

# Social Engineering

## Compromised Users

In this section, you'll find vital information regarding users who have recently fallen victim to phishing simulations, offering valuable insights into potential vulnerabilities within your organization's cyber security defenses. Here's what you need to know:

- **Top Compromised Users:** The section presents a concise list of the top three users who have recently failed phishing simulations, highlighting individuals who may be particularly susceptible to social engineering attacks.
- **Recent Activity:** By focusing on recent incidents, you can stay informed about the latest trends and patterns in social engineering attempts, allowing you to take proactive measures to mitigate risks and enhance user awareness and training.
- **Targeted Intervention:** Identifying compromised users enables you to provide targeted support and additional training to enhance their resilience against social engineering tactics, reducing the likelihood of future breaches and strengthening your organization's overall security posture.
- **Risk Mitigation:** By addressing vulnerabilities at the individual user level, you can mitigate the risk of successful social engineering attacks, safeguarding sensitive data and protecting your organization from potential security breaches.



This section serves as a valuable tool for risk assessment and mitigation, empowering you to address weaknesses in user awareness and behavior and fortify your organization's defenses against social engineering threats. Explore this section to stay vigilant and proactive in safeguarding your organization's assets and data against evolving cybersecurity risks.