## Executive Assistant (New-starter)

**Industry:** Technology  
**Most Likely Targeted By:** CEO Fraud  
**Data They Access:**  
- Login credentials for C-Suite execs  
- Credit card information  
- Travel itineraries  
- PII of employees  
- Customer/client data  
- Intellectual property

**Why Are They Frequently Targeted?** In companies with over 1,000 employees, employees working in Technology are the most likely to fall for scams and hackers often prey on new-starters who aren’t yet familiar with policies or people. They also probably haven’t had security training yet. This means they’re less likely to be able to distinguish between a normal and suspicious email request.

## Office Administrator

**Industry:** Healthcare  
**Most Likely Targeted By:** Email Spoofing  
**Data They Access:**  
- Health records  
- Clinical trials  
- Insurance information  
- Credit card details  
- PII of patients  
- PII of employees  
- Payroll information

**Why Are They Frequently Targeted?** The healthcare industry is in the top three most vulnerable across all company sizes. They also continue to suffer from the costliest breaches. Why? Employees in healthcare process and hold tons of sensitive data, and many public organisations lack the funding for strong security controls or frequent staff training.

## Accounts Payable Manager

**Industry:** Manufacturing  
**Most Likely Targeted By:** Business Email Compromise (BEC)  
**Data They Access:**  
- Payroll information  
- PII of employees  
- Client list  
- Third-party data  
- Intellectual property

**Why Are They Frequently Targeted?** Hackers are financially motivated. And, because organisations in Manufacturing tend to be involved in long supply chains, they’re a prime target for attacks. Last year, Manufacturing saw the most breaches from social attacks, like BEC, and spear phishing of any industry, and between Q1 2020 and Q2 2020, incidents involving payment and invoice fraud increased by 102%.

## Senior Partner

**Industry:** Legal  
**Most Likely Targeted By:** Whaling Attacks  
**Data They Access:**  
- PII of clients  
- Credit card information  
- Health records  
- Client lists  
- Intellectual property  
- Insurance information

**Why Are They Frequently Targeted?** High-ranking employees are high-risk when it comes to social engineering. They have access to a lot of sensitive data, tend to work across several projects, and are generally time-poor, distracted, and stressed, which makes them more likely to make mistakes. While the Legal sector isn’t in the top three most targeted industries, nearly 80% of firms say they’ve been targeted by a phishing attack.

---

Learn more about the most likely targets of spear phishing attacks and how to protect yourself on email with Tessian.

Tessian’s mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees’ workflows. Our expert employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel and Balderton and has offices in San Francisco and London.