timus

What's a ransomware attack and how do I protect my organization?

A ransomware attack is a malicious cyber assault in which cybercriminals infiltrate a victim's computer or network and encrypt essential files and data, rendering them inaccessible. Perpetrators then demand a ransom, typically in cryptocurrency, in exchange for the decryption key necessary to regain access to the compromised data. This coercive tactic exploits victims' desperation, often threatening permanent data loss or exposure of sensitive information if the ransom isn't paid. Ransomware attacks can cripple businesses, disrupt critical infrastructure, and compromise personal privacy. This highlights the urgency of cybersecurity measures and backup protocols to prevent and mitigate the devastating consequences of digital extortion. Here are some eye-opening facts and what you can do to protect your organization from ransomware and other cyber attacks.

$10 Trillion

Cyberattacks are expected to cost more than $10 Trillion in damages by 2025.

McKinsey estimates damages from cyberattacks will amount to more than $10 trillion annually by 2025 — a 300% increase from 2015.

Source: McKinsey & Company
https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

300% increase in cyberattack damages from 2015 to 2025

Cyberthreats in Focus: Phishing, Ransomware, and BEC Trends

Phishing Vulnerability:

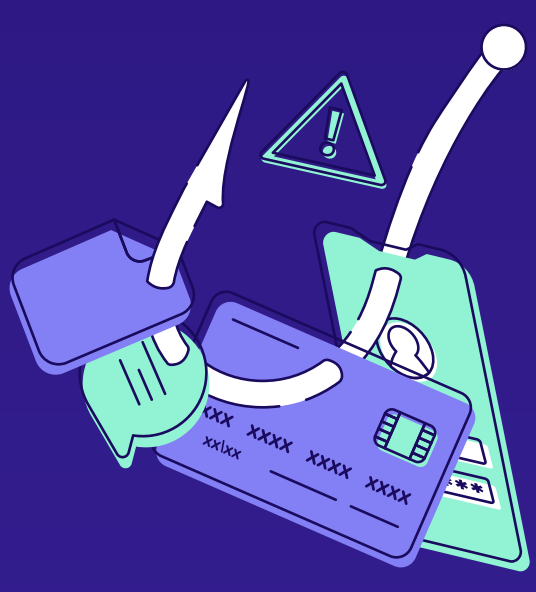
The median time for users to fall for phishing emails is **less than 60 seconds.**

Ransomware Financial Impact:

The median financial loss from ransomware and extortion breaches is **$46,000**, with cases ranging from **$3 to $1,141,467.**

Business Email Compromise (BEC):

BEC incidents accounted for **24%-25% of financially motivated attacks** over the past two years.



Source: Verizon
https://www.verizon.com/business/resources/Td54/reports/2024-dbir-data-breach-investigations-report

68% of breaches include a human element

68% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of Stolen Credentials, or Social Engineering.

23% of breaches are ransomware

Ransomware is the most common approach taken by attackers — 23% of all attacks include ransomware.

Source: Verizon
https://www.verizon.com/business/resources/Td54/reports/2024-dbir-data-breach-investigations-report

How can I protect myself against ransomware attacks?

Here are the two most important steps you can take to protect your organization.

1.Replace your VPN with a Zero Trust solution:

VPNs are subject to credential theft because they tend to give broad access to your network in one swift move. Adopt a Zero Trust Network Access solution like Timus Networks to access data and apps remotely.

2.Replace your hardware-based firewall with an Adaptive Cloud Firewall:

Hardware firewalls were built for a time when data lived inside the walls of the office. Today, apps, data, and people are everywhere. Adaptive cloud firewall solutions like Timus Network's protect company networks and data, no matter where the data lives.

Timus is the network security solution for the cloud era.

Timus Networks helps companies orchestrate secure access while protecting the network against cyberattacks. Timus combines secure, zero-trust network access with an intelligent cloud firewall that adapts in real time.

Get started in less than 30 minutes
timusnetworks.com