

Norme di igiene informatica

Roberto Cecchini

Roma, 23 Novembre 2017

Pericoli informatici



A chi fa gola il vostro pc?

- Hacker
- spammer
- virus / worm
- il vostro PC, se non opportunamente protetto e senza le ultime versioni del software installato (e anche con queste...), può essere facilmente compromesso (con, o anche senza, il vostro aiuto attivo).

... e perché?

- untore
- spam
- attacchi DDoS (Distributed Denial of Service)
- testa di ponte per altri attacchi
- deposito di materiale illegale
- cava di password
- recupero informazioni personali

Virus

- Un **virus** è un codice in grado di riprodursi attaccandosi ad un altro programma (o documento), in modo che venga eseguito ogni volta che lo sia il programma infettato.
 - Si propaga trasportato dal programma infetto
 - internet, cd rom, penna usb, floppy...
 - Di solito, ha bisogno di una qualche azione da parte dell'utente.

Worm

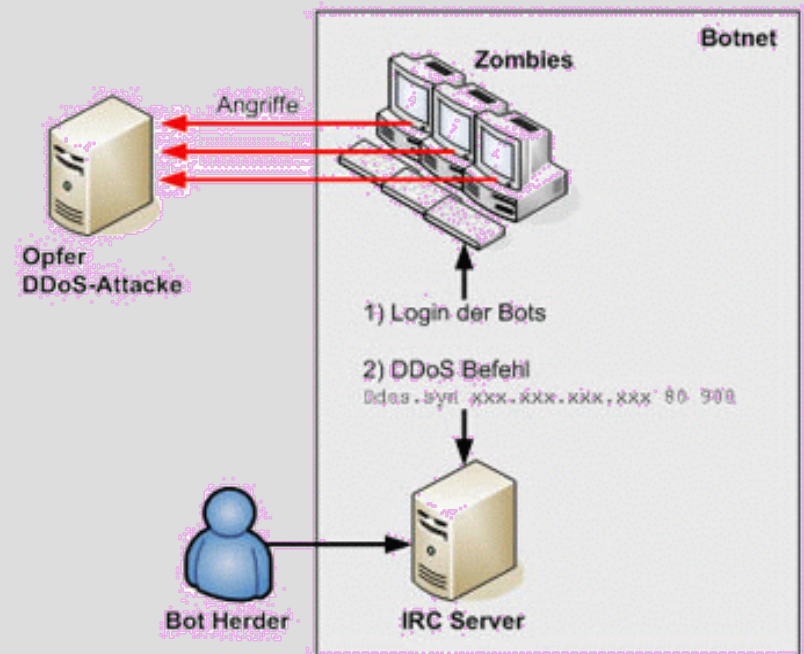
- Un **worm** è un eseguibile in grado di creare copie di sé stesso, senza infettare altri programmi (come fanno i virus).
 - Si propaga via posta elettronica o sfruttando difetti dei programmi installati.
 - Non necessita di azioni da parte dell'utente (a parte la trascuratezza ...).

Virus & worm

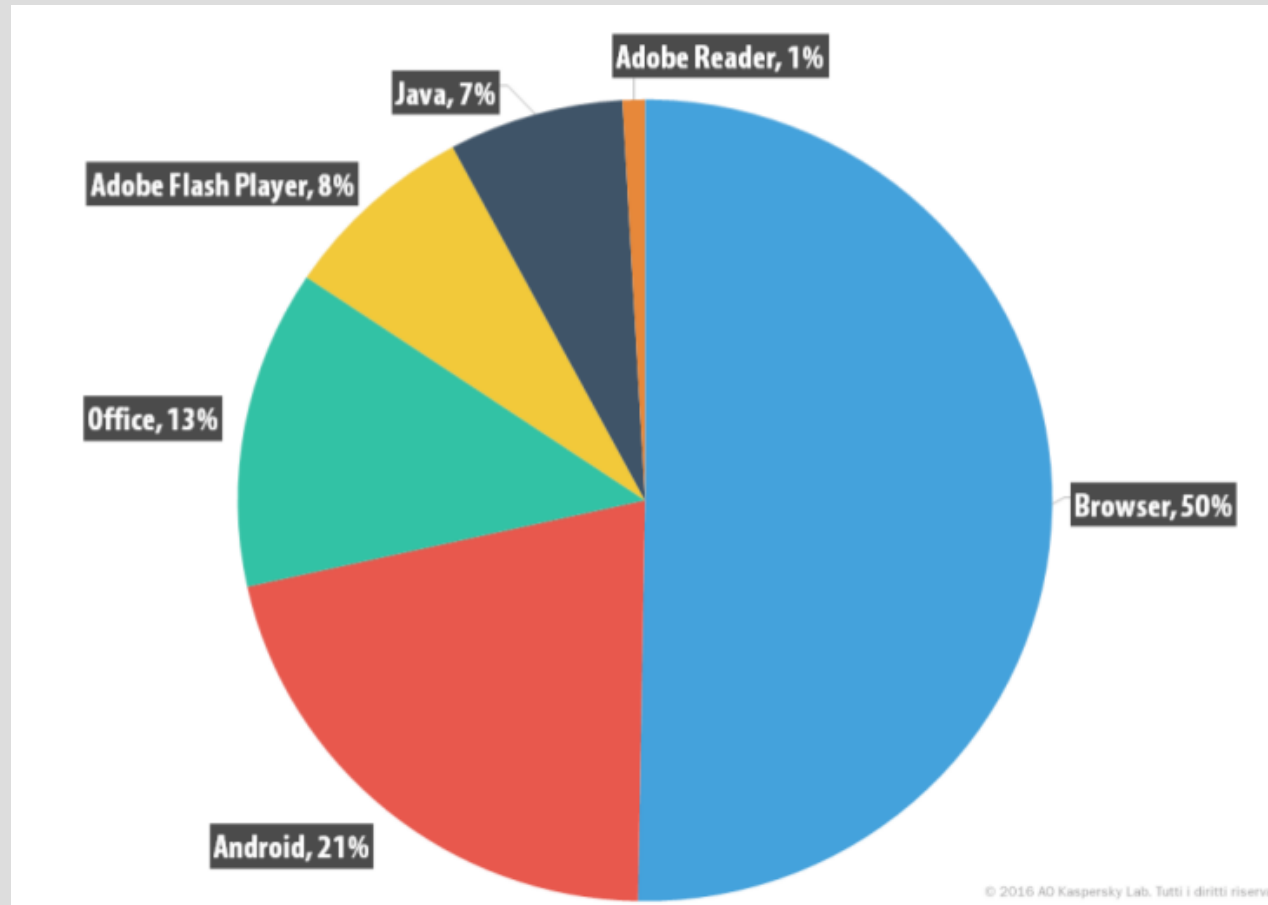
- Virus e worm, oltre a propagarsi, possono compiere un'infinità di altre azioni nocive:
 - cancellare file;
 - diffondere informazioni riservate (compresi i vostri mail privati ...);
 - permettere ad intrusi di accedere alla vostra macchina;
 - spedire mail di spam
 - ...

Botnet

- Una rete di software robot
 - installati su macchine compromesse
 - comandate remotamente
 - utilizzate per scopi criminali: spam, **attacchi DOS**.
- Le macchine facenti parte di una botnet sono stimate intorno ai **10 milioni**



Metodi di attacco



Kasperski, Security Bulletin 2016

Spam

- Un messaggio non richiesto
 - a carattere pubblicitario
 - truffe
 - nigeriana, amico in difficoltà, ecc. ecc.
- oltre il 50% degli email inviati!



Spyware

- Inseriti in altri programmi (ad es. client p2p, salvaschermo, sfondi), inviano informazioni sulle attività dell'utente
 - molti Internet Explorer toolbar add-on o finti anti-spyware
 - attenzione durante l'installazione di programmi quando vi viene chiesto se volete altre funzionalità

Phishing

- Un tentativo di carpire informazioni riservate e sensibili quali password o credenziali bancarie
- Un attacco di phishing inizia con l'invio di una mail che contiene un'offerta allettante o richiede un'azione quale:
 - compilare un modulo (ad es. cambio password)
 - cliccare su un link che conduce ad un sito fasullo
 - aprire un allegato infetto (ad es. uno zip che dovrebbe contenere una fattura).

Phishing

- Secondo Verizon è alla base del 90% degli incidenti di sicurezza
- La creazione di siti di phishing al momento è stimata intorno a 1,4 milioni al mese
- Molto difficili da filtrare

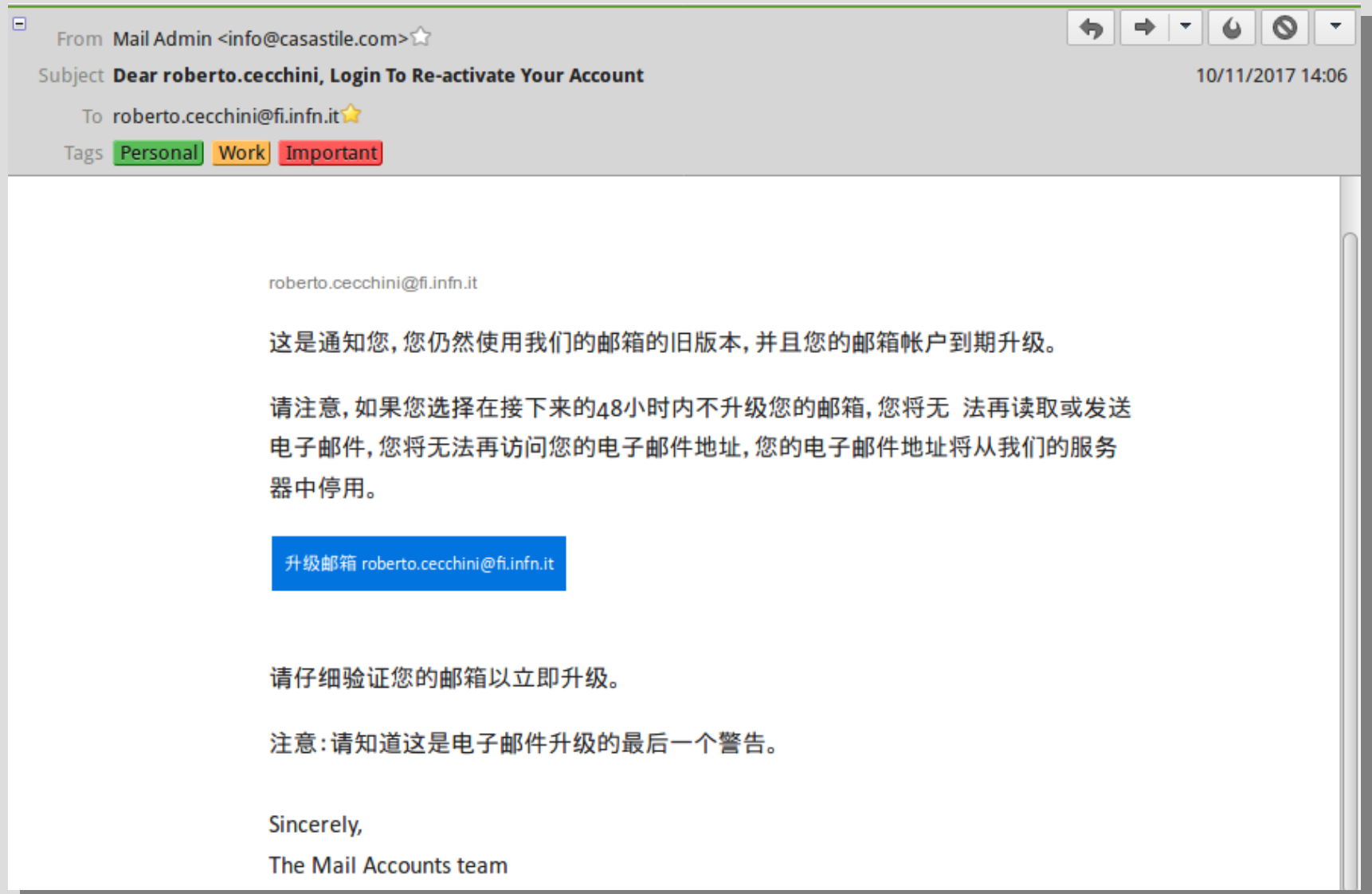
Phishing?

- Link non corrispondente a quello visualizzato
- Analizzare il dominio a cui si chiede di accedere: ad esempio `login.bancaintesa.web.com/credenziali`
- Messaggio sgrammaticato o in inglese
- Richiesta di azioni urgenti
- Richiesta di informazioni personali. Diffidate di messaggi in cui vi si chiede di accedere al sito per motivi di “aggiornamento” o “operazioni da confermare”.
- Offerte molto interessanti
- Richiesta di soldi
- Agenzia governativa: Equitalia, Agenzia delle Entrate e tutte le altre
- Richieste dal Servizio Calcolo (casella postale piena, account in scadenza, ecc. ecc.)

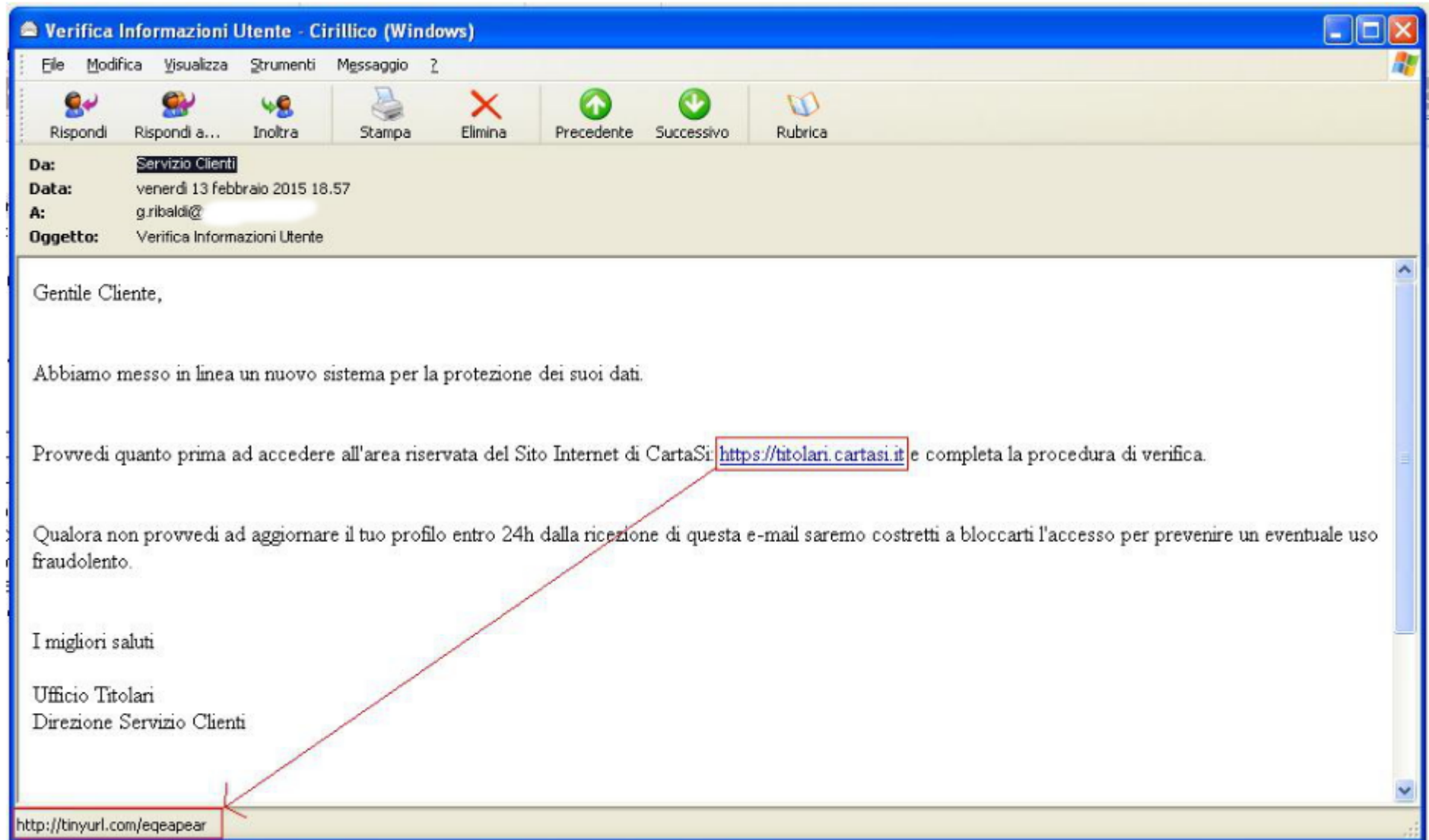
Protegetevi!

- Non rispondete mai a richieste di password, codici di sicurezza, PIN ecc.
- Fate molta attenzione agli allegati
- Elementi sospetti
 - email che sollecitano azioni urgenti.
 - email con formule generiche quali “Caro cliente” o “Gentile Signora/Egregio Signore”.
 - email con errori di grammatica o ortografia.
- Se c'è un link, fateci passare sopra il puntatore e controllate la vera destinazione che apparirà nella barra degli indirizzi.

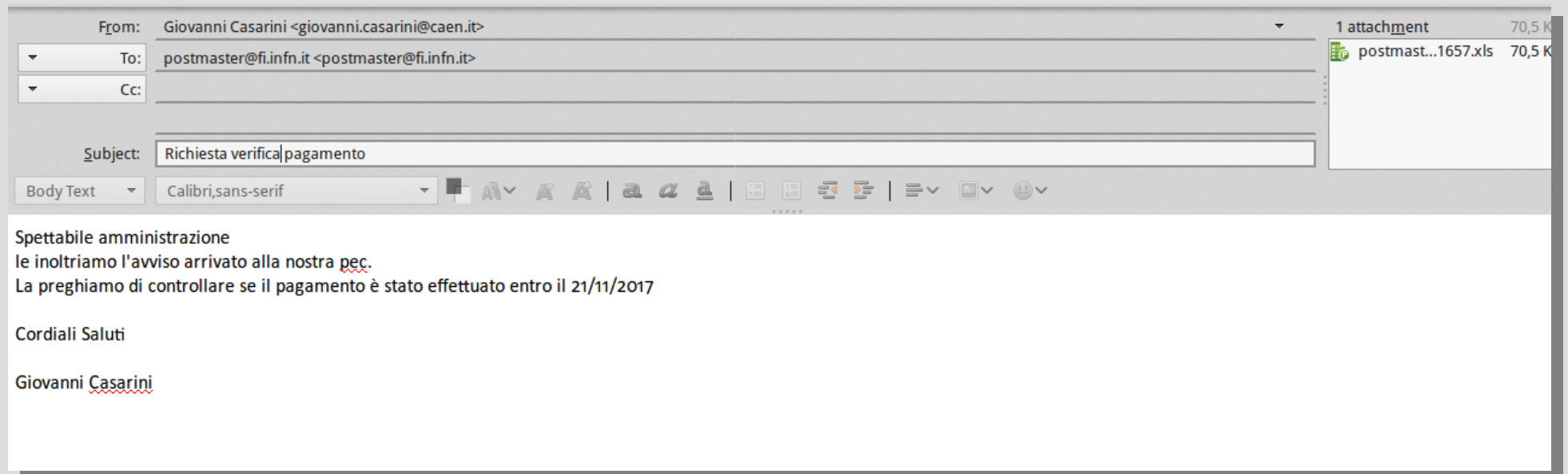
Phishing: esempio 1



Phishing: esempio 2



Phishing: esempio 2



Phishing: esempio 2 (segue)



17 / 37

17 engines detected this file

SHA-256 6f03603b7718410b32b09eb40c38ea6b063b6385abc78fbb4a077b1328277b88
File name domi-1820.xls
File size 70.5 KB
Last analysis 2017-11-22 07:41:14 UTC
Community score -78

Detection

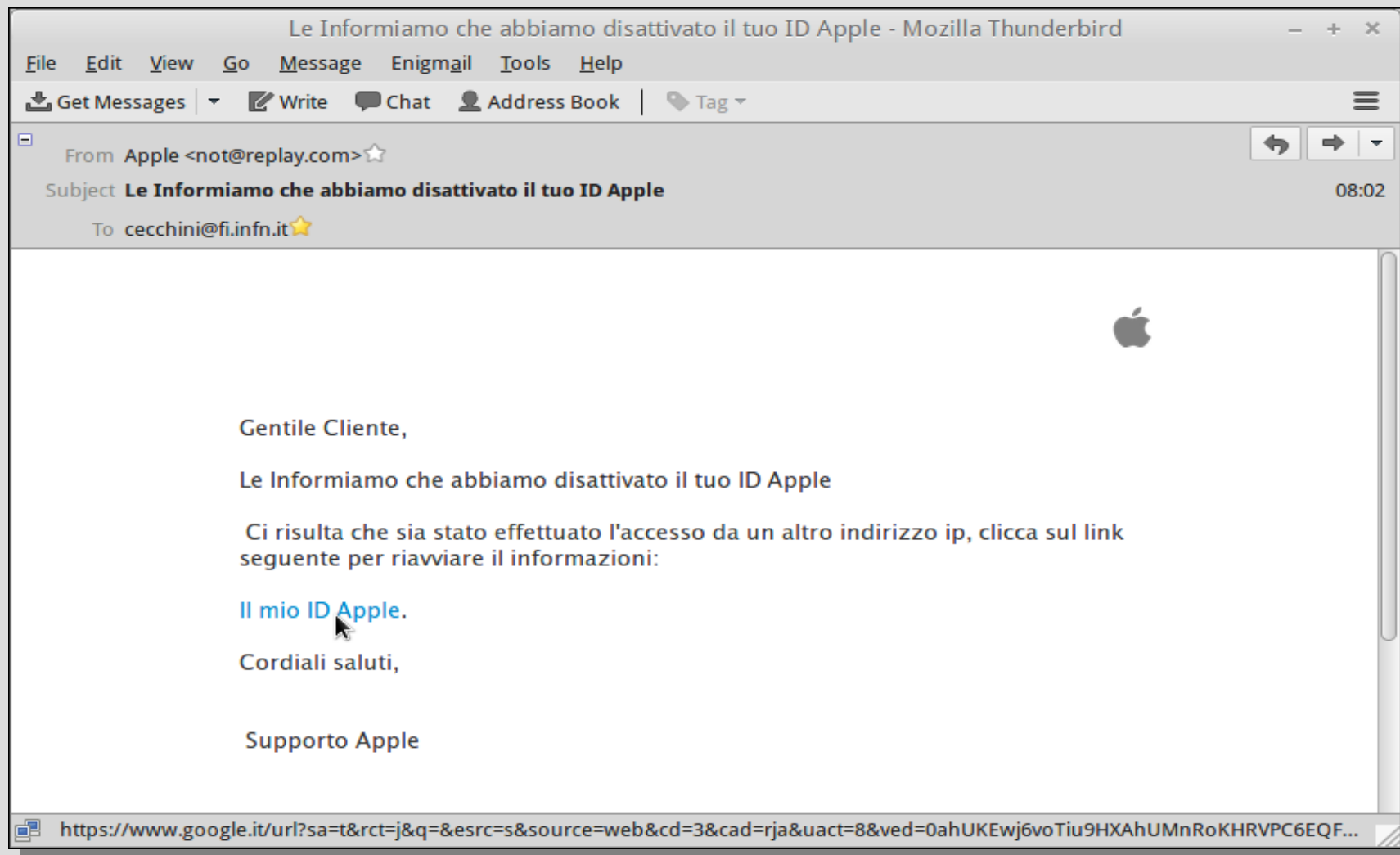
Details

Relations

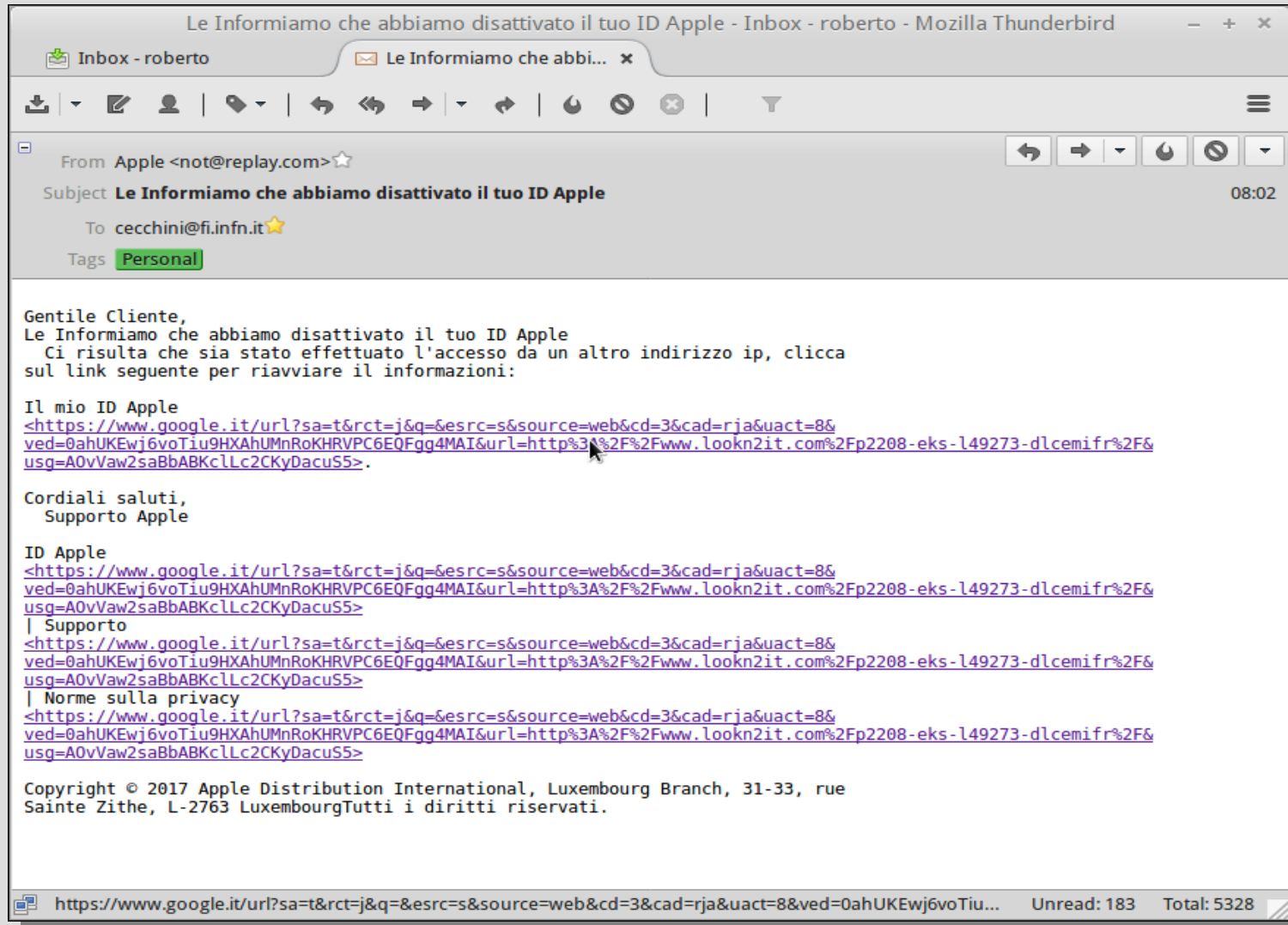
Community 3

Ad-Aware	VB:Trojan.VBA.Downloader.HT	Arcabit	VB:Trojan.VBA.Downloader.HT
BitDefender	VB:Trojan.VBA.Downloader.HT	ClamAV	Doc.Dropper.Agent-6380017-0
Cyren	X97M/Agent.gen	DrWeb	W97M.DownLoader.2222
Emsisoft	VB:Trojan.VBA.Downloader.HT (B)	eScan	VB:Trojan.VBA.Downloader.HT
ESET-NOD32	VBA/TrojanDownloader.Agent.FKY	Fortinet	VBA/Agent.EZM!tr.dldr
Ikarus	Trojan-Downloader.VBA.Agent	MAX	malware (ai score=89)
NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druvzi	Qihoo-360	virus.office.qexvmc.1085
Symantec	Trojan.Mdropper	Tencent	Win32.Trojan-downloader.Agent.Anps
ZoneAlarm	HEUR:Trojan.Script.Agent.gen	AhnLab-V3	Clean
ALYac	Clean	Antiy-AVL	Clean

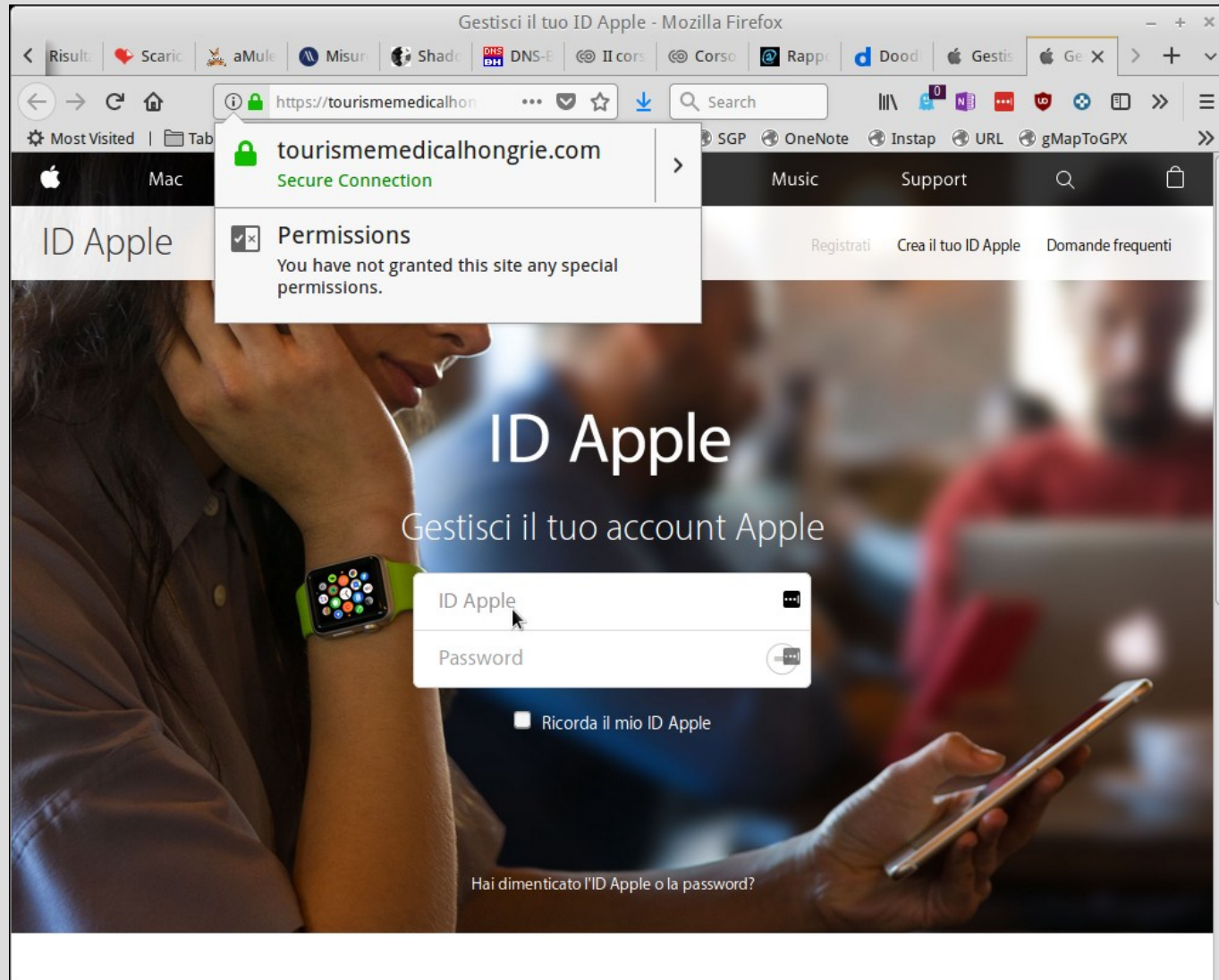
Phishing: esempio 3



Phishing: esempio 3 (segue)



Phishing: esempio 3 (segue)



Le “bufale” (Hoax)

- Non sono un'invenzione recente, ma internet le rende particolarmente pericolose.
- Notizie false:
 - aumentano le e-mail inutili in circolazione;
 - diffondono indirizzi di e-mail;
 - effetti simili a quelli di un virus.
- Frasi tipiche:
 - “Nuovo virus pericolosissimo”;
 - “Notizia proveniente da Microsoft/IBM”;
 - “Bambina/o in fin di vita”;
 - “Diffondete la notizia quanto più possibile”.

Le “bufale” (Hoax) **segue**

- Prima di ridiffondere la notizia, controllatene l'autenticità:
 - CICAP, bufalopedia, ecc. ecc.
- Anche se la notizia è vera (anche se per una nobile causa) valutate attentamente l'opportunità della sua diffusione via la rete GARR.
- **In ogni caso, mettete i destinatari in BCC:**

Misure elementari di sicurezza



Autenticazione: password

- **Personale e non cedibile**
- Di buona “qualità”
- Da proteggere con la massima cura
- Da non conservare in chiaro
- Da cambiare periodicamente

Pwd manager (p.e. LastPass)

The screenshot shows a Mozilla Firefox browser window with the URL `dp.infn.it/module.php/wawa/login.php/plain/?StateId=_7bbdabcd35282580f49d`. The page title is "INFN Identity Check - Mozilla Firefox". The browser's address bar shows "il sentiero del west". The browser's tab bar contains several tabs, including "Identiti...", "Pubblicate ir...", "ixi DNS Respon...", "Using Doma...", "DNS DNS-BH - M...", "Misure mini...", "Misure mini...", and "Il Respons...".

The main content of the page is the "INFN Identity Check" login form. It features the INFN CCR - AAI logo on the left. The form has two input fields: "Username" with the value "rcecchin" and "Password" with masked characters ".....". Below the fields is a large orange "LOGIN" button. To the right of the login form, there are two blue boxes for alternative login methods: "X.509 Cert" and "Kerberos5 G". Each box has a sub-label "Accesso tramite c..." and an orange "ACCEDI" button. Below the login form, there are links for "How to obtain an account for INFN-AAI" and "Change or Reset Password - Retrieve Username". At the bottom of the page, a red warning message reads: "DO NOT BOOKMARK THIS PAGE! After login you will be redirected to".

Overlaid on the right side of the browser window is the LastPass vault interface. It features a search bar at the top with the text "Search LastPass Vault". Below the search bar is a list of vault items: "Open my Vault", "Sites", "Secure Notes", "Form Fills", "Generate Secure Password", "Show Matching Sites" (with a red "48" badge), "Recently Used", "More options", "Preferences", and "Help". At the bottom of the vault interface, there is a "Log Out: zlbaldino@gmail.com" button.

Salvaschermo

Attivate il salvaschermo con password per evitare che possano impersonarvi in vostra assenza.

Dal Disciplinare:

... non devono mantenere connessioni remote inutilizzate né lasciare la postazione di lavoro con connessioni aperte non protette

Antivirus

- È **obbligatorio** installare un antivirus
 - Il Servizio di Calcolo dispone di software e licenze e può prestare consulenza al riguardo
- In ogni caso:
 - non aprite allegati di e-mail di cui non siete sicuri, **anche se il mittente è una persona di cui vi fidate**;
 - ricordate che il campo From: è **attendibile solo se il mail è firmato digitalmente**
 - usate solo programmi provenienti da fonti fidate

Crittografia

- I dati (mail, file, database, cartelle) possono venire cifrati:
 - “impossibili” da capire tranne che per i possessori della chiave di cifratura;
 - la chiave può essere di tipo hardware (ad es. smart card) o software (password);
 - se la chiave viene persa, i dati sono irrecuperabili.

Posta: firmare e cifrare

- Un messaggio “firmato” garantisce l'identità del mittente
 - tutti possono firmare i propri messaggi (dopo aver ottenuto un certificato digitale)
- Un messaggio cifrato impedisce la lettura a chi non è tra i destinatari
 - è necessario che anche i riceventi abbiano un certificato digitale
- I certificati digitali sono disponibili per chiunque abbia un account AAI INFN

Posta firmata

The screenshot shows an email client interface. At the top, there is a list of four emails, each with a star icon and the subject 'Re: [mailmgr] SPF per indirizzi infn.it'. The dates and sizes are: 21/02/... 14, ..., 21/02/... 15, ..., 20/02/... 14, ..., and 20/02/... 30, ...

The selected email is from Luca Carbone <luca.carbone@mib.infn.it> with the subject 'Re: [mailmgr] Configurazione sendmail x cert TCS'. It was sent on 09/10/2017 at 09:25. The email is marked as read with a red dot on the envelope icon, which is circled in red. The email content is as follows:

From Luca Carbone <luca.carbone@mib.infn.it>★
Subject **Re: [mailmgr] Configurazione sendmail x cert TCS**
Reply to mailmgr@lists.infn.it★, Luca Carbone <luca.carbone@mib.infn.it>★
To Stefano Bagnasco <bagnasco@to.infn.it>★, mailmgr@lists.infn.it★

Considera che nel Subject dei certificati personali Digicert:
C=IT, ST=Rome, L=Frascati, O=Istituto Nazionale di Fisica Nucleare, CN=Luca Giovanni Carbone

In ogni caso...

- Il Servizio Calcolo, anche se spesso non ha risorse sufficienti, va comunque sempre interpellato.
- Il System Manager è il vostro miglior amico!



Domande?

