Cyber-Attack Demo Videos

RIA (Information System Authority) needed audio-visual materials to showcase the five most common cyber-attack methods, the motivation and strategy behind each one of them along with the devastating outcome after a success of such an attack.

The purpose of these animation was to make the target audience understand, that anyone can become the target for cyber-attack. It is never personal - the perpetrator usually approaches his/her task like the way the target approaches their daily job.

Key numbers:

$600 billion Approximate cost to the global economy from cybercrime in 2017
3164 Number of significant incidents in Estonia in 2019

The solution:

To make the viewer understand the motives and direction of the attack better, we constructed the scripts as two monologues. One describing the emotions and actions of the attacker, the other the same for the victim. They describe their days/hours prior, during and after the attack revealing the gain and cost of both sides.

Because the attacks are not personal vendettas, the identities of both sides are not important. Thus we decided to only show the their hands and focus more on the transitions between the abstract and physical world.

The client verdict:

The general public needs to be constantly aware of the prevailing cyber security risks, receive risk management advice and be emphasized that the development of cybersecurity knowledge and skills are a shared responsibility of all cyberspace actors.

Therefore, explanatory animated videos were created to improve the understanding of the public sector, businesses, the press and policy makers about the threats in cyberspace so that they can (without falling victim to a cyber-attack themselves) make and justify cybersecurity decisions. The animations explain in a simple and humane way what cybercriminals are, what their motives are, and how easy it is to fall victim to cybercrime.