

# WHO'S AT RISK?

## Executives, Sales and the Board

### How separate roles influence exposure to phishing attacks

Executives, the Board, and sales face the highest rates of attempted phishing. Don't be surprised — these groups have access, influence and a public persona. Good news: they also tend to have lower click rates compared to other employees.

### Phishing events among highly targeted roles (per user per year)

**80+** Phishing attacks faced by executives

**60** Phishing attacks experienced by board members

**75** Phishing attacks received by sales

### The actions security pros can take

Cybersecurity starts and ends with people. To keep click rates in this highly targeted group low, take these steps:

#### STEP 1

**Leverage risk-specific training and intervention:**  
Use advanced behavioral analytics to deliver targeted training to employees in roles more susceptible to phishing attacks.

#### STEP 2

**Enhance risk visibility:**  
Ensure that user-based risk analysis accounts for more than just phishing simulation exercises.

#### STEP 3

**Develop role-based protections:**  
Ensure that user-based risk analysis accounts for more than just phishing simulation exercises.

#### STEP 4

**Adopt a holistic Human Risk Management framework:**  
Integrate security technologies with a humancentric strategy that fosters continuous engagement and accountability.

Dive deeper into this topic by reading the full **Exposing Human Risk** report.