

# Most Likely Targets of Spear Phishing Attacks 2020



TITLE

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 the security training yet. This means they're less likely to be able to distinguish between a normal and suspicious email request.

TITLE

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.

TITLE

Accounts Payable Manager

INDUSTRY

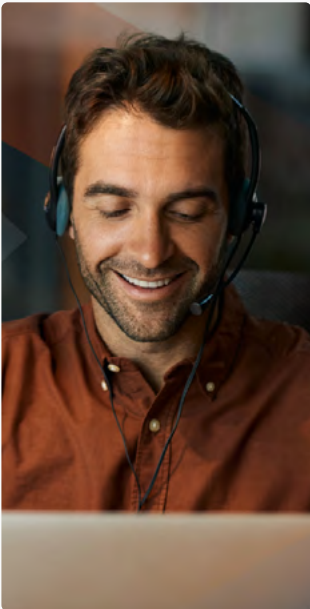
Manufacturing

MOST LIKELY TARGETED BY

Business Email Compromise (BEC)

DATA THEY ACCESS

Payroll information  
PII of employees & third-parties  
Credit card information  
Invoices  
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 112%.

TITLE

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.