THE BEST PROTECTION AGAINST SPEAR PHISHING

SPEAR PHISHING: A HARD SCAM TO DETECT

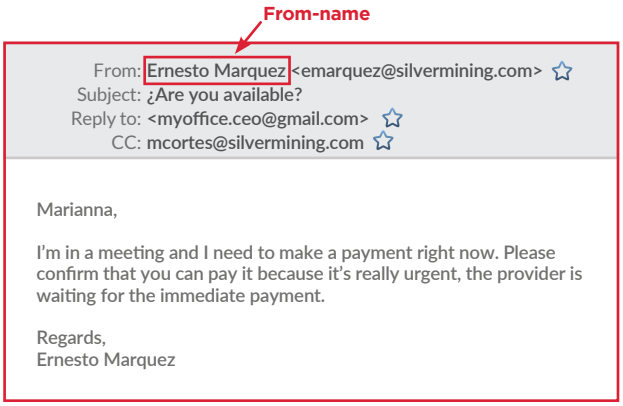
Spear Phishing, also called identity theft, is a technique used by hackers to carry out scams known as Business Email Compromise **(BEC) or CEO fraud.** These email-spread threats are growing rapidly, and unlike Phishing campaigns, which target many people at once, Spear Phishing singles out specific groups or individuals.

These attacks are of great concern to IT managers because they are difficult to detect and, when successful, are capable of causing costly damages.

Zerospam has developed advanced features, and a cutting-edge option called Targeted Threat Mitigation, which blocks Spear Phishing attacks. These two methods provide the best level of protection that exists against threats.

Keys to identify Spear Phishing email

- Emails sent to a limited group or specific individual by a sender within the organization
- The sender is a person with the authority to initiate money transfers or share sensitive data
- At first glance, messages appear to be internal emails
- Emails usurp the identity of people in positions of power **(CEO, CFO, Manager, etc.)**



1 - ZEROSPAM TARGETED THREAT MITIGATION (TTM) - AN ADVANCE

After analyzing the problem thoroughly, **Zerospam** has created the **TTM security option**; available at no additional cost. This option blocks incoming emails based on the most incriminating part of a Spear Phishing campaign: the identity of the person the hacker is trying to appropriate. When activated, the option allows you to define a list of "usurped senders" based on the names of the people that cybercriminals could try to usurp. Since Spear Phishing attempts are meant to pass as internal emails, our specialized option will quarantine messages sent to your organization's network using the From-Name of people on the list.

Example:

Based on the assumption that hackers could try to usurp the identity of Jorge Morales or María Hernández, any incoming mail from those From-Names will be quarantined.

Name	Action to take
Jorge Morales	Quarantine
María Hernández Antonio	Quarantine

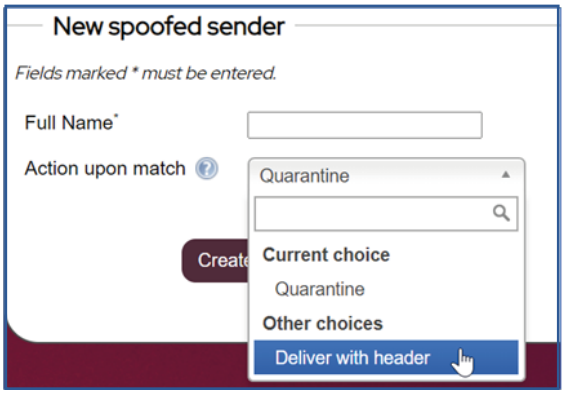
INTCOMEX CLOUD

zerospam

Additional Information

- When adding a new "usurped sender", you can also put in place **transportation rules** to take action when Spear Phishing emails are detected—for example, adding a danger label to emails. This can be done using the Zerospam header once the email has been filtered.

- Before adding a new name to the "usurped senders" list, personal email addresses used to send legitimate messages (such as Gmail or Hotmail) should be whitelisted; otherwise, all mail from these addresses will be blocked.

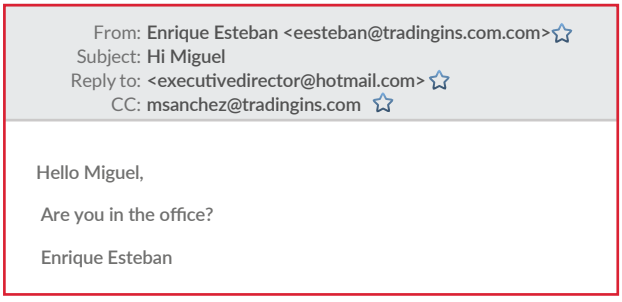


2 - INCORPORATED PROTECTION AGAINST SPEAR PHISHING

Zerospam also includes protection that recognizes and blocks Spear Phishing attempts. No special configuration is required; clients are protected by default.

Example Step 1 of a Spear Phishing email

During the preparation of his social engineering, the spammer knows that he must usurp Enrique Esteban and send his request to Miguel Sánchez. If Miguel answers the received mail, the spammer can continue to the next level and send his instructions by mail. Since Miguel has had a previous exchange with Enrique, he will be less likely to suspect.

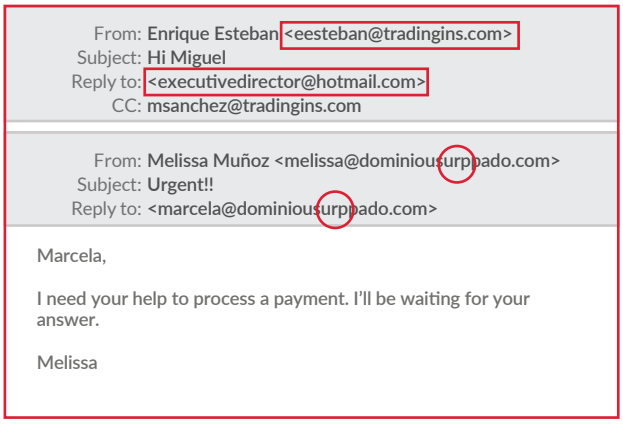


In 2017, after a Spear Phishing campaign managed to trick a group of employees into wiring money to hacker-controlled bank accounts overseas, Google and Facebook lost $ 100 million each. Spammers don't just attack big companies; victims range from small businesses to corporate giants.

Zerospam built-in protection against Spear Phishing uses advanced features that are based on:

- The correspondence between the email address of the content-from (visible part of the FROM), the envelope-from (the actual location of the sender), and the reply-to address
- The reputation and validity of the sending domain
- Differences between FROM and TO domains
- Diagnosis derived from machine learning algorithms

Notice that the reply-to address is a Hotmail address. Most users would not have noticed.
The Targeted Threat Mitigation option and built-in Spear Phishing protection work independently. When combined, they offer the most comprehensive protection against Spear Phishing out there.



To protect yourself against Spear Phishing and other email-borne threats, sign up for the free 30-day trial

30 DAYS FREE TRIAL

ventascloud@intcomex.com

INTCOMEX CLOUD

zerospam