Just like most of technological developments and innovations, Artificial Intelligence (AI) is also a double-edged sword. On one end, it has helped in more robust network security, whereas on other end, it can prove to be a powerful tool for cyber criminals.

As companies delve deeper into the digital era, it is imperative to protect against the ever-emerging cyber threats. Artificial Intelligence is one technology that can thwart the increasing number of attacks organizations face every day. It not only saves your time and resources, but also helps increase the accuracy and speed of defense.

Let’s see in detail how Artificial Intelligence can help stop hackers from successfully attacking your organization’s network.

**How AI Fits into the World of Cyber Threats?**

It was a rather painful task in the past to monitor all cyber threats manually. Even with more time, effort, and resources spent on detecting and monitoring the threats, the results were still not very desirable. However, with the introduction of AI, the process has transformed entirely. AI has optimized the capability to detect, monitor, and fight potential threats. With automated defense, organizations can now easily counter incoming threats before they become real attacks.

As cyber criminals use AI to deploy complex strategies, the same can be used by organizations to recognize threats and identify vulnerabilities. It can be used for scraping devices, applications, and networks to assess vulnerabilities and improve defense against emerging threats.

**How Can AI Help in Stopping Hackers?**

Once leveraged with high level capabilities like computer vision and machine learning, hackers can find it challenging to conduct successful cyber-attacks. Here’s how AI can help.

**Detects Anomalies**

As deep learning does not require going through a rigorous manual process, it can quickly detect and track anomalous patterns in data. These anomalous patterns may include suspicious email send frequency or insider threats detected from [footprint devices](http://www.cardzgroup.com/ContactSmartCard.html).

**Helps Fight Phishing and Spamming**

With deep learning powered by AI, it is now possible to identify phishing and spam emails with hidden or repetitive content, or containing messages with newly created links. This can also help in areas with higher chances of human error or negligent behavior on part of employees.

**Identifies Advanced Malware**

AI has allowed companies to improve malware protection by improving the accuracy and quantity of the data under analysis. Though malware is an ever-growing threat to security, AI provides larger defense to companies by growing along with the newly emerging threats. As each malware passes through the AI model, it enhances its capability to identify advanced malware.

**Protects DNS Data**

When we talk about cyber defense such as firewalls, hackers are used to accessing critical business or customer information by using Domain Name System (DNS) data. DNS data is mostly able to pass through firewalls as it works on slightly different rules. This also makes it more vulnerable to hackers.

With machine learning AI, companies are protected from hacking attempts by making analysis of billions of DNS queries and understanding where the bad actors are hiding.

**Safeguards Authenticity**

Many websites today ask users to create an account to login. This feature is mostly used to collect visitor information and provide customized features. When AI is added as an extra protection layer, users feel safer in sharing and authenticating their account. AI features such as fingerprint or facial recognition are popular subfields of AI in this regard.

**Advantages of AI in Cybersecurity**

Now that we know the ways in which AI can prevent or stop hackers from carrying out successful attacks, let’s have a look at some advantages AI can bring to your organization.

**Eliminates the Need of Manual Monitoring**

Cybercriminals are relentless in their attacks. Hiring someone to monitor potential attacks can be a monotonous process which can lead to fatigue, and eventually result in human error. AI can handle repetitive data with great accuracy while learning from every new piece of data and making future decisions accordingly.

**Easily Processes Huge Amount of Data**

With more organizations moving to the cloud, it is now more important to safeguard innumerable amount of data being exchanged. The best solution lies in AI, as it allows organizations to safely transfer huge sets of data without worrying about malicious actors hiding in the way.

**Provides Automatic Alerts to Latest Threats**

AI also enhances cybersecurity by instantly identifying and reporting threats. It triggers real-time alerts when suspicious behavior is detected. Furthermore, predictive AI models find threats even before they happen.

**Conclusion: Fighting Technology with Technology**

When implementing a strategy for cybersecurity, Artificial Intelligence is a powerful technology that allows organizations to stay atop growing threats. From identifying an attack before it happens, getting real-time alerts, and eliminating human error – it is possible to develop an improved security posture. The result is improved business efficiency, lower cost and more secure data.