Help your employees fill the gap between phishing simulations and phishing attacks

vade

Romain Basset
Head of Presales @ Vade

ABOUT US

We protect digital communications

- **Global leader**
  in predictive email defense.
- **Specialized in the fight against cyber-attacks**

  Phishing, Spear phishing,
  Malware, Ransomware.
- **Focus**
  on threat detection, user awareness and incident response.

Where the magic happens

Lille, Paris	**France**
Tel Aviv	**Israel**
Boston, San Francisco	**US**
Montreal, Vancouver	**Canada**
Tokyo	**Japan**

Go to Market

Consumer email
through ISPs & Telcos

BT · Telefónica · vodafone · orange · COMCAST · EarthLink · verizon media · NTT Communications · SoftBank · TELSTRA · Spark

1 billion mailboxes protected

Corporate market
100% through Channel

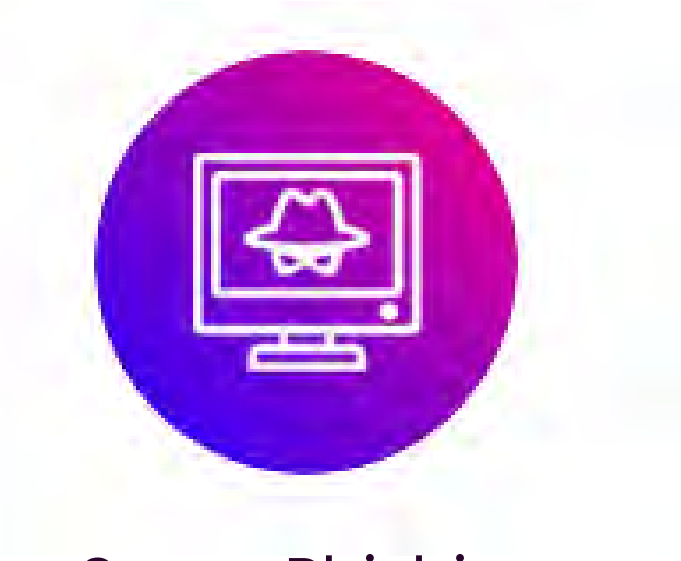
ALSO · resello · Microsoft Partner Network · MINDWARE · ARROW · D&H · LOGICOM · Orange Cyberdefense · GIACOM · GLOBAL SECURITY NETWORK · ALLTRON · SYNNEX CORPORATION · CRIS · MiEL

A little pat on the back

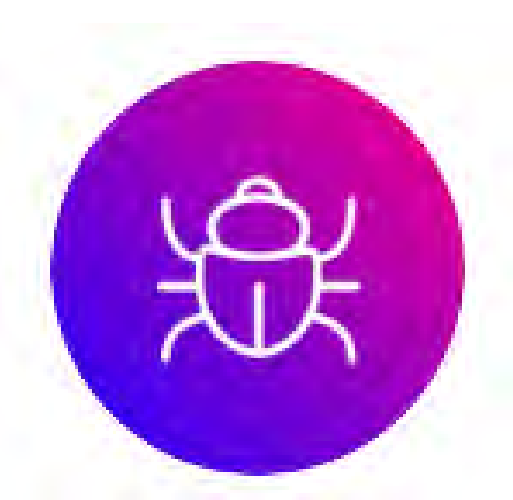
Threat landscape & current trends

Most common types of threats employees face

Phishing



Spear Phishing

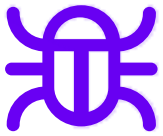


Malware / Ransomware

Current trends

91% of cyberattacks start with an email [1]

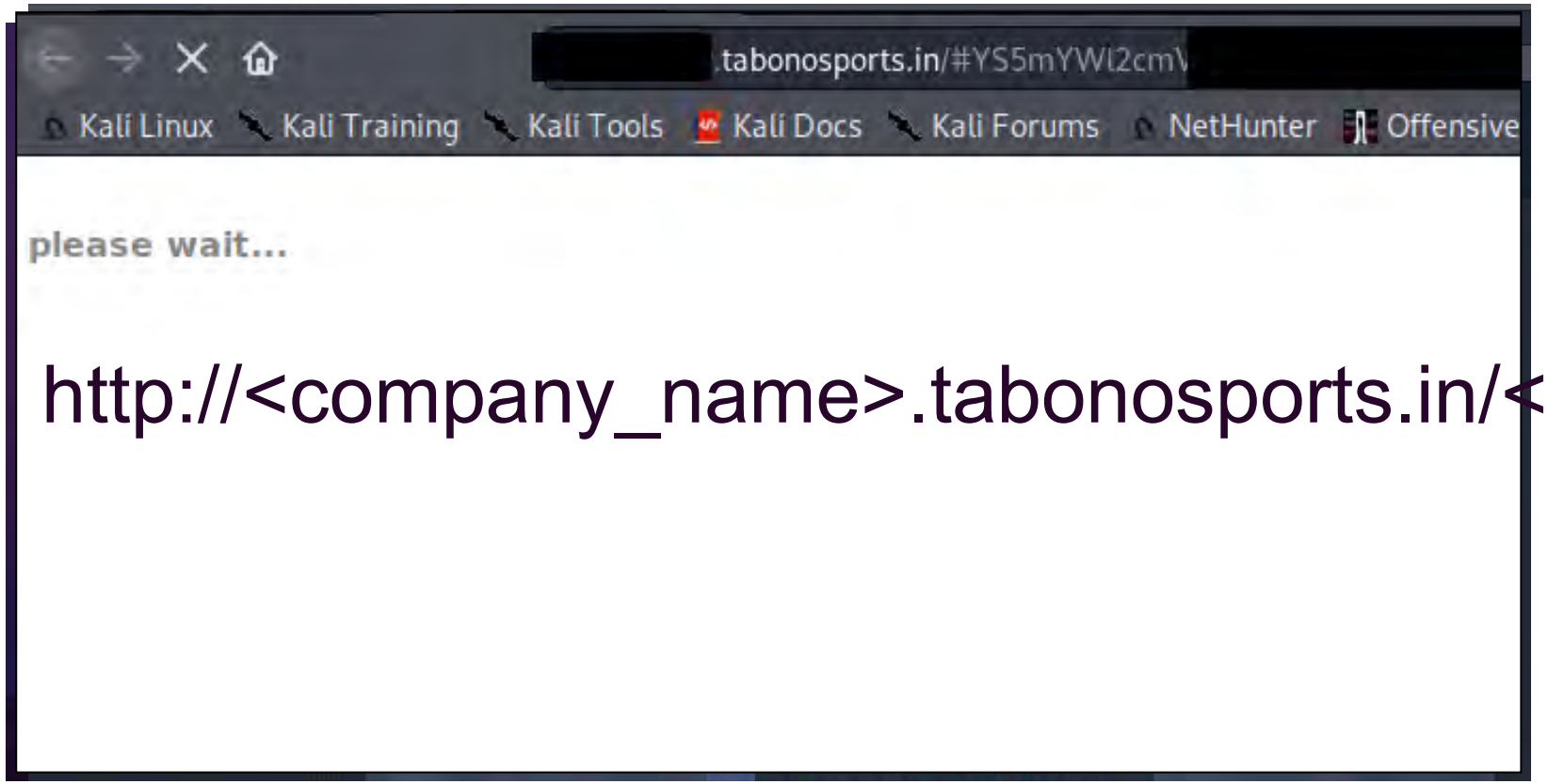
Attacks are much more targeted



Cybercriminals use leaked data or ongoing events to make their attacks look more credible

[1] Deloitte, Jan 2020

Phishing example



Abuses Microsoft API to automatically pull background and logo from the targeted organization

Spear-Phishing example

URGENT

EC

Elizabeth [redacted] <mngnt123@icloud.com>

À Erica [redacted]

ven. 07/05

Erica Are you busy ?
Need you to run a quick errand, in a meeting
so wont be able to take calls just reply to this mail...

Spoofed CEO targeting assistant

Phishing Simulations

Benefits and Limitations

Phishing awareness training is highly effective at reducing phishing click rates, with the average click rate dropping to 3% in 2021.

But what happens after the training sessions and phishing simulations are over?

Click rates rise and reporting rates drop:

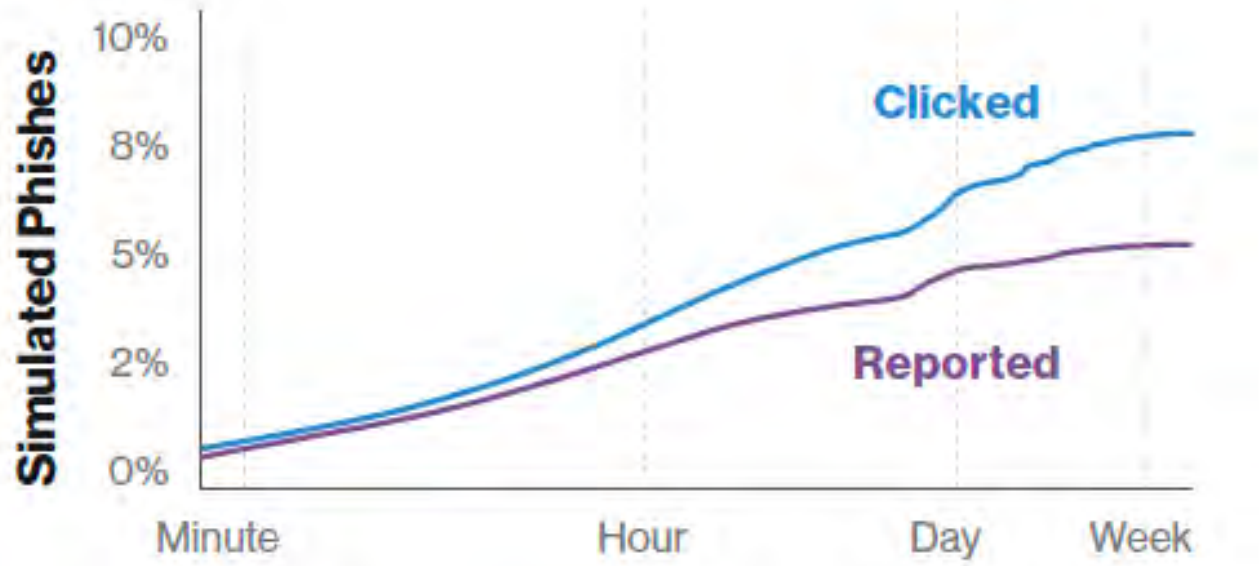


Figure 61. Click and reporting rate in public simulated phishes over time

Why are users still clicking after training?

They're generic: A generic phishing simulation doesn't connect with users on a personal level.

They're static: "Build your own phishing email" simulations are one-off emails that are time-consuming to create and difficult to generate on an ongoing basis.

They're periodic: Phishing simulations are sent at random intervals and not at the moment of need.

The importance of training in context

Lack of context = low click rates

"The simulations and training offered by most security education teams do not mimic real life situations, do not parallel the behaviors that lead to breaches, and are not measured against real attacks the organization receives."

"2021 Data Breach Investigations Report"

Verizon

Providing continuous contextualized training

- Simulations without context result in low click rates.
- The more targeted the email, the more successful the phish.
- Creating contextual, targeted phishes is time-consuming.
- Targeted phishes need to be sent on a continual basis.

Adding reinforcements between simulations and training

Catch them while you can

Vade Threat Coach

Demonstration

Key Benefits for Businesses

On the Fly

Delivers training content at the moment of need – post-incident.

Contextual

Generates contextual training content based on the user's profile.

Dynamic

Uses real phishing emails, updated daily with fresh examples.

Key Benefits for MSPs

Automated

Requires no manual setup, administration or maintenance.

Complementary

Reinforces best practices/ complements simulation platforms.

Added-Value

Provides added value without added costs for the MSP.

Questions?

vade

romain.basset@vadesecure.com