

Spam ed e-mail pericolose

16/3/2018



E-mail

Posta tradizionale (veloce, non sempre)

Comunicazione asincrona

Comunicazione non verbale

Inadatta al confronto/scontro e alla critica

Non inviare informazioni sensibili e/o illegali

Pericoli di spedizione

Scripta manent

Inoltro indesiderato

Amplificazione dei destinatari

Lista in To: (usare Bcc:)

Pericoli in ricezione

Malware - Virus - Ransomware - Spyware - Adware - Trojan

Phishing - Furto di credenziali

Spam - Posta indesiderata

Spoofing - Mittente ingannevole

Backscatter - Conseguenza dello spoofing

Malware

Allegati (protetti da password)

Blocco eseguibili e zip

Antivirus - Firme apposite

VirusTotal

Link - URL shortener

Allegati

Italiano stentato

Password semplice

Non è spam

Buongiorno,

RingraziamoLa per ordine dei biglietti tramite la nostra sistema elettronica,

Dalla sua carta di credito e' stato preso 86 EUR.


la parola su archivio: 1234567

P.S. Se i dati non sono visualizzati, includono macroistruzioni.

Grazie.

--

Distinti saluti,
Ticket Service

▶  1 attachment: new8.zip 65,9 KB

↓ Save ▾

Phishing

Social engineering

Offerta imperdibile / segreta

Problemi con l'account

Problemi di consegna spedizione

Transazione / pagamento (non) a buon fine

Phishing

Non cliccare sui link

Non rispondere

Campagne

Firme AV apposite

PhishTank

The image shows a screenshot of an email interface with several red annotations pointing to suspicious elements:

- From:** Amazon <management@amazoncanada.ca> on behalf of @sheridanc.on.ca. A red box highlights the email address, with an arrow pointing to it and the text "not an Amazon email address (note the missing A in Amazon)".
- Subject:** Suspension.
- Body:** The email features the Amazon.com logo. Below it, the text "Dear Client," is highlighted with a red box and an arrow pointing to it with the text "Generic non-personalized greeting".
- The main body text reads: "We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it."
- A red box highlights the link: <https://www.amazon.com/exec/obidos/sign-in.html>. An arrow points to it with the text "Hovering over the link reveals it points to a non-Amazon site - 'http://redirect.kereskedj.com'".
- The email is signed "Sincerely, The Amazon Associates Team" with the Amazon logo.
- At the bottom, it says "© 1996-2013, Amazon.com, Inc. or its affiliates".

Spam

Pubblicità indesiderata (spedizione costa poco)

Newsletter (<https://www.mail-tester.com/>)

Interactive Marketing Solution | La Mirada Blvd, La Mirada, La Mirada, CA 90638

[Unsubscribe filippo.carletti@nethesis.it](#)

[Update Profile](#) | [About our service provider](#)

Sent by markconstant@interactivemarketingsoln.com in collaboration with

Trusted Email from
Constant Contact - Try it

FREE today.

Try it free today

Spam

SpamAssassin e Rspamd

Regole e Punteggi (Reject o Tag)


Filtri Bayesiani

DNSBL (RBL) - Delisting

Black e White list (From: -> whitelist)

Regole

Regole: positive, negative, neutre

Score  13.79 (Bayes: undefined, Fuzzy: undefined)

Rules RCVD_COUNT_TWO(0.00), HTML_SHORT_LINK_IMG_1(2.00), GREYLIST(0.00), ASN(0.00), SUBJECT_ENDS_EXCLAIM(0.00), RCVD_NO_TLS_LAST(0.00), FROM_HAS_DN(0.00), TO_DN_NONE(0.00), MX_GOOD(-0.50), PRECEDENCE_BULK(0.00), R_SPF_ALLOW(-0.20), RCPT_COUNT_ONE(0.00), TO_MATCH_ENVRCPT_ALL(0.00), DBL_SPAM(6.50), R_DKIM_PERMFAIL(0.00), FROM_NEQ_ENVFROM(0.00), R_WHITE_ON_WHITE(4.00), MIME_GOOD(-0.10), FORGED_SENDER_VERP_SRS(0.00), DMARC_NA(0.00), IP_SCORE(0.09), PREVIOUSLY_DELIVERED(0.00), INFO_TO_INFO_LU(2.00)

Invio Spam

SPF e DKIM

PTR

Abuso del server

Password deboli

Backscatter

Errori

Falso positivo - Mail valida in Spam

Falso negativo - Spam in Inbox

Allenamento filtri bayesiani

Analisi intestazioni (header)

Protezioni

Blocco allegati

Antivirus

Antispam

Filtro Contenuti

Client (MUA): non scaricare contenuti remoti

Rspamd

Prestazioni

Greylisting

Punteggi

Beta

Forum

Rspamd filter stats

