**Must-Know Phishing Statistics**

How many phishing attacks was your company targeted by?

- 9% No Attacks
- 10% 1-10 Attacks
- 37% 11-50 Attacks
- 28% 50-100 Attacks
- 12% Over 100 Attacks
- 4% Unknown

Attacks faced by companies in 2019.

Top 5 subject line keywords for business email compromise:

- Fw: Urgent Invoice
- Important: Please Read
- RE: Finance Request for CEO of Acme
- Attention: Credentials needed for login to secure mainframe
- Urgent Do Not Ignore!

96% of phishing attacks arrive by email.

When asked about the impact of successful phishing attacks, security leaders around the world cited the following consequences:

- 60% of organizations lost data.
- 52% of organizations had credentials or accounts compromised.
- 47% of organizations were infected with ransomware.
- 29% of organizations were infected with malware.
- 28% of organizations experienced financial losses.

The most impersonated brands overall in Q1 2021 were:

- Microsoft
- Amazon
- Rakuten
- LinkedIn
- Google
- PayPal
- Chase

$150 is the average cost per compromised record.

$3.92m is the average cost of a data breach.

But, what about prevention?

While you can’t stop hackers from sending phishing or spear phishing emails, you can make sure you and your employees are protected when one is received. Learn how Tessian Defender uses machine learning to detect and prevent spear phishing attacks before data or credentials are stolen.

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. As a result, 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.