

INSIDE

New findings this month

Multi - Factor Authentication

Key Aspects – what to expect

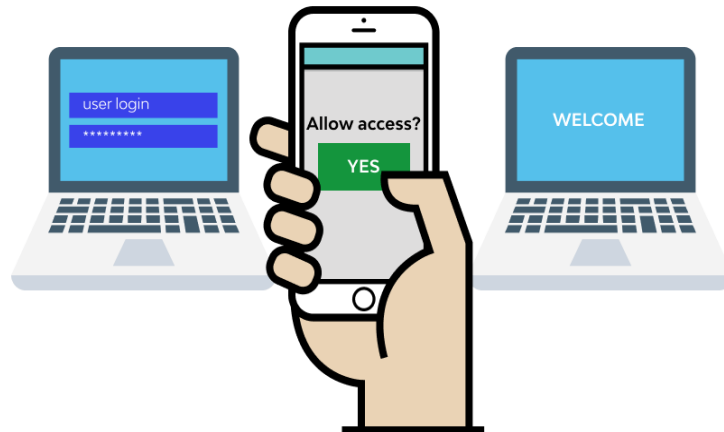
Our contact details

Tel: +357 24 023203

Email: info@geevo.eu

Visit us: www.geevo.eu

Multi-Factor Authentication (MFA)



NEW FINDINGS THIS MONTH

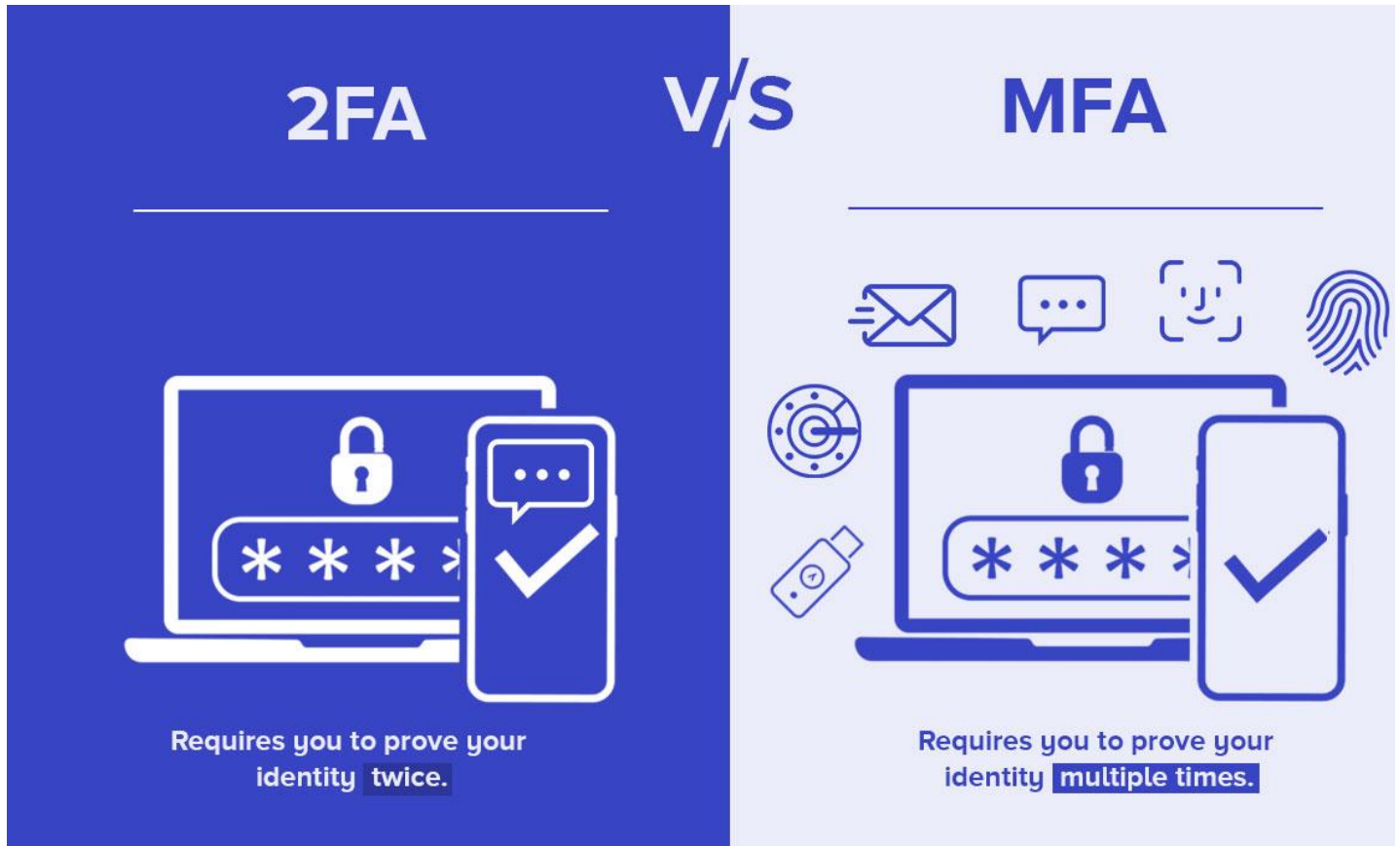
By Vikentios Vikentiou, Managed Security Services Manager

Multi-Factor Authentication (MFA): A Must Have for Cyber Protection of Individuals and Companies

Multi-factor Authentication (MFA) is a security mechanism that confirms a user's identity for a login or other transaction by requiring multiple ways of authentication from separate categories of credentials. Multi-factor authentication combines two or more separate forms of identification: what the user is (through biometric verification methods) and what they have (such as a security token or password). MFA aims to make it more difficult for an unauthorized person to access a target, such as a physical place, computing device, network, or database. The attacker must still overcome at least one or more barriers even if one is compromised or broken in order to get access to the target.

Speak to our Cybersecurity experts!

Differences between 2FA and MFA



What you will expect

- **Stronger Security:** Protecting sensitive information.
- **Simple Login Mechanism:** Assurance of dependable and continuous access to private information.
- **Reduce Operating Costs:** Fraud is less likely to occur as a result of MFA, which also frees up workers to work on more complicated customer care issues and minimizes help desk activity.
- **Regulatory Compliance:** To prevent unauthorized users from accessing payment processing systems, the Payment Card Industry Data Security Standard (PCI-DSS) mandates that MFA be deployed in certain circumstances.

THINK WE CAN DO THIS TOGETHER? GET IN TOUCH!