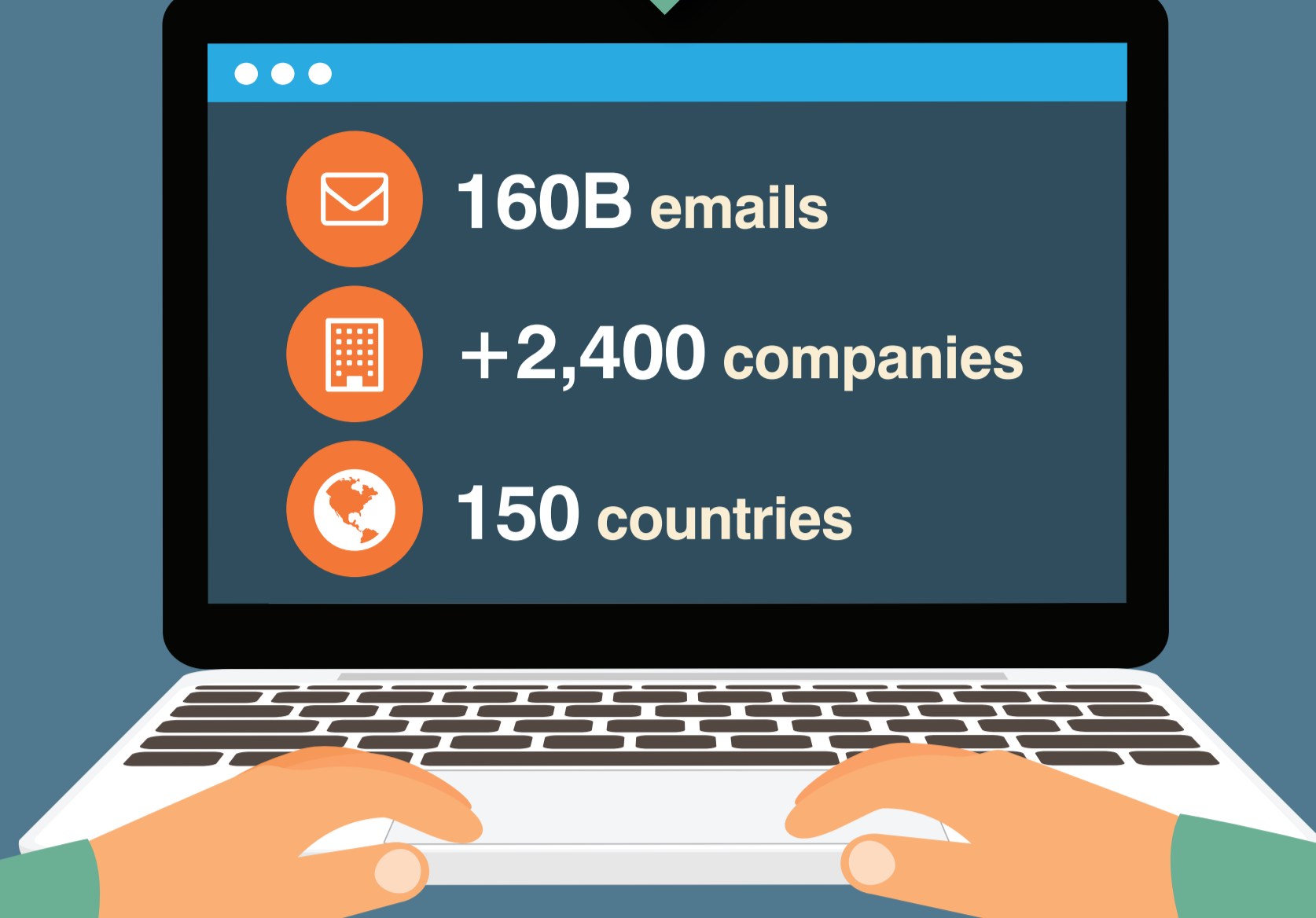


# THE STATE OF EMAIL FRAUD YEAR IN REVIEW

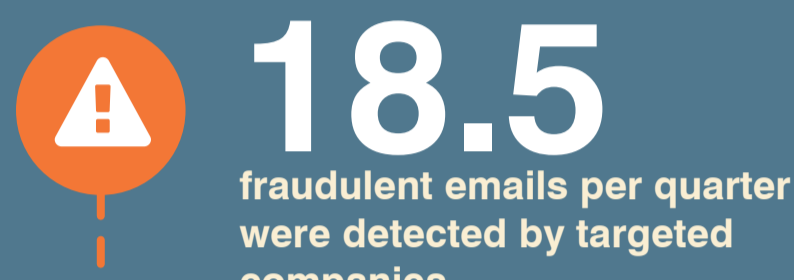
Email fraud is one of today's greatest cyber threats. To better understand the scope of the problem and the tactics used, Proofpoint analyzed more than...



Here is a snapshot of our findings for 2017.

## EMAIL FRAUD IS ON THE RISE

Attackers targeted more organizations and more frequently vs. the previous year.



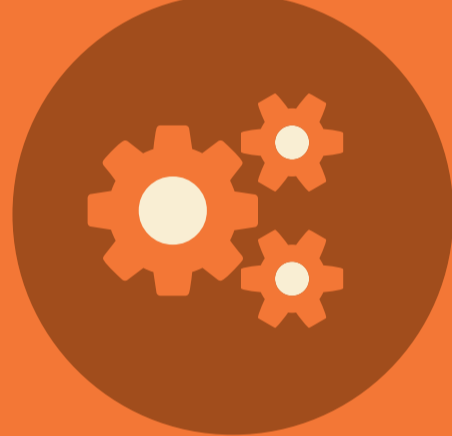
An average of 13 people per organization were targeted in Q4

## WHO GETS TARGETED?

Email fraud doesn't discriminate—it targets companies of all sizes across all industries. Here are some of the biggest industries targeted by email fraud (by average attacks per company in 2017):



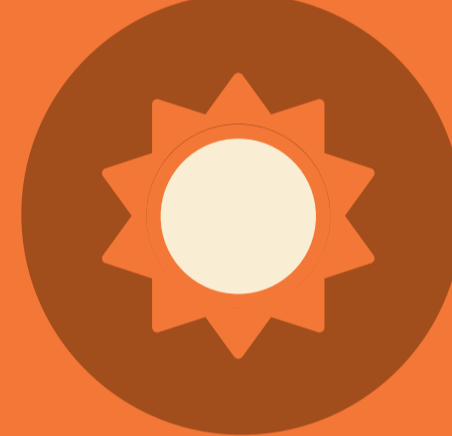
Financial Services  
**93**



Manufacturing  
**159**



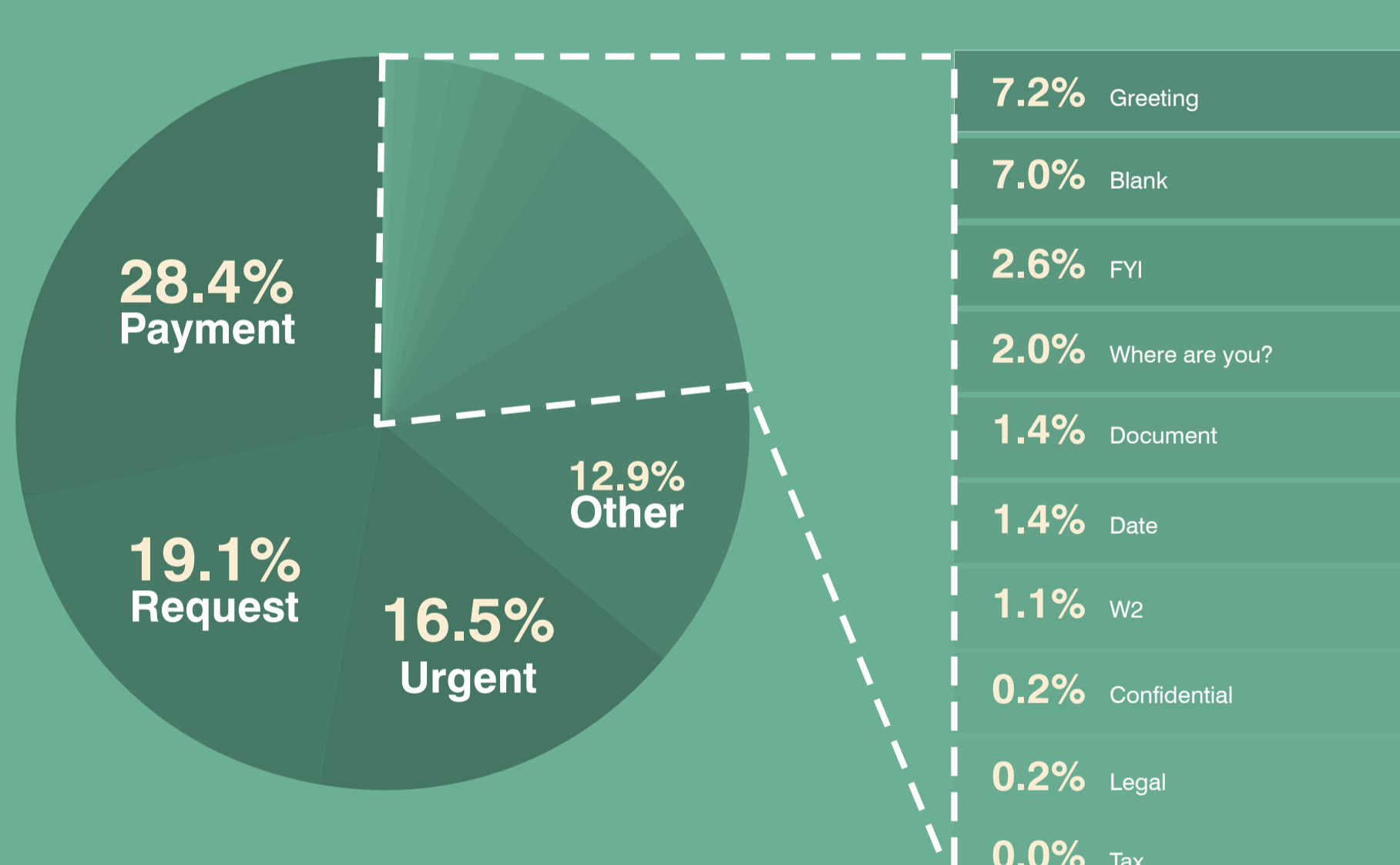
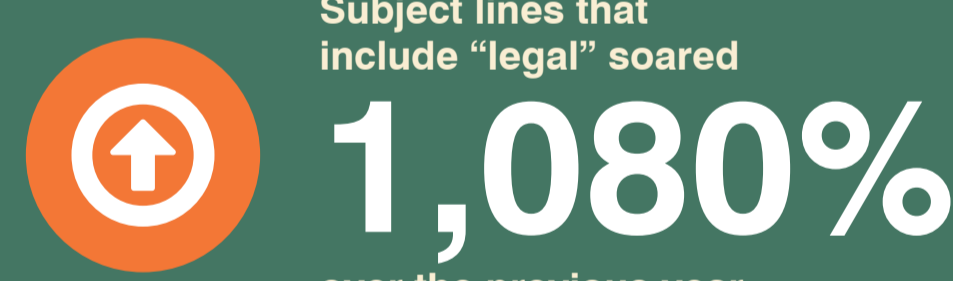
Healthcare  
**79**



Energy/Utilities  
**120**

## TOP EMAIL FRAUD SUBJECT LINES

Email fraud attacks use all kinds of headers to get recipients to click.



## TOP EMAIL FRAUD TECHNIQUES



### Fake Email Histories

The percentage of total email fraud threats that contain fake email histories grew to **11% of all email attacks in Q4, vs. just 7.31% the previous year.**

### Domain Spoofing

In 2017, **93% of organizations experienced at least one domain spoofing attack**, where a fraudster hijacks an organization's trusted domain to defraud someone.



### Lookalike Domain Spoofing

Attackers register domains that are confusingly similar to those of trusted brands. **Swapping letters is the top technique at 38% of all lookalike domain spoofing.**

Read the full report here

[proofpoint.com/us/resources/analyst-reports/email-fraud-report-2017-review](http://proofpoint.com/us/resources/analyst-reports/email-fraud-report-2017-review)