YOU DESERVE THE BEST SECURITY

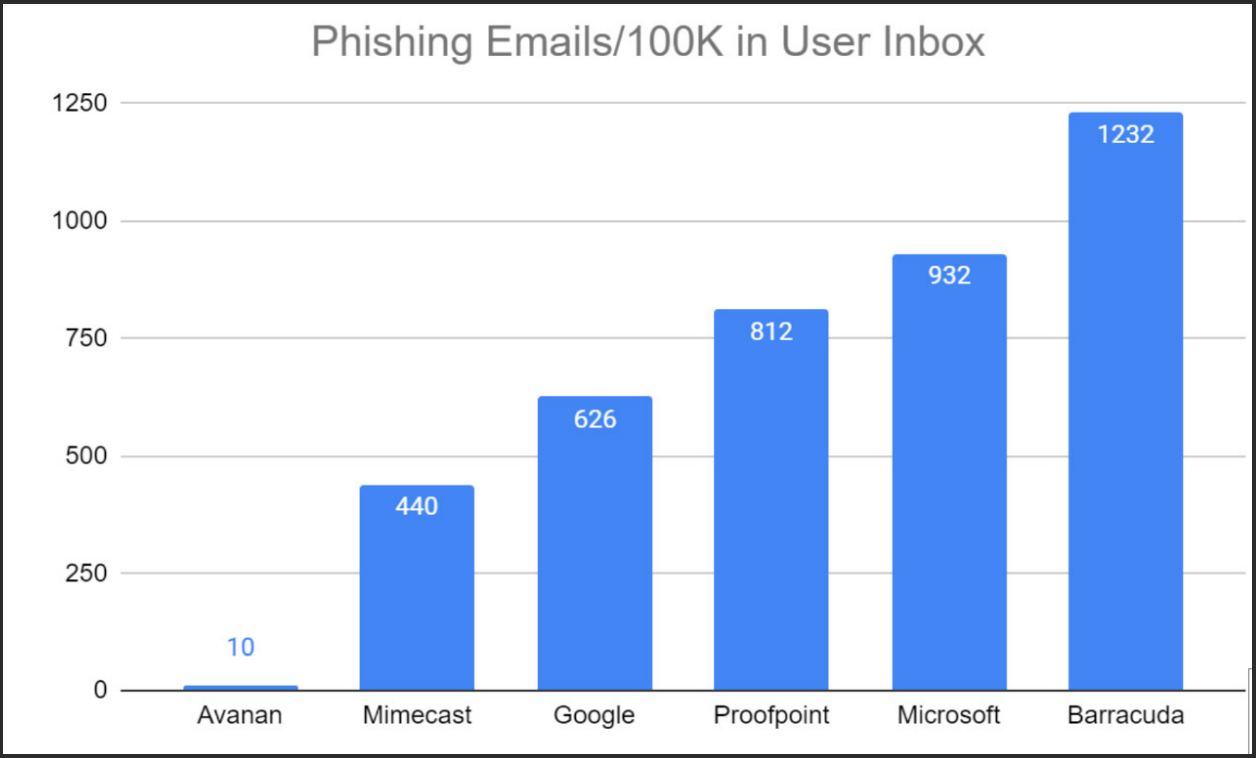
How Many Phishing Emails Do Security Solutions Miss?

Executive Summary

In a new study, Avanan analyzed over 300 million emails to determine the efficacy of vendors at keeping phishing emails out of the end-users inbox.

Measuring such results is only possible through Avanan's unique positioning. With our embedded approach behind Microsoft, Google, and SEGs like Proofpoint, Mimecast and Barracuda, we see the attacks that they miss. This allows us to analyze their true miss rate.

In this study, we analyzed emails over a course of six months, from April 2021 to October 2021. We measured the number of phishing emails hitting the inbox per every 100,000 messages. According to our findings, we found that legacy approaches consistently allow far more phishing emails into the inbox than Avanan.

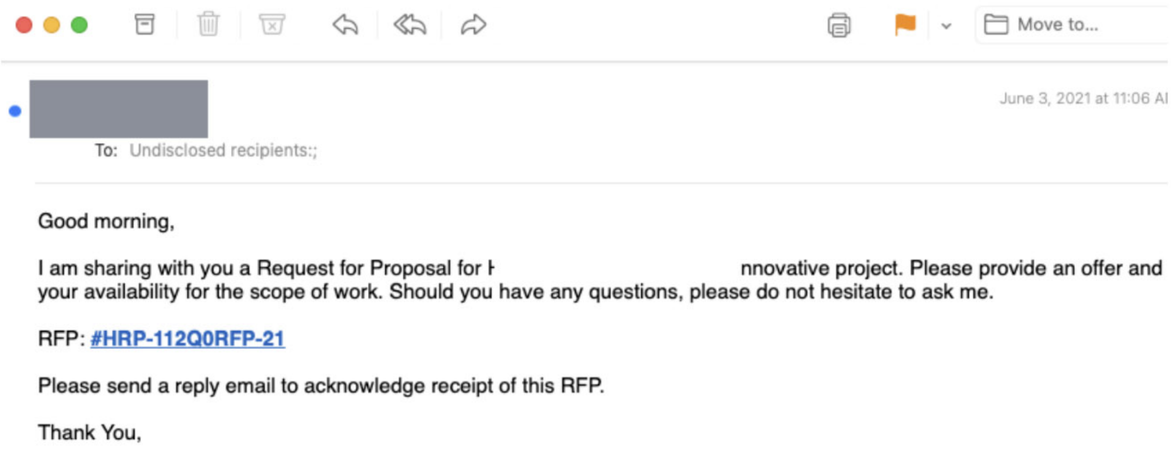


Avanan stops the attacks that others miss, which is one reason for the large discrepancy between our solution and the others.

When analyzing other solutions, we need not go far to see examples of attacks that all these other companies missed. In this report, we'll examine some real-world attacks that were missed by legacy solutions and ended up in the user's inbox.

Mimecast

In this attack that Mimecast missed, hackers leverage sites that are already on static allow lists. To do so, they embed phishing content with these services, in this case, Adobe Spark. Because Adobe is a major company that's often trusted by users, it's on Allow Lists, and so it sails through to the inbox, regardless of whether phishing content has been embedded on the platform. According to Avanan research, 8.14% of phishing emails ended up in the user's inbox due to an Allow or Block list misconfiguration. When using an SEG like Mimecast, that number rises to 15.4%.



[redacted]

June 3, 2021 at 11:06 AI

To: Undisclosed recipients:;

Good morning,

I am sharing with you a Request for Proposal for H nnovative project. Please provide an offer and your availability for the scope of work. Should you have any questions, please do not hesitate to ask me.

RFP: #HRP-112Q0RFP-21

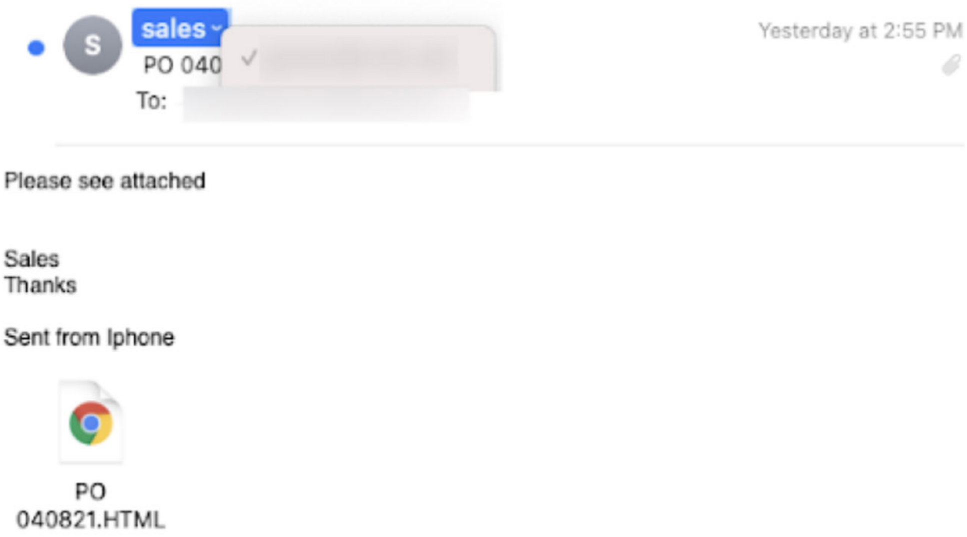
Please send a reply email to acknowledge receipt of this RFP.

Thank You,

Google
The static HTML file in this email may look harmless, and Google thought so as well. However, when clicking on the HTML attachment, the user is directed to a webpage that looks a lot like an Excel spreadsheet:

Google

The static HTML file in this email may look harmless, and Google thought so as well. However, when clicking on the HTML attachment, the user is directed to a webpage that looks a lot like an Excel spreadsheet.



PO 040 [redacted]

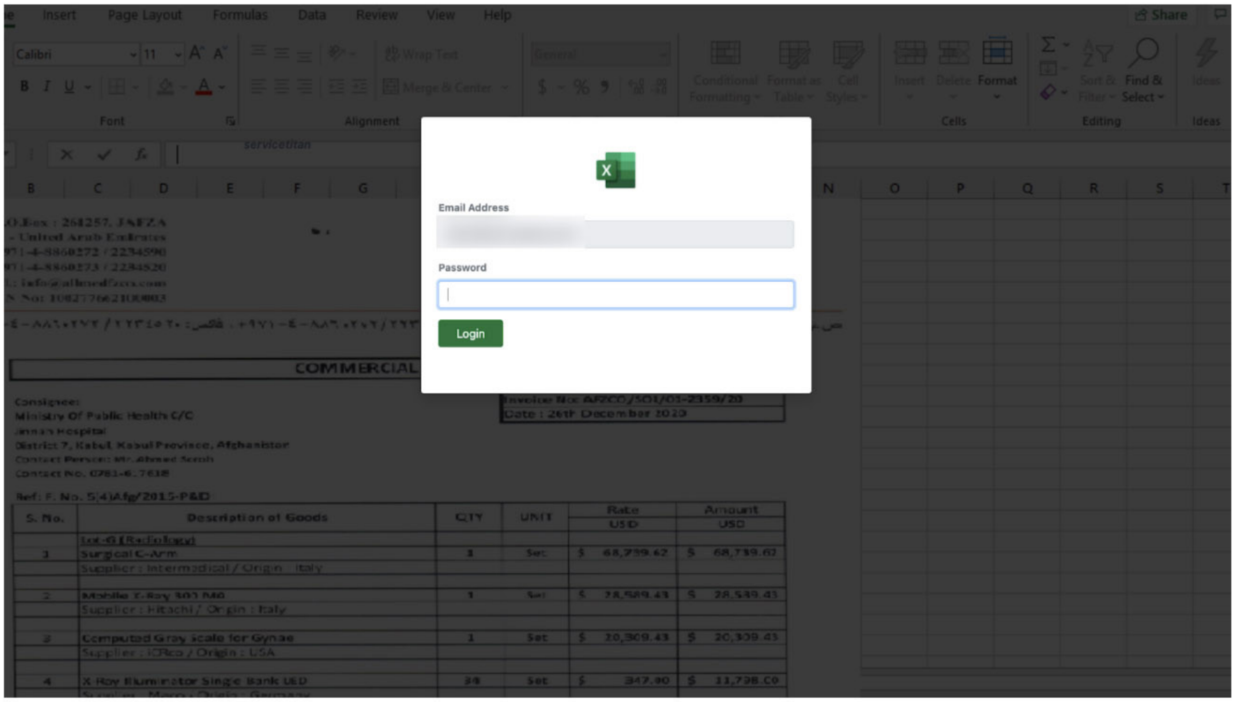
To: [redacted]

Please see attached

Sales
Thanks

Sent from Iphone

PO
040821.HTML



Email Address

[redacted]

Password

Login

O.Box : 261257, JAFZA
- United Arab Emirates
971-4-8860272 / 2234590
971-4-8860273 / 2234520
L: info@alliedfzco.com
N No: 100277662100003

COMMERCIAL

Consignee:
Ministry Of Public Health C/C
Jinnah Hospital
District 7, Kabul, Kabul Province, Afghanistan
Contact Person: Mr. Ahmed Sorsh
Contact No. 0781-6.7618

Invoice No: AFZCO/SOI/01-2359/20
Date : 26th December 2020

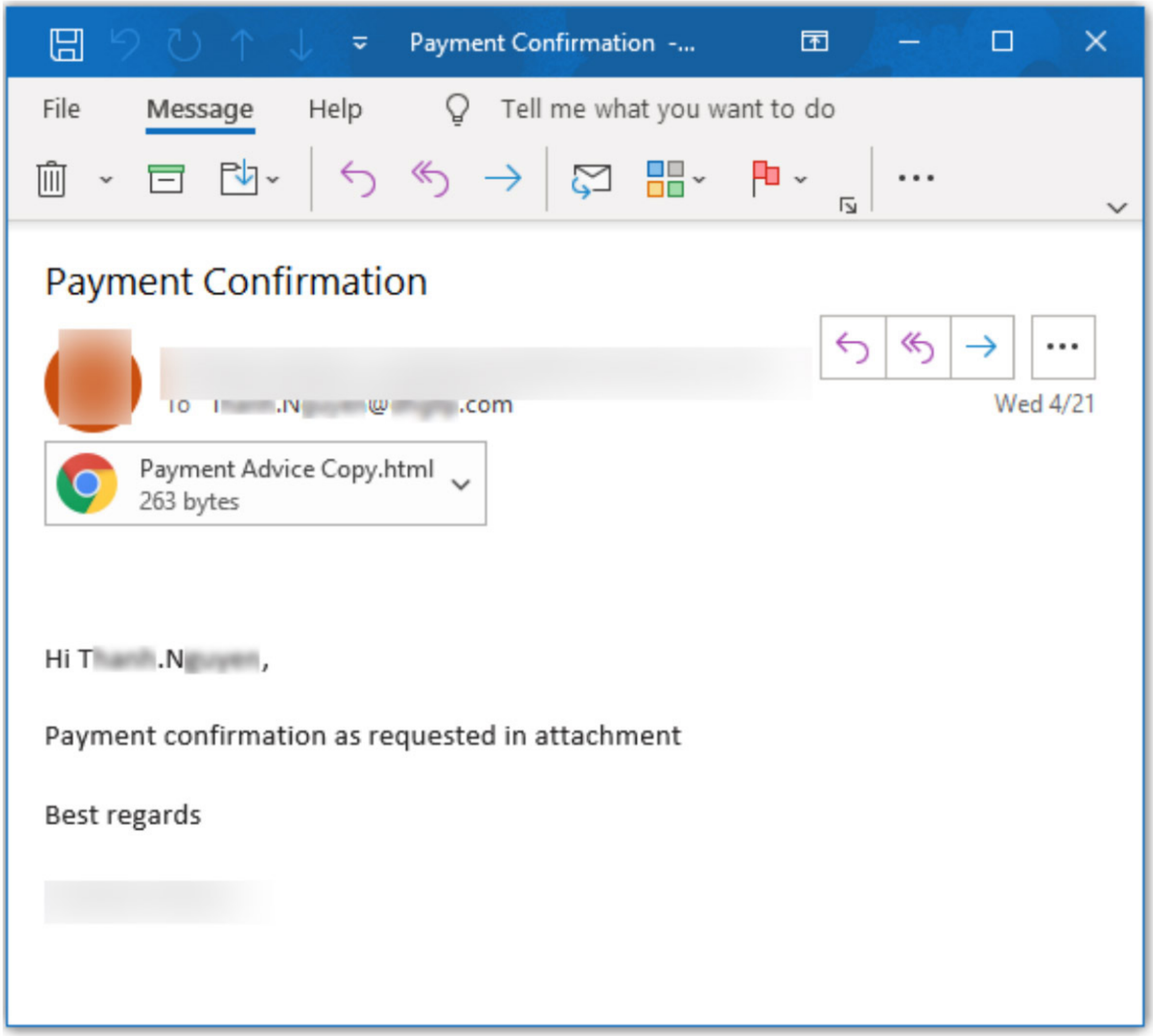
Ref: F. No. 5(4)Afg/2015-P&D

S. No.	Description of Goods	QTY	UNIT	Rate USD	Amount USD
	Lot-G (Radiology)				
1	Surgical C-Arm	1	Set	$ 68,739.62	$ 68,739.62
	Supplier : Intermedical / Origin : Italy				
2	Mobile X-Ray 300 MA	1	Set	$ 28,589.43	$ 28,539.43
	Supplier : Hitachi / Origin : Italy				
3	Computed Gray Scale for Gynae	1	Set	$ 20,309.43	$ 20,309.43
	Supplier : ICRco / Origin : USA				
4	X-Ray Illuminator Single Bank LED	34	Set	$ 347.00	$ 11,798.00
	Supplier : Mavo / Origin : Germany				

When entering a password, it immediately gets stolen by the hackers.

Proofpoint

In this email missed by Proofpoint, end-users see what looks like a payment confirmation notice.



Payment Confirmation

[redacted]

To T[redacted].N[redacted]@[redacted].com

Wed 4/21

Payment Advice Copy.html
263 bytes

Hi T[redacted].N[redacted],

Payment confirmation as requested in attachment

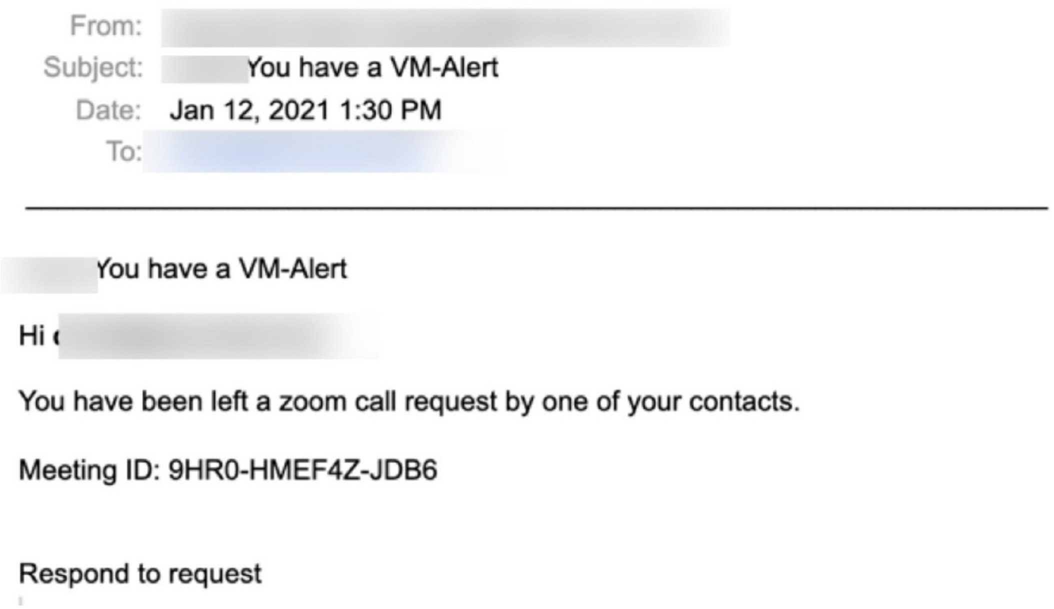
Best regards

[redacted]

One of the many reasons our AI detected this as phishing was due to an insignificant historical reputation with the sender. Our research has found that 84.3% of all phishing emails do not have a significant historical reputation with the victim.

Microsoft

Many attacks leverage popular apps. This attack, missed by ATP, pretends to be a request for a Zoom call. However, the Zoom meeting ID is static, and the link is malicious.



From: [redacted]
Subject: [redacted] You have a VM-Alert
Date: Jan 12, 2021 1:30 PM
To: [redacted]

[redacted] You have a VM-Alert

Hi [redacted]

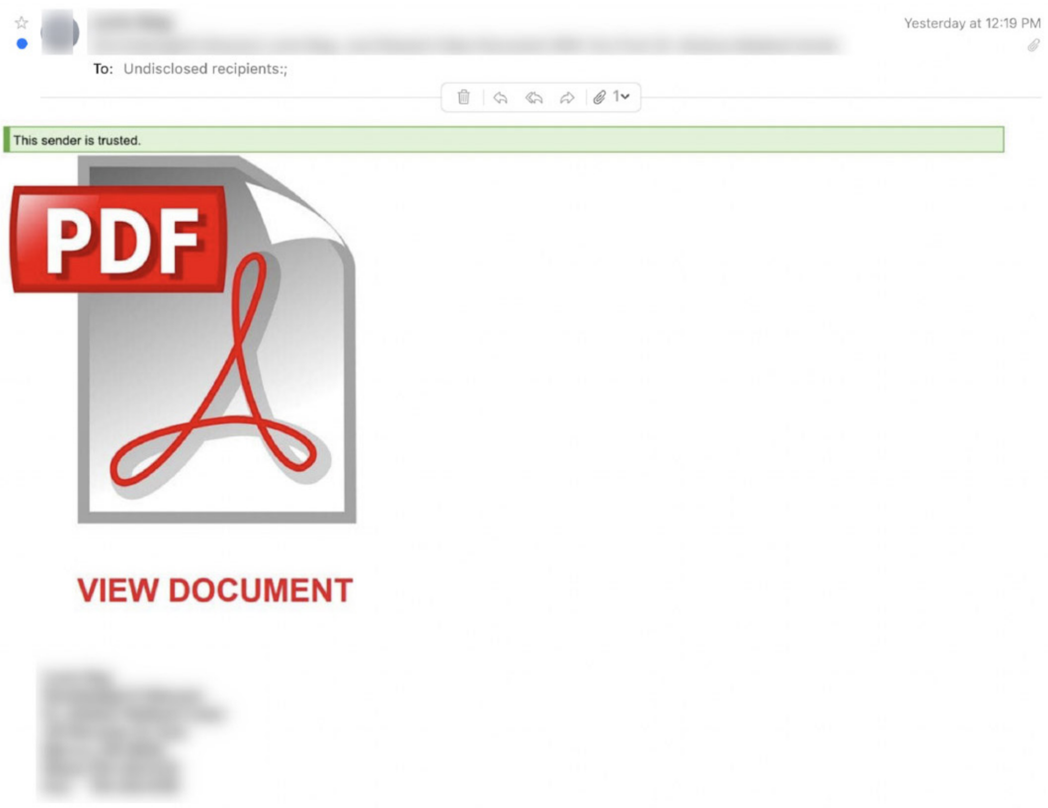
You have been left a zoom call request by one of your contacts.

Meeting ID: 9HR0-HMEF4Z-JDB6

Respond to request

Barracuda

In this attack, hackers are sending emails from a trusted user. The hacker adds a header that says, “This sender is trusted,” allowing the end-user to believe that email can, in fact, be trusted. On the contrary, the PDF logo is actually just a large image, with an embedded link that leads to a credential harvesting website. According to our research, credential harvesting scams make up 54% of all attacks.



[redacted] Yesterday at 12:19 PM

To: Undisclosed recipients:;

This sender is trusted.

VIEW DOCUMENT

[redacted]

What Makes Avanan So Effective?

Avanan's patented approach to email security clearly protects inboxes better than legacy options. Avanan is an API-enabled email security provider, embedded within cloud email. Being embedded is critical to establishing an AI and ML-based detection system. By training our AI on a robust set of data and the attacks that others miss, we're able to provide a far superior catch rate with more capabilities and can install in just five minutes.

Additionally, as a Check Point company, Avanan's SmartPhish integrates with Check Point's ThreatCloud, a threat intelligence database that includes 42 separate machine learning and AI engines. These engines do 86,000,000,000 transactions a day, finding over 7,000 previously unknown malware and zero-day malware per day. By combining superior email security with superior threat intelligence, Avanan's email security offering has established itself as the clear market leader.

CALCULATE YOUR SOLUTION'S MISS RATE

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com