- Unsolicited calls or emails

intact INSURANCE

Loss Prevention

Take a proactive approach to loss prevention!

Data Breach

- Multiple persons on the sender list
- If it seems too good to be true, it's probably not true
- Grammatical errors, uncommon file types, suspicious file attachments

Avoid fraud:

Educate employees and managers Ask them not to transmit information or click on questionable hyperlinks or files.

Recheck email addresses Start by examining the domain names of incoming messages.

Review suspicious or unusual requests Criminals will often send messages asking an employee to make electronic wire transfers or to provide sensitive information.

Restrict access to data You are less at risk when access to your most sensitive data (financial account numbers or employee personal information, for example) is limited to just a few people and protected by encryption protocol.

intact INSURANCE