Cyber 2.0

## Cyber 2.0 – Total Defense Against the Spread of Cyber Attacks

**Cyber 2.0 is the only system in the world that provides total defense against the spread of cyber attacks within organizational networks. (Viruses, ransomware, trojan, information leakage, browser hijacking, and every new attack)**

**The first computer may be penetrated, but Cyber 2.0 will isolate the attack and block its spreading.**
**The infected computer will also be blocked from sending information outside the organization, even if it was infected before the installation of Cyber 2.0**

We are aware of the immediate responses: "there is no 100%", and "it's too good to be true".

Therefore, we decided to We announced The biggest hackers challenge: We invited all hackers to hack our system, for a reward of NIS 100,000. We didn't ask them to find our weakness or a loophole. We simply said "No one is going to hack. Do you want to try? Go ahead".
All of them failed.

Next step: January 10, 2019 in Atlanta, for a reward of 100,000$.
And we will continue to do it over the world, and to increase the reward each time.

We have 70 clients in process of implementation, who said at the start "It's too good to be true" and are now very satisfied with our technology.

All attacks (of hacking companies and hackers) against Cyber 2.0 failed.

Cyber 2.0 Registered 9 Patents (the most important were already approved in the USA).

We are supported by the Israel Innovation Authority (3 consecutive years)

We believe that Cyber 2.0 will make most other cybersecurity systems irrelevant.

### Our unique solution:

The cyber world (defensive and offensive) is based on biological models, making them vulnerable to penetration by systems using similar models (virus vs. anti-virus). Cyber 2.0 system is based on **mathematical chaos model**, that cannot be breached.

The classic process is "Detection>Prevention": first you have to detect and to recognize every new malicious, then try to prevent (or to alert).

It is known that there is no 100% detection! (because of new malicious every second). It is also known that there is no 100% prevention! (because once the system is penetrated, the organization is no longer protected

Cyber 2.0 does not fail the Detection Test, because it skips over it, effectively blocking every malware without first identifying it.

Cyber 2.0 does not fail the Prevention Test, because by using the **chaos** model, it blocks 100% of what is required to be blocked, since it is designed in a way that even if it is bypassed or deactivated, it still protects the organization.

Unlike other systems: We don't study the organization's routine, we don't use attack database, we don't look for anomalies, we don't legitimize previous malicious programs, we don't rely on the infected computer, we don't have false positives or delayed response to real threats. We simply block all malicious software.

All the ordinary methods of attacking cyber companies, including bypassing, deactivating, adding malicious software to the legitimate software list- will fail.

## The team

The team is made up of professionals with management and technological skills:

**Hertzel Ozer**, Founder & CEO:
Highly experienced leader in the telecommunications, retail, manufacturing, food and consumer goods industries:
CEO & Chairman of the Board of 8 leading companies, last one is HOT Telecommunication Systems Group/

**Erez Kaplan Haelion** – Founder & CTO:
Highly experienced in leading large-scale computer projects:
worked as a senior advisor of Microsoft.
An inventor with many breakthrough solutions

Link to company's presentation:

cyber20.com/Resources/Cyber20pre.ppsx