BYE-BYE, BURNOUT: SAVE SECURITY TEAMS TIME WITH AUTOMATION

Employees are often described as weak links in organizations' security. But when companies make it easy to report phishing emails, employees can be the first line of defense.

More reported emails makes more work for security teams. That's why automation is key.

On average, organizations with 1 000 seats report

116

emails per month.

On average, organizations with 10 000 seats report

1 160

emails per month.

Time to manually investigate a phishing report

EXPERIENCED SECURITY TEAMS

15 minutes to an hour

INEXPERIENCED/ UNDERSTAFFED TEAMS

Up to 5 hours

Automated phishing triage saves security teams time

OUT OF THE REPORTED EMAILS,

over 99%

WERE HANDLED PURELY BY AUTOMATION

Less than 1%

REQUIRED SOMEONE TO INVESTIGATE MANUALLY

Time spent manually investigating phishing reports per month

FOR A 1000-SEAT COMPANY:

29 hours to 580 hours

FOR A 10,000-SEAT COMPANY:

290 hours to 5800 hours

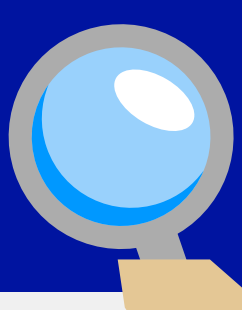
Time spent manually investigating phishing reports per month, with automated phishing analysis and triage

FOR A 1000-SEAT COMPANY:

17 minutes to 5.8 hours

FOR A 10,000-SEAT COMPANY:

2.9 hours to 58 hours

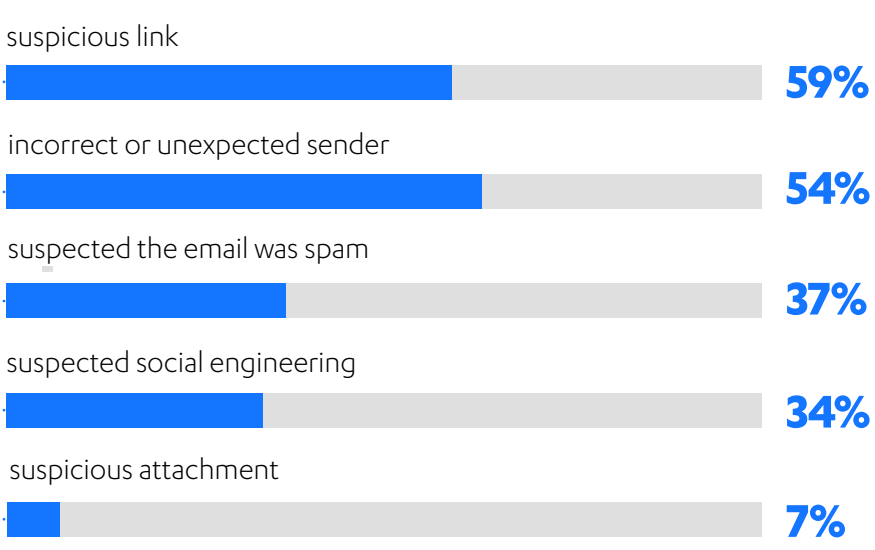


MAKING PHISHING REPORTING EASY IS WORTHWHILE

99% of the reported emails were handled purely by automation. 33% were automatically deemed malicious or suspicious.

The remaining 1% of emails were submitted for additional manual analysis, and 63% of those were deemed malicious or suspicious.

Employees' reasons for reporting...

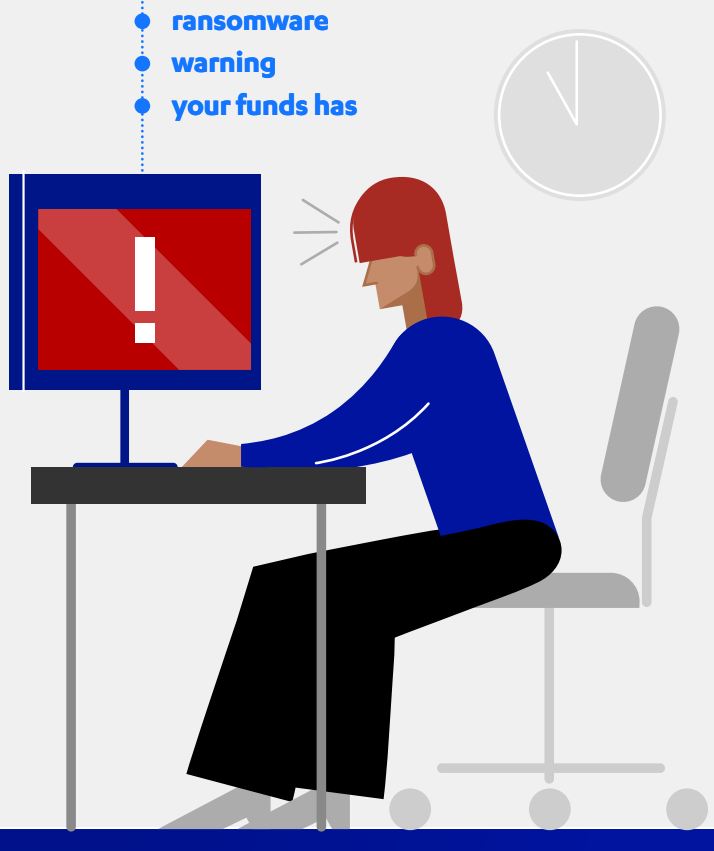


Top 10 most common suspicious words and phrases found in reported emails

	Phrase/word	Percentage containing word/phrase	Risk level
1.	click here	15	Medium
2.	Login	8	Medium
3.	Payment	8	Low
4.	please click	7	Medium
5.	Password	7	Low
6.	Record	6	Low
7.	please visit	5	Medium
8.	click here to	4	Medium
9.	M&A	3	Medium
10.	Bitcoin	3	Medium

High risk words and phrases

- dropbox
- amount of usd
- message is from a trusted
- ransomware
- warning
- your funds has



F-Secure