





Information Security Session

ANMA 2.05.2022

Innar Järva
Chief IT Officer
Estonian Academy of Music and Theatre

Daily life

- Factories have stopped production, lost goods and sales due to cryptoviruses as backups are useless
- Huge companies have lost data that cannot be repaired
- In 21-25th April Estonia suffered cyberwar
- Stealing passwords lead to impersonations
- ddos-attacks from infected computers
- Cyberwars in 2050 last 3 milliseconds
- etc



What happened in Nordplusmusic?

- About a year ago a mail password was leaked
- Impersonator learned the language and style, and by filtering and separating the emails - nobody noticed anything
- Google and Outlook passed everything as mail came from trusted site and authentic user (DKIM + DMARC)
- As there were no bank details in agreements then all asked transactions were successfully made to the group of impersonators
- Legal authorities are investigating the case (Interpol, banks, etc)

What measures can you take?

- Notify the people you've been mailing with, also the police (GDPR data), banks and IT administrators – also give a call to cancel transactions, contracts, orders
- Changing the password after crime – good or bad idea?
- Keystrokes and computer screens can be visible – change the computer



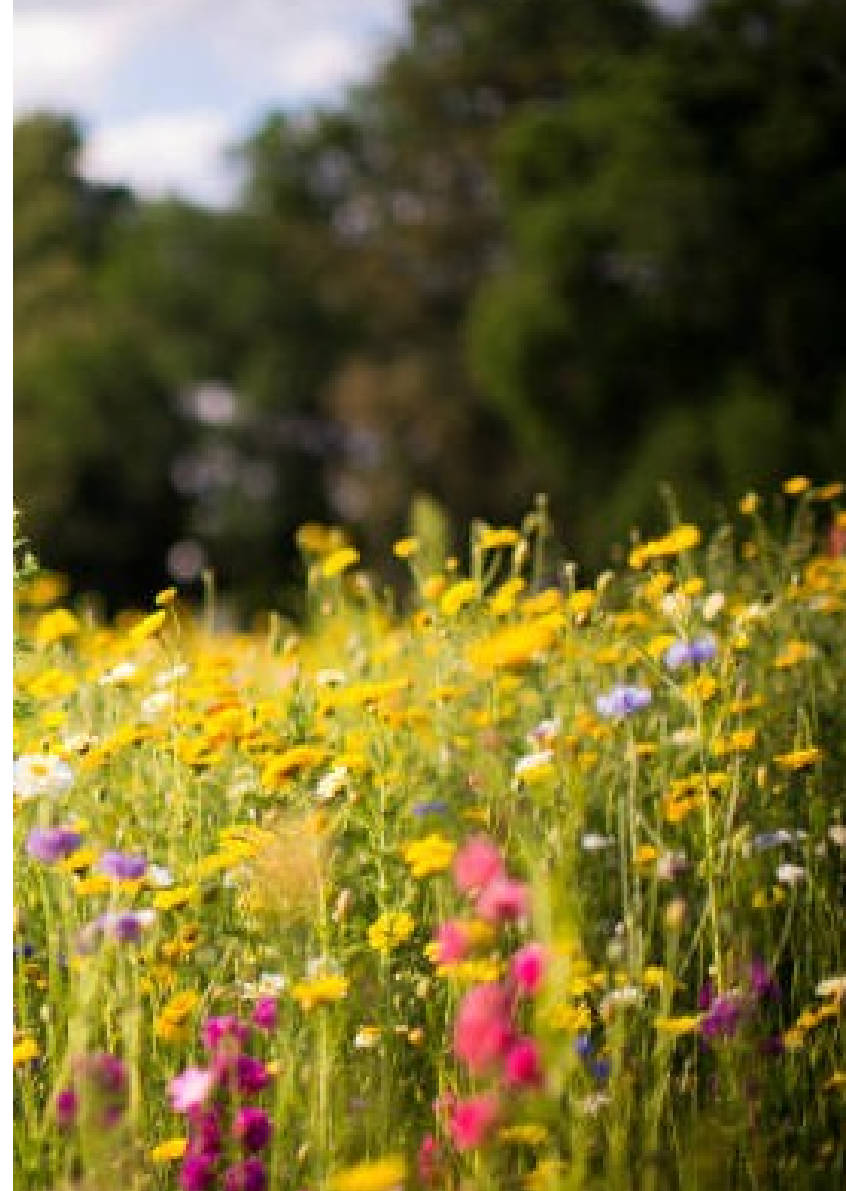
How to make your IT life secure – technical aspects

- Use 2FA authentication – also do not press „agree“ to every authentication request
- Change your password often enough, if no 2FA is used
- Check the logins to your account
- Do not use same password everywhere
- Do not log in to systems from strange computers or unknown networks – use VPN



Be sharp

- Check if mail is from authentic domain, Google vs Google
- Check the links in the mail
- Verify bank accounts
- Never give out passwords or credit card information
- Collect only the information needed (GDPR)
- If your computer acts strangely, have it checked
- If you have a doubt – make a call



Bright future

- Each worker has to understand their responsibility in creating secure environment
- Bank details on public website
- Confirmation Zoom/Teams/phonecalls
- Small contracts subsystem for double-checking

