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

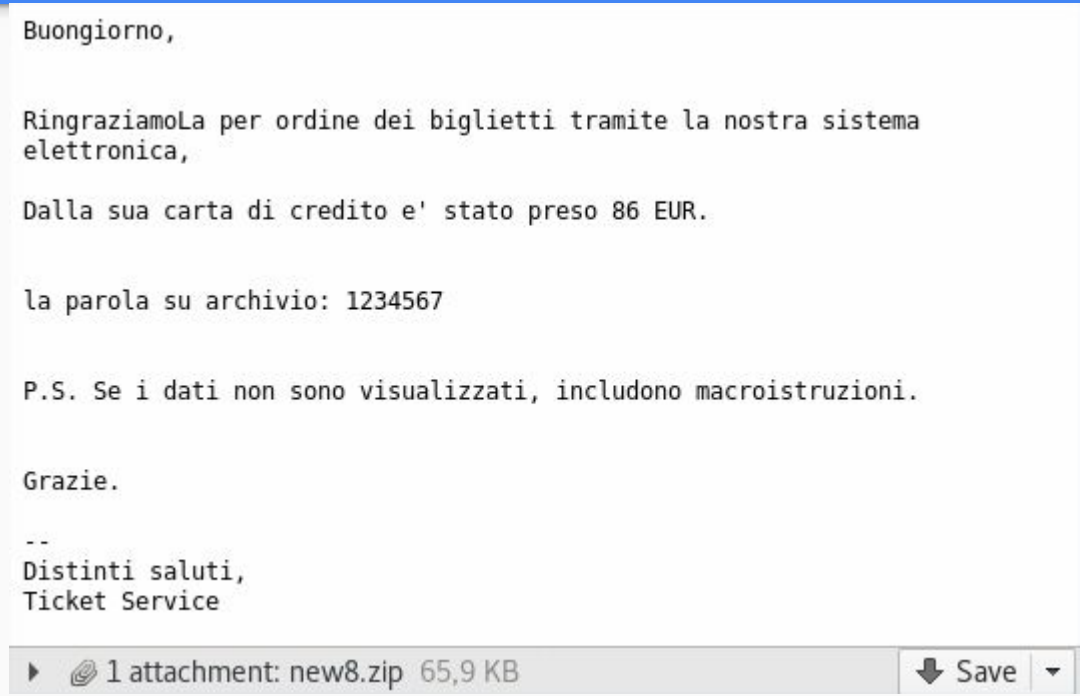
Link - URL shortener

Allegati

Italiano stentato

Password semplice

Non è spam



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

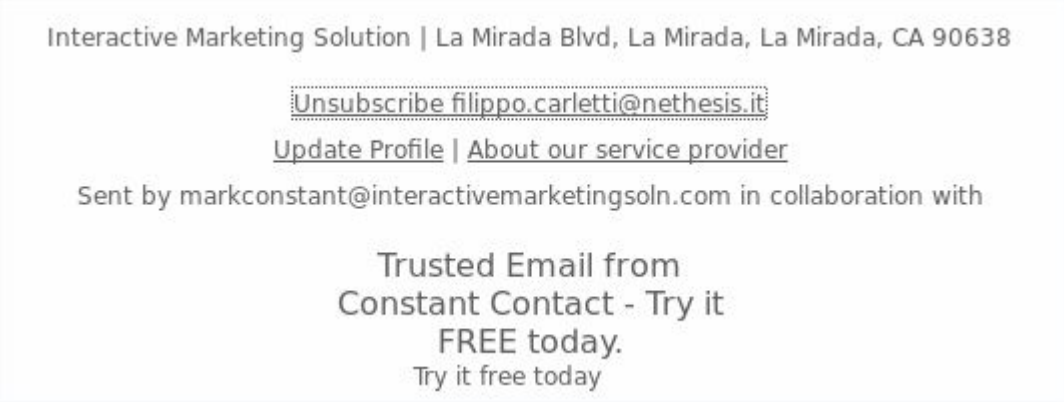
Firme AV apposite

PhishTank

Spam

Pubblicità indesiderata (spedizione costa poco)

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



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