Barracuda

PARTNER LOGO

# Never Give in to Ransomware!

In recent years we have seen more computer systems are being seized and attackers are demanding payment in return for unlocking the assets.

**RANSOMWARE** attacks are surging, and losses are skyrocketing, panic and fear ensues – it is no difference from terrorism!

One thing is for sure: ransomware gangs can never be trusted. There were cases in which victims did not regain access to their critical data after paying the ransom or had to pay again to keep the stolen data secret. Some ruthless hackers even broke their word and sold the data after getting paid! There is no reason to reward criminals for their crimes – it does not mean that you are putting an end to the nightmare, but it will continue to perpetuate this offensive activity.

## How can organizations bolster their defense against ransomware attacks?

**There are three critical steps we should take.**

1. Combating PHISHING to block the primary attack vector of ransomware.
2. Securing WEB APPLICATIONS to remediate cybersecurity vulnerabilities.
3. Optimizing DATA BACKUP to put a contingency plan in place for potential outages.

**Never bow down to evils. Fight against them!** Take a proactive step to safeguard your critical data assets in the increasingly perilous cyber world.

Read more about how Barracuda Networks gives you effective solutions against catastrophic ransomware attacks.

Let's begin with a free trial of the Barracuda Email Threat Scanner for a system health check and contact us today for a free consultation.

Contact Us

Forward this to a colleague

f 🐦 G+ ▶ in

Privacy Policy I Unsubscribe