Cyber Security

Raising public awareness and formulation of educational base

Vladimer Svanadze
Managing Partner
Cyber Security Academy CSA
Main directions

- Research and analysis
- New legislative - normative base
- Institutional coordination of cyber security
- **Raising public awareness and formulation of educational base**
- International cooperation
- Cyber Security Laboratory

Georgian Cyber Security Strategy
2013 – 2015 & 2017 – 2018
Formulation of Educational Base

• Integration in Education Modules
  - University of Georgia UG
  - Caucasus University CU
  - Business and Technology University BTU

• Implementation in Private/Public School
  - Private School “IB Mtiebi” - First time in Georgia, was implemented project "Introduction in Cybersecurity" as a subject for schools
  - Pilot Project by Georgian National Communication Commission only for Public Schools
Raising Public Awareness

- Cyber Hygiene
- Cyber Bullying
- Protect Children Online
- Personal Data Protection
- Introduction in Cybersecurity
- Online Newsletter CyberStellar

- LEPL Data Exchange Agency DEA of the Ministry of Justice
- Georgia's Innovation and Technology Agency GITA
- Georgian National Communication Commission
- Internet Development Initiative IDI
- Media Development Foundation MDF
- Georgian Research and Educational Networking Association GRENA
- Cyber Security Academy CSA of Georgia
Cyber Hygiene

• Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security.

• These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.

• Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.

• Having a routine cyber hygiene procedure in place for your computers and software is beneficial for two distinct reasons – maintenance and security.

• All hardware (computers, phones, connected devices), software programs, and online applications used should be included in a regular, ongoing maintenance program. Each of these systems have specific vulnerabilities that can lead to different problems.
Cyber Hygiene

**Cyber Hygiene Policy**

- **Password Changes**  Complex passwords changed regularly can prevent many malicious activities and protect cyber security.

- **Software Updates**  Updating the software you use, or perhaps getting better versions should be a part of your regular hygienic review.

- **Hardware Updates**  Older computers and smartphones may need to be updated to maintain performance and prevent issues.

- **Manage New Installs**  Every new install should be done properly and documented to keep an updated inventory of all hardware and software.

- **Limit Users**  Only those who need admin-level access to programs should have access. Other users should have limited capabilities.

- **Back Up Data**  All data should be backed up to a secondary source (i.e. hard drive, cloud storage). This will ensure its safety in the event of a breach or malfunction.

- **Employ a Cyber Security Framework**  Businesses may want to review and implement a more advanced system (e.g. the NIST framework) to ensure security.
Thank you