

Impersonation Attack Prevention

Attackers seek opportunities to impersonate employees and trusted third parties in order to gain a foothold inside your organization's infrastructure and steal data and assets.

Picnic offers a multi-layered approach to proactively prevent impersonation attacks against your employees and your company.

Select Capabilities & Services

- Corporate and personal social engineering risk scoring
- High-value and high-risk employee identification
- Ongoing monitoring of digital footprints
- Red Team reconnaissance
- LinkedIn profile impersonation
- identification and takedown service



CISO

Safeguard digital identity assets, respect customer privacy, counter social engineering risks, and ensure business continuity.



CFO

Invest in tools that proactively mitigate the risk of fraudulent transactions, preventing them from occurring and resulting in measurable savings.



Identity & Access Management Professionals

An intelligence-based approach to identity protection allows you to thwart adversaries before they can cause harm and provides the ability to prevent account takeover.



Third-Party Risk Professionals

Get the tools to make informed risk management decisions quickly regarding the companies within your organization's supply chain.



[Schedule a demo](#)