



## Phishing – the Driving Force of Ransomware attacks

In the cat-and-mouse battle for cybersecurity, hackers make every effort to break the last line of defense and launch an effective attack. While traditional ransomware exploited known vulnerabilities to hack into organizations, hackers are also using PHISHING as a vector for more sophisticated ransomware attacks. To overcome these new tactics, organizations should strengthen malware and phishing email detection and user security awareness training.

### Some useful tips on the technology side:

- Email protection should focus not only on tracking malicious links and attachments, but also on the use of machine learning to detect hackers' social engineering tactics.
- Enhancing account takeover protection to identify and alert about malicious activities such as suspicious logins or attacks from compromised accounts.
- Phishing is no longer associated with email only, but also through other channels such as SMS and voicemail.

### How can Barracuda help?

Barracuda Total Email Protection provides comprehensive protection against all [13 EMAIL THREAT TYPES](#), from spam to socially engineered threats such as spear phishing, business email compromise, and account takeover. It combines email gateway defenses with artificial intelligence and security awareness training which help your employees understand the latest phishing techniques and recognize subtle phishing clues, transforming them from a potential security risk to a powerful line of defense against damaging phishing attacks.

Are you ready? Let's begin with a free trial of the [Barracuda Email Threat Scanner](#) to identify phishing attacks missed by your current email protection or [contact us](#) for a free consultation.

[Contact Us](#)

[Forward this to a colleague](#)

