# THE ULTIMATE SPEARPHISHING PROTECTION

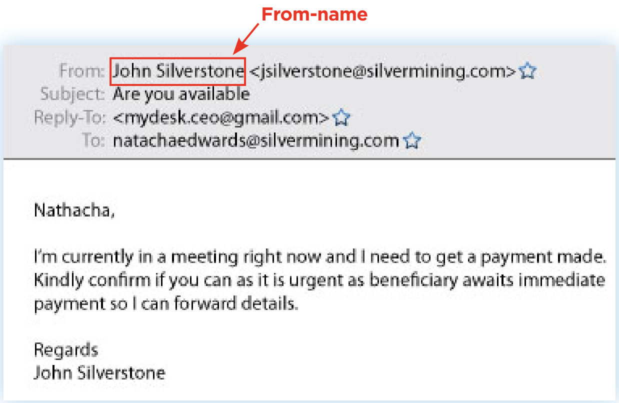
## SPEARPHISHING – A VERY DANGEROUS AND HARD TO DETECT SCAM THAT WEARS MANY NAMES

Spearphishing, also called Whaling, is a technique used by spammers to perpetrate scams called Business Email Compromise (BEC), CEO Fraud, or Business Executive Scam. This highly dangerous threat, usually propagated through email, is growing at a rapid rate. Contrary to phishing attacks which are one to many, these are aimed at a small number of very targeted individuals. IT Managers are extremely concerned about spearphishing because these attacks, when successful, represent huge losses and they are notoriously difficult to catch.

ZEROSPAM has developed advanced heuristics and a revolutionary Targeted Threat Mitigation module to effectively block spearphishing attacks. These two approaches currently represent the best protection in the industry against this type of fraud.

### Key identifiers of spearphishing messages

- Emails sent to a small number of recipients in your organization, at times, even only one.
- Recipients are people who can initiate wire transfers or release sensitive information.
- Messages are constructed to appear as though they are coming from inside your organization.
- Messages impersonate a key decision-maker in your organization (CEO, CFO, president, etc).



From-name

From: John Silverstone <jsilverstone@silvermining.com>
Subject: Are you available
Reply-To: <mydesk.ceo@gmail.com>
To: natachaedwards@silvermining.com

Nathacha,

I'm currently in a meeting right now and I need to get a payment made. Kindly confirm if you can as it is urgent as beneficiary awaits immediate payment so I can forward details.

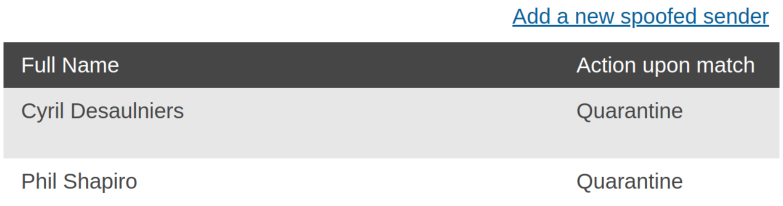
Regards
John Silverstone

## 1 - TARGETED THREAT MITIGATION FROM ZEROSPAM – A BREAKTHROUGH TECHNIQUE

After in-depth analyses of the problem, ZEROSPAM has built a Target Threat Mitigation module that is available at no extra cost. This feature blocks incoming messages based on the most incriminating factor in any spearphishing attack: the name of the person the spammer is impersonating. When activated, it enables organizations to define a list of Spoofed Senders based on the names of the people spammers will try to impersonate. Since spearphishing threats are built to appear as if they were coming from inside your organization, this highly specialized system will quarantine all incoming messages sent from outside your organization using any of the names entered in the Spoofed Senders list as a From-Name.

### Example

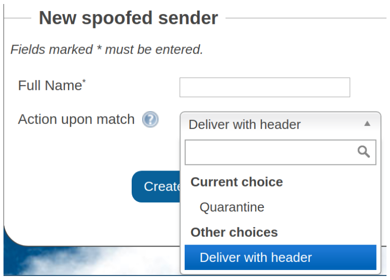
Since spammers will want to impersonate Cyril Desaulniers or Phil Shapiro, any messages received from outside your organization with these From-Names will be quarantined.



| Full Name | Action upon match |
|---|---|
| Cyril Desaulniers | Quarantine |
| Phil Shapiro | Quarantine |

### Additional information

- When adding spoofed senders, clients can also choose to implement transport rules on their server to take special action (such as adding a warning tag) when spearphishing messages are identified using the special header that ZEROSPAM adds.
- Before entering a name on the spoofed senders list, any personal email address (such as gmail, yahoo, hotmail, etc.) that may be used by this person to send legitimate messages to his organization must be whitelisted. Otherwise messages sent from this address will be blocked.



New spoofed sender

*Fields marked * must be entered.*

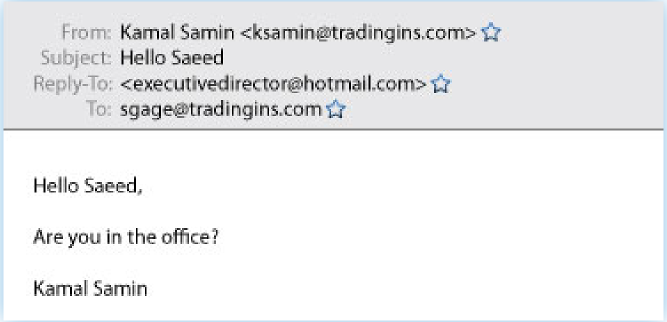
Full Name*:
Action upon match: Deliver with header

## 2 - BUILT-IN SPEARPHISHING PROTECTION

ZEROSPAM also offers built-in spearphishing protection that recognizes and blocks most spearphishing emails. It does not require any special configuration so customers are protected by default.

### Example of Stage 1 baiting spearphishing email

*From preparatory research, the spammer knows he needs to impersonate Kamal Samin and send his request to Saeed Gage. If Saeed replies, the spammer goes to the next stage and sends instructions by email. Since Saeed is now expecting him to reach out, he will be less suspicious.*



From: Kamal Samin <ksamin@tradingins.com> ☆
Subject: Hello Saeed
Reply-To: <executivedirector@hotmail.com> ☆
To: sgage@tradingins.com ☆

Hello Saeed,

Are you in the office?

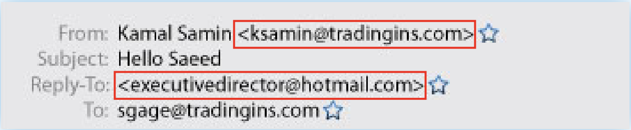
Kamal Samin

***In 2017, after a spearphishing email successfully induced employees into wiring to overseas bank accounts under the control of a hacker, Google and Facebook were taken for US$ 100 million each. But spammers are not just after huge organizations. The victims range from small businesses to large corporations.***

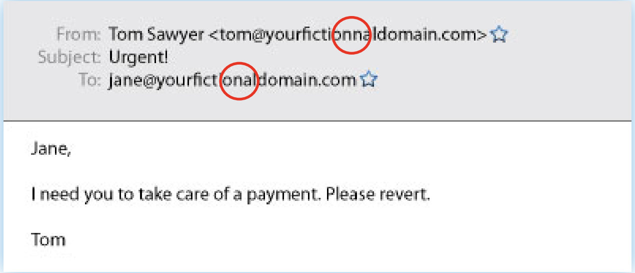
ZEROSPAM's built-in spearphishing protection uses advanced heuristics based on:

- The correspondence between the content-from (visible in the email FROM) and envelope-from addresses (the address that was really used to send this email) and the reply-to address
- The validity and reputation of the sending domain
- Small lexical differences between the FROM and TO domains
- Diagnosis derived from machine-learning algorithms

*Notice the reply-to is a Hotmail address. Most users would not notice this.*



From: Kamal Samin <ksamin@tradingins.com> ☆
Subject: Hello Saeed
Reply-To: <executivedirector@hotmail.com> ☆
To: sgage@tradingins.com ☆



From: Tom Sawyer <tom@yourfictionnaldomain.com> ☆
Subject: Urgent!
To: jane@yourfictionaldomain.com ☆

Jane,

I need you to take care of a payment. Please revert.

Tom

The advanced spearphishing module and the generic built-in spearphishing protection work independently from one another. When used together, they offer the most powerful protection currently available in the email security market against this very targeted and dangerous threat.

**30 DAY FREE TRIAL**

To protect yourself against spearphishing, and all other email-borne threats, sign up for the ZEROSPAM 30-day free trial at **www.zerospam.ca**

ZERO SPAM