# CHATGPT-FUELED PHISHING

## safeguarding your organization

Digital Security
**Progress. Protected.**

# ChatGPT-Fueled Phishing Rises as Defender Teams Trim Down

Tech companies worldwide are adopting leaner approaches, accomplishing more with fewer staff members. However, this trend also empowers attackers, as clever automation provides them with a new advantage. By generating natural language phishing emails tailored to specific regions, these attacks become significantly more challenging to detect and are likely to result in higher click rates.

Considerable ethical research surrounds ChatGPT and its large language model (LLM) counterparts, aiming to prevent malicious use such as creating harmful malware. However, numerous alternatives yield excellent results through slight question modifications. So, for instance, rather than asking how to attack an organization, tell the model you are doing a report about the subject and need some help with examples. Then cut/paste those into your attack, and it can be a great boost to your workload. In a game of cat-and-mouse, attackers can still significantly reduce their workload by utilizing the model and its competitors.

To address this issue, defending organizations should strengthen their defenses by assuming a higher effectiveness of phishing attacks. Additionally, they should implement automation measures to proactively prevent any potential data breaches from being exfiltrated by attackers.

## PROTECTIONS OF THE ANTISPAM LAYER

Organizations are frequently targeted by phishing attempts through various channels, including email messages, web pages designed to mimic trusted sources, and even phone calls. It’s important to note that SMS messages and messaging apps on smartphones can also be potential sources of phishing attacks.

In the case of email, phishing messages are typically handled as a type of spam, since it is an unwanted communication. While they may not be considered spam in the conventional sense, as they are neither a bulk communication nor a commercial advertisement, phishing messages can be highly targeted to the victim’s role and interests. However, it is important to note that the message body itself is of a criminal nature. This means that machine learning techniques can be used to analyze both the message body and header to identify phishing characteristics by classifiers in an antispam engine running on the mail server and/or the endpoint.

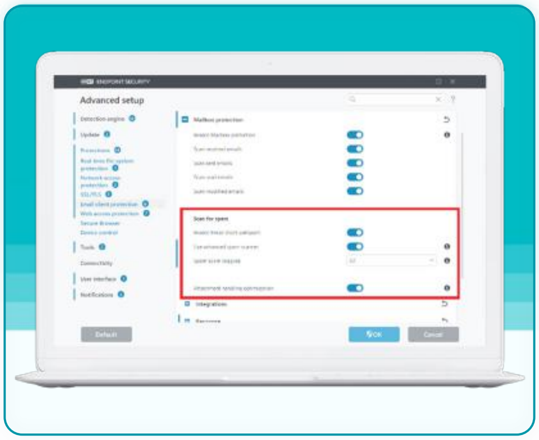
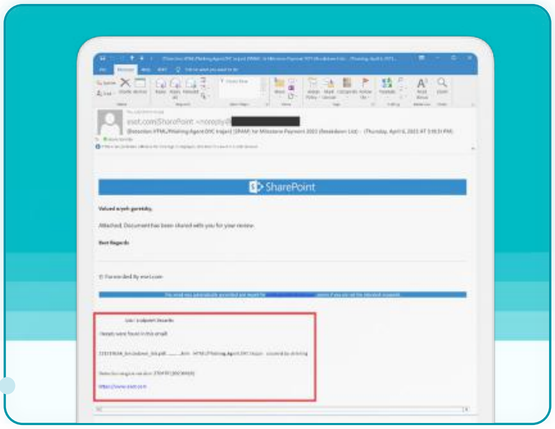


*Figure 1 - Example of antispam engine configuration options on an endpoint.*

When it comes to message headers, domain names, email addresses, and other metadata, they can be compared to previously seen messages to identify any attempts of typo-squatting. Analyzing header information would have little effect against a phishing attempt sent from a legitimate but compromised email account.

A message's header and body are not the only places that can be analyzed for phishing. Both the header and the body of an email message can appear harmless, while the actual phishing component may be a document attached to the message.

The attached document itself does not necessarily need to have any malicious code in it, although it could. It could contain a set of detailed instructions for the victim to follow, or it may simply include an email address, website, or phone number with a pretext for the victim to contact. The message may not even be typed; it could be a screenshot that has been pasted into the document. Alternatively, it could be a document with fields to fill out and return to the phisher.



eset.com/SharePoint <noreply@[redacted]

SharePoint

Attached, Document has been shared with you for your review.

Best Regards

*Figure 2- Example of detection of HTML phishing content in a PDF file.*

Regardless of the various methods through which a file can convey information to a target, its contents can be analyzed to determine if it contains a phishing attempt. Even an image of text can be read through OCR technology, allowing the contents to be evaluated. However, depending on the environment, it may be more efficient to handle this process at the mail server rather than at the endpoint.

## FIGHTING SUPER PHISHING WITH AUTOMATION

To combat amped-up phishing, operators should look at implementing a variety of techniques like Data Loss Protection (DLP), which classifies data based on the context of its sensitivity and then restricts access.

Many organizations are implementing additional measures to restrict data exfiltration. These measures assume that an attack may be successful but aim to limit the overall impact through techniques such as EDR, MDR, and XDR.

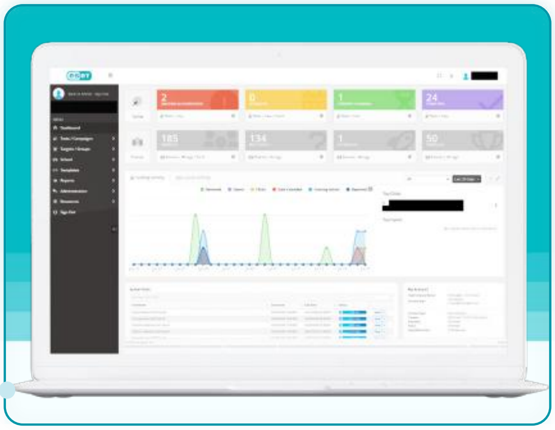
## FIGHTING FIRE WITH…USER EDUCATION?!

It is important to note that despite the use of high-tech means for phishing and countermeasures to block them, no technical solution can guarantee 100% effectiveness at all times. The reason for this is not due to any deficiency in defensive technologies, but rather because phishing is not solely a technological problem—it is also a psychological one.

Adversaries utilize LLMs to enhance, rework, and rewrite their phishing attempts, aiming to make the messages more compelling and believable to recipients. They do so to elicit the desired response, even though such actions ultimately work against the victim's self-interest.

So, how do you protect against an idea? It is possible to combat these ideas as well, but through user education.

A fundamental reason phishing attacks are successful is that victims often fail to realize they are being targeted. They assume the communication they receive is authentic, sincere, and beneficial to their own self-interest because it appears to come from a trusted source such as a manager or business partner.



[redacted]
[redacted]

*Figure 3 – Example of measurable results from training.*

The key to preventing this is user education. By offering users cybersecurity awareness training, you can provide them with the mental tools necessary to recognize signs of phishing and build a kind of HIPS or firewall to protect against such attacks, safeguarding your organization before any compromise occurs.

## ABOUT ESET

For more than 30 years, ESETR has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide. ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

Digital Security
**Progress. Protected.**