

---

# Cyber Security on wired internet connections

---

Organising an event usually involves the use of a network. It is crucial to be absolutely sure that network is secure to avoid placing yourself, your visitors and exhibitors at risk or registration and other applications being interrupted. Cyber Security should be a major point of attention during every event. Malware, phishing and DDoS attacks can shut a company down completely. What can you do to protect your event against cyber risks and how can RAI Amsterdam assist you?

## Malware, Phishing and DDoS

**Malware** is software that infects a computer after visiting a website and then gains access to personal or company data. Via that one computer it can even take control of your entire (company) network.

**Phishing** occurs on websites that pretend to be familiar, reliable websites but which are actually designed to intercept and then abuse login details.

**DDoS attacks** are attempts to make a website or service unusable by overwhelming them with requests.

RAI Amsterdam works with the best Cyber Security software available, which has a database of all website addresses worldwide that is continuously updated and earmarks websites that form a risk. The internet connection we set up checks every attempt to visit a website against this database. If a website is known to contain malware, for example, a visit to the site is blocked so the computer cannot be infected.

Security Settings	Basic	Premium	Ultimate
<b>Malware</b> Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.	✓	✓	✓
<b>Command and Control Callbacks</b> Prevent compromised devices from communicating with attackers' infrastructure.	✓	✓	✓
<b>Phishing</b> Fraudulent websites that aim to trick users into handing over personal or financial information.	✓	✓	✓
<b>Potential Harmful Domains</b> Domains that exhibit suspicious behavior and may be part of an attack.		✓	✓
<b>DNS Tunneling VPN</b> VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.		✓	✓
<b>Newly Seen Domains</b> Domains that have become active very recently. They are often used in new attacks.		✓	✓
<b>Dynamic DNS</b> Block sites that are hosting dynamic DNS content.			✓
<b>Crypto Mining</b> Crypto Mining allows organizations to control crypto miner access to mining pools and web miners.			✓

# Levels of Security

On our internet connections, we offer three levels of security. Depending on your requirements, we can offer a suitable set of security measures. In the scheme, you can find what is included in the different levels.

# Making life easy

We provide a complete package of full-service IT products and customized services. Like to know more about our other IT services? See [www.raai.nl/itservices](http://www.raai.nl/itservices) or ask your account manager for more information +31 549 1212

## Content Policy

Access to these sites will be restricted based on the type of content served by the pages of the site

	Basic	Premium	Ultimate
Blocks all adult-related websites	✓	✓	✓
Blocks Illegal activity social networking sites		✓	✓
Blocks video sharing sites			✓

## Application Policy

Select applications or application categories to be blocked or allowed for the users in your network

Create a custom set of applications			✓
-------------------------------------	--	--	---

## Destination List

List of sites to block or allow

Block or Allow URL/sites.			✓
---------------------------	--	--	---

## Custom no rights page

Define the appearance and bypass options for the no rights pages

Custom no rights page and bypass options		✓	✓
--	--	---	---