Phishing is a type of [social engineering attack](https://www.imperva.com/learn/application-security/social-engineering-attack/) often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a [malicious](https://www.imperva.com/learn/application-security/malware-detection-and-removal/) link, which can lead to the installation of malware, the freezing of the system as part of a [ransomware attack](https://www.imperva.com/learn/application-security/ransomware/) or the revealing of [sensitive information](https://www.imperva.com/learn/data-security/sensitive-data/).

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an [advanced persistent threat](https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/) (APT) event. In this latter scenario, employees are [compromised](https://www.imperva.com/learn/application-security/cyber-security/) in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Phishing techniques:

* Email phishing scams
* Spear phishing:

[Spear phishing](https://www.imperva.com/learn/application-security/spear-phishing/) targets a specific person or enterprise, as opposed to random application users. It’s a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

Prevention of phishing:

2FA( 2 factor authentication)