SAFEGUARD CYBER

Disrupting Social Engineering Attacks

In light of recent breaches, it's clear that sophisticated social engineering attacks remain a major threat. Move beyond just security awareness training and **establish controls with Social Engineering detection technology**. Start with a communications risk assessment securing your business communications environment.

Here's how to start today:

1. Inventory your business communications channels

Understand what every line of business is using to collaborate and communicate internally and externally.

Enterprise Apps

Personal Apps
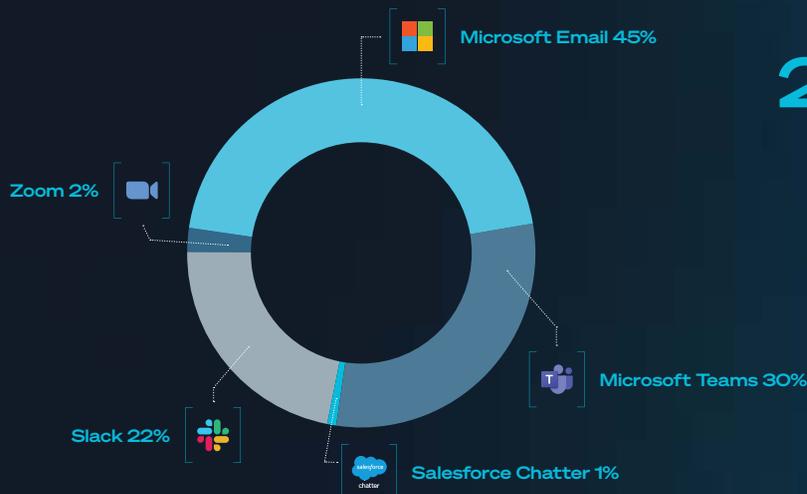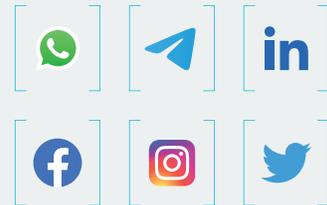
2. Get a no-cost 30-day Risk Assessment on the SafeGuard Cyber platform to quantify visibility gaps

Microsoft Email 45%

Zoom 2%

Microsoft Teams 30%

Slack 22%

Salesforce Chatter 1%

On average, **45% of business communications occur outside of email,** with some lacking any visibility into 1/3 of inbound and outbound communications.

Chart based on real customer's monthly data.

3. Use metrics that matter to continuously assess risk with leadership and stakeholders

34.8K
External Communications

27.4K
Inbound Attachments

9.5K
Outbound Attachments

OVERALL RISK LEVEL

| Low | Medium | Elevated | High | Critical |

Chart based on real customer's montly data.

SafeGuard Cyber integrates directly into communication channels via APIs to process content and metadata in over 50 languages. Using patented Social Engineering Detection technology, we help organizations to detect and respond to cyber risk in human communications at scale.

CONTACT US