ARBONIA

Information Security Newsletter

Dear Employees,

According to the motto ***THINK BEFORE YOU Click.Post.Type*** we want to inform you about current dangers in dealing with information technologies and make you aware of your co-responsibility in protecting against cybercriminals. Because only together can we maintain IT security and thus protect the business activities and competitiveness of the Arbonia Group from major damage.

Increasing networking, digitalisation and the Internet are leading to a rapid rise in cyber crime. The threat situation has become even more acute and also more complex. Even our direct business environment has not been spared serious cyber incidents (e.g. Meier Tobler) in recent months. However, adequate information protection cannot be achieved by technical measures alone. It also depends heavily on your behaviour and handling of data and information systems. As an Arbonia employee, you are a central link in the security chain and must actively assume this responsibility. Promoting a common information security culture in the Arbonia Group is a very important concern for us.

The most common and widespread attack tool is and remains e-mail, followed by social engineering (manipulation or influencing a person) and the Internet. For this reason, it is extremely important to recognise suspicious sources as such. Incorrect behaviour can lead to serious impairment of business activities and financial damage to the Arbonia Group. If suspicious events occur, disconnect your computer from the network immediately (unplug the network cable, switch off WLAN) and inform your IT department as soon as possible.

Below you will find some general tips for your everyday digital business and private life:

- **Be critical and do not blindly trust e-mails from seemingly known senders**, as they could be fake. Do not get tricked by personal forms of address and error-free e-mail texts!
- If in doubt, ask the sender in a separate e-mail or by telephone whether the e-mail was actually sent by that person. Never use the "Answer" button for such queries, but use the contacts from the Outlook address book.
- Never reply to suspicious e-mails.
- **Never open suspicious attachments.** If in doubt, delete them or have them checked by your IT department.
- **Do not allow yourself to be pressured into any action in the case of dubious telephone inquiries**. The attackers want to take you by surprise, arouse your curiosity or scare you, only to entice you into a rash action. You should raise such cases immediately with your superior.
- Never allow remote maintenance connections to your personal device unless you know the person who is connecting to your PC or laptop (e.g. internal IT helpdesk department).
- **Never share your personal access data with anyone.** There is no reason for this.
- Always keep in mind what personal and business data / information you disclose. Avoid business communication via social media (e.g. Facebook, Instagram).
- **Always use strong passwords and change them regularly.**
- Use your business e-mail address exclusively for business correspondence, not for private purposes such as web shops or participation in competitions.
- Do not save business data on your private device and do not copy private data to your business device.
- Do not be afraid to inform and involve your supervisor or the IT department in the event of an incident.

Thank you very much for your support!

Kind regards,

Alexander von Witzleben
CEO

Daniel Wüest
CFO

Patrick Langenegger
CIO