NOT EVERYONE IN YOUR ORGANIZATION IS A VIP.

But anyone can be a VAP: Very Attacked Person™

And these VAPs aren't always the people you expect.

Our latest Protecting People report analyzes email attacks on Fortune Global 500 companies between October 2018-January 2019. We examined who's being targeted, how, and what organizations can do about it. Here are some highlights:

WHO'S BEING ATTACKED

Among the most targeted malware and credential phishing attacks, nearly

30% targeted generic email aliases.

These email addresses are typically shared within an organization.

Individual contributors and lower-level management accounted for

72% of highly targeted malware and phishing attacks,

up 5 percentage points from the previous quarter.

Your VAPs aren't always your VIPs.

Workers in production and operations functions were by far the most targeted group,

22% of highly targeted attacks.*
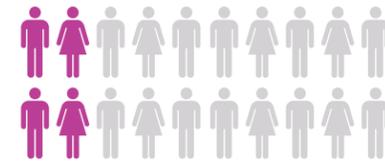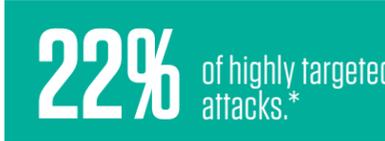
sales 14%
management 13%

*malware and credential phishing

Attacks against telecommunications firms skyrocketed more than

1,700%*
477 attacks per company.

Most industries saw triple-digit or higher surges in the number of email fraud attacks.

Attacks against government agencies soared nearly

1,648%*
107 attacks per entity.

*vs. the year-ago quarter

HOW THEY'RE BEING ATTACKED

Among organizations targeted in email fraud nearly

60% saw fraud attempts that spoofed more than five identities.

Nearly 80% were targeted in attacks that tried to send fraudulent email to six or more people.

Among organizations targeted by email fraud, more than

40% were the intended recipients of 50 or more fraudulent emails.

That's 4x the year-ago percentage.

Web-based attacks that use social engineering grew

150% vs. the previous quarter.
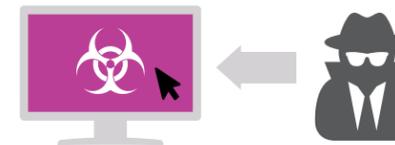
Fraudulent social media support account phishing, jumped

442% vs. the year-ago quarter.

Download the full report at proofpoint.com/us/resources/threat-reports/quarterly-threat-analysis

0219-063