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

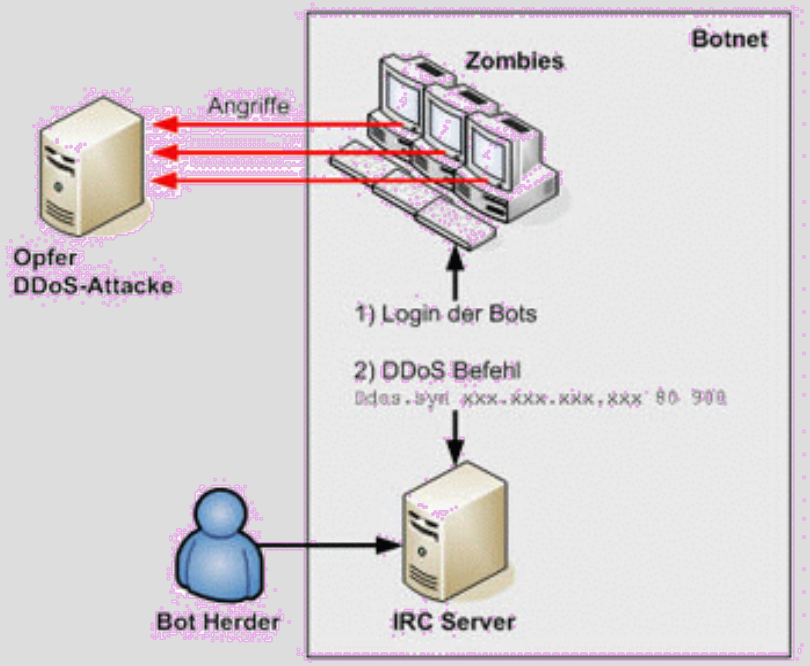
- Un **worm** è un eseguibile in grado di creare copie di sé stesso, senza infettare altri programmi (come fanno i virus).
  - Si propaga via posta elettronica o sfruttando difetti dei programmi installati.
  - Non necessita di azioni da parte dell'utente (a parte la trascuratezza …).

Virus & worm

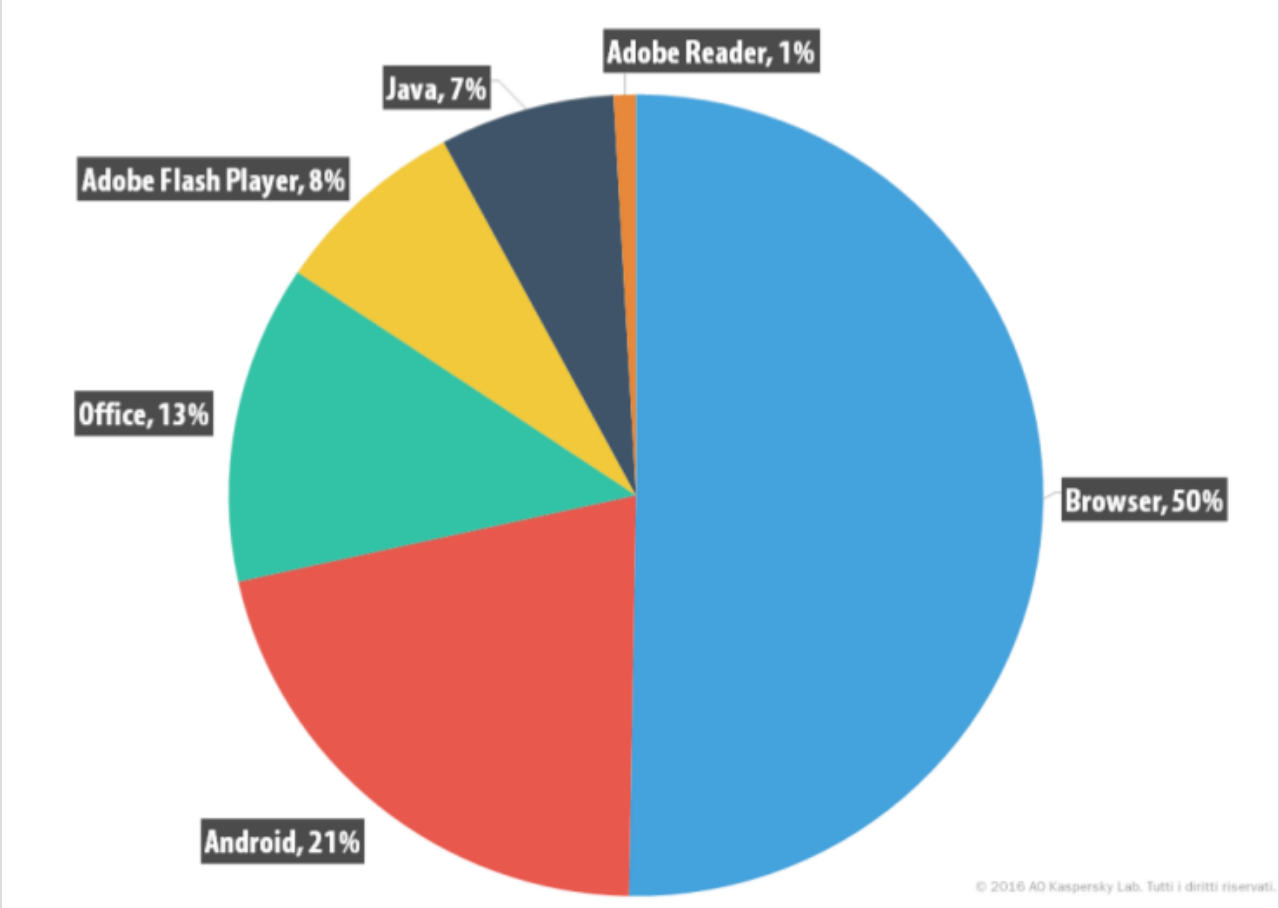
- Virus e worm, oltre a propagarsi, possono compiere un'infinità di altre azioni nocive:
  - cancellare file;
  - diffondere informazioni riservate (compresi i vostri mail privati …);
  - permettere ad intrusi di accedere alla vostra macchina;
  - spedire mail di spam
  - …

Botnet

- Una rete di software ro**bot**
  - 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 phising al momento è stimata intorno a 1,4 milioni al mese
- Molto difficili da filtrare

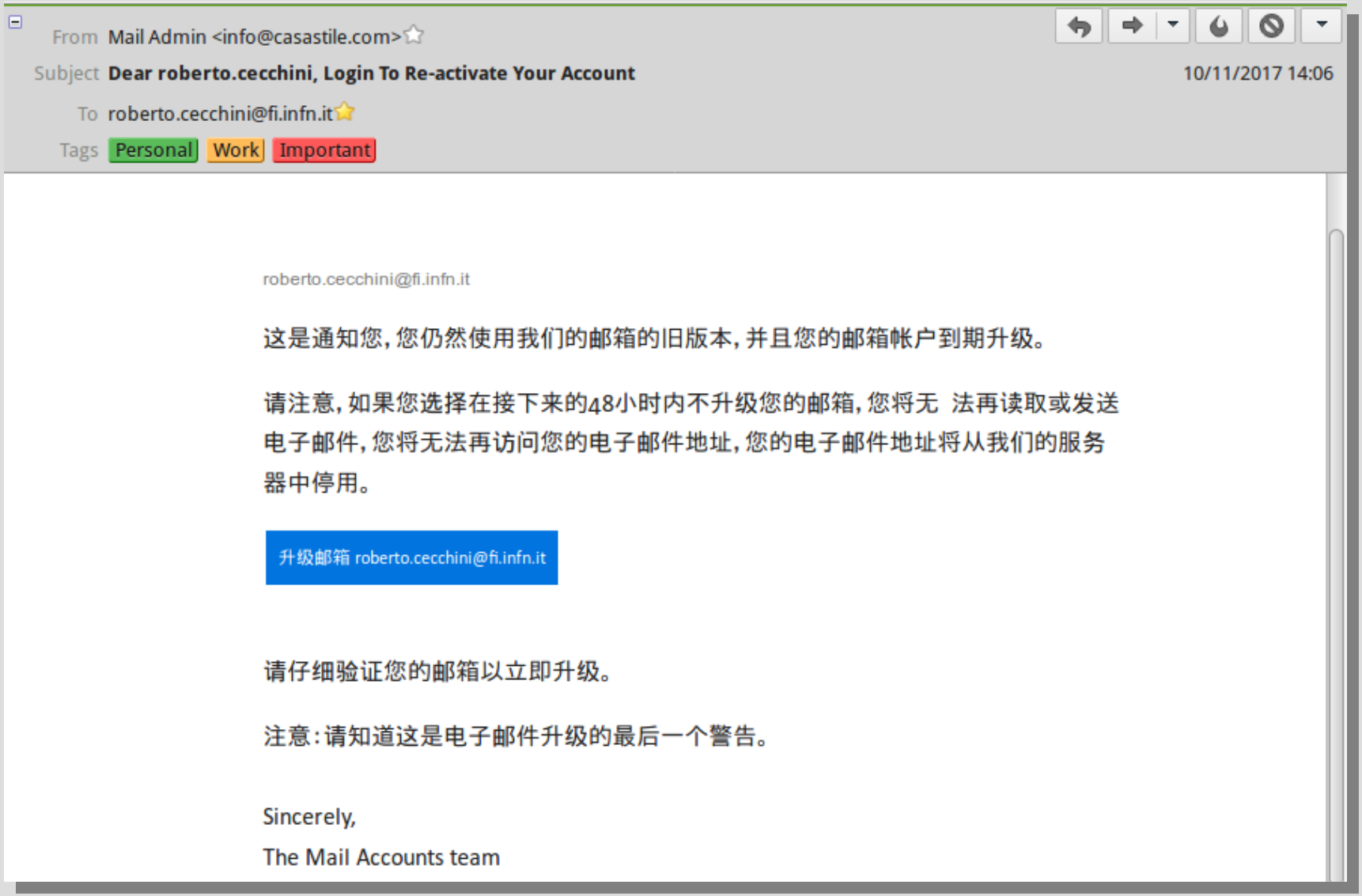
Phishing?

- 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.)

Proteggetevi!

- 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



From Mail Admin <info@casastile.com>

Subject **Dear roberto.cecchini, Login To Re-activate Your Account** 10/11/2017 14:06

To roberto.cecchini@fi.infn.it

Tags Personal Work Important

roberto.cecchini@fi.infn.it

这是通知您，您仍然使用我们的邮箱的旧版本，并且您的邮箱帐户到期升级。

请注意，如果您选择在接下来的48小时内不升级您的邮箱，您将无 法再读取或发送电子邮件，您将无法再访问您的电子邮件地址，您的电子邮件地址将从我们的服务器中停用。

升级邮箱 roberto.cecchini@fi.infn.it

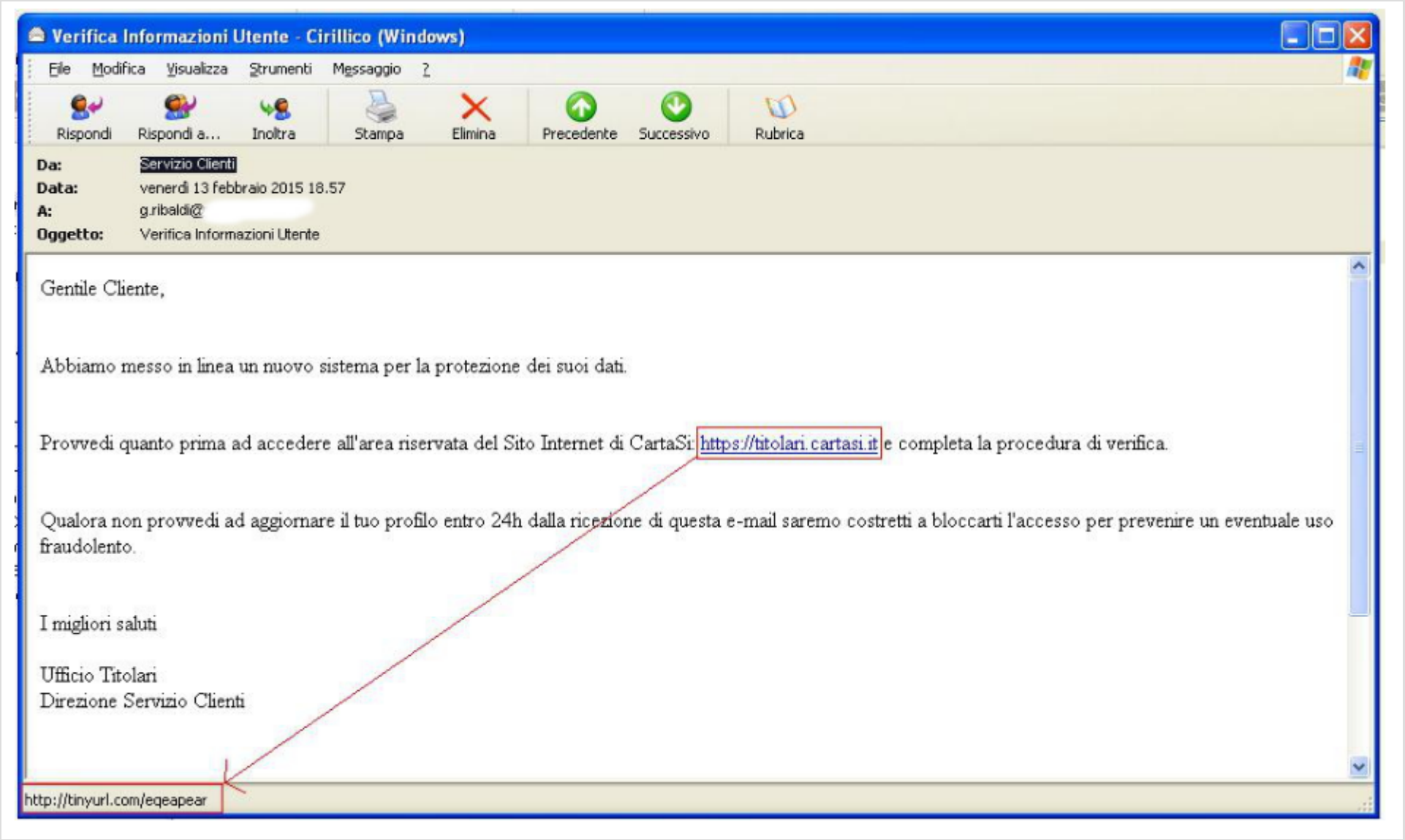
请仔细验证您的邮箱以立即升级。

注意：请知道这是电子邮件升级的最后一个警告。

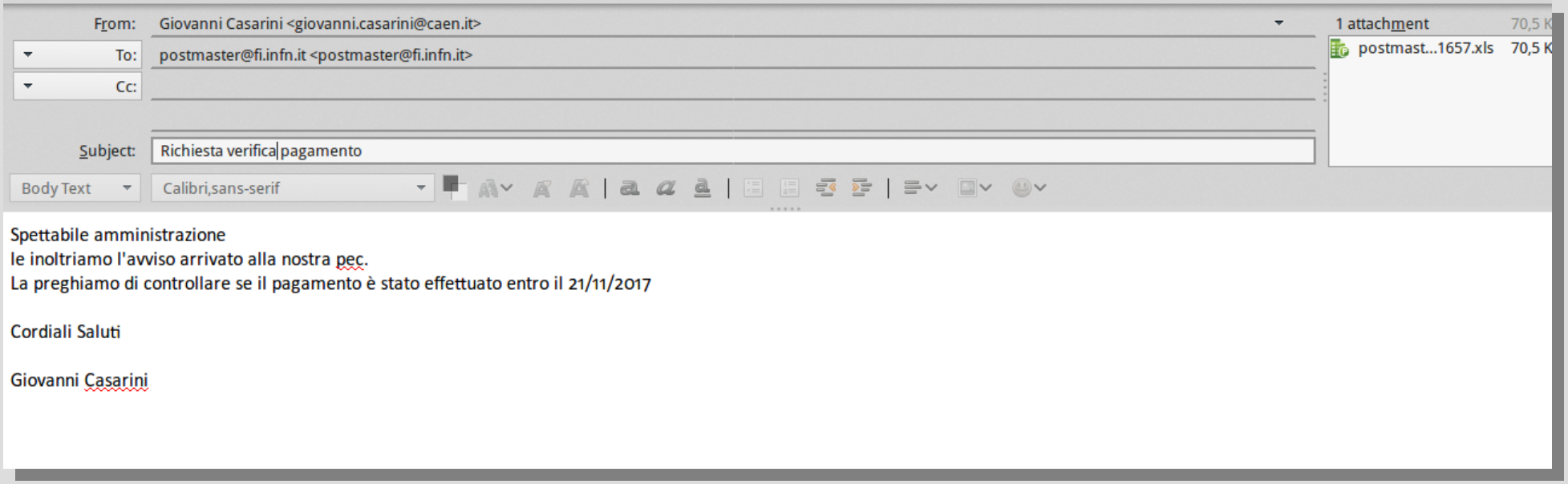
Sincerely,

The Mail Accounts team

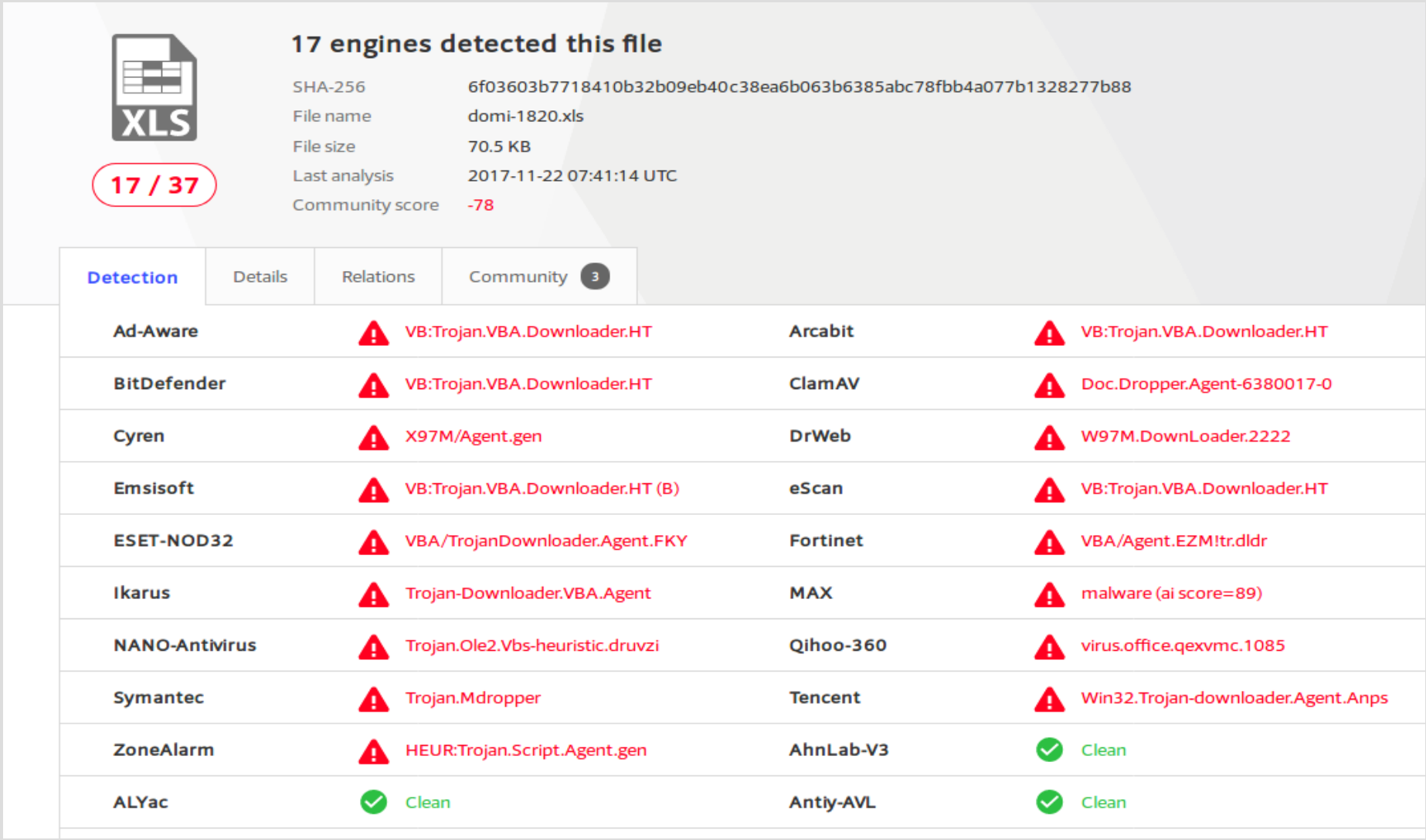
Phishing: esempio 2



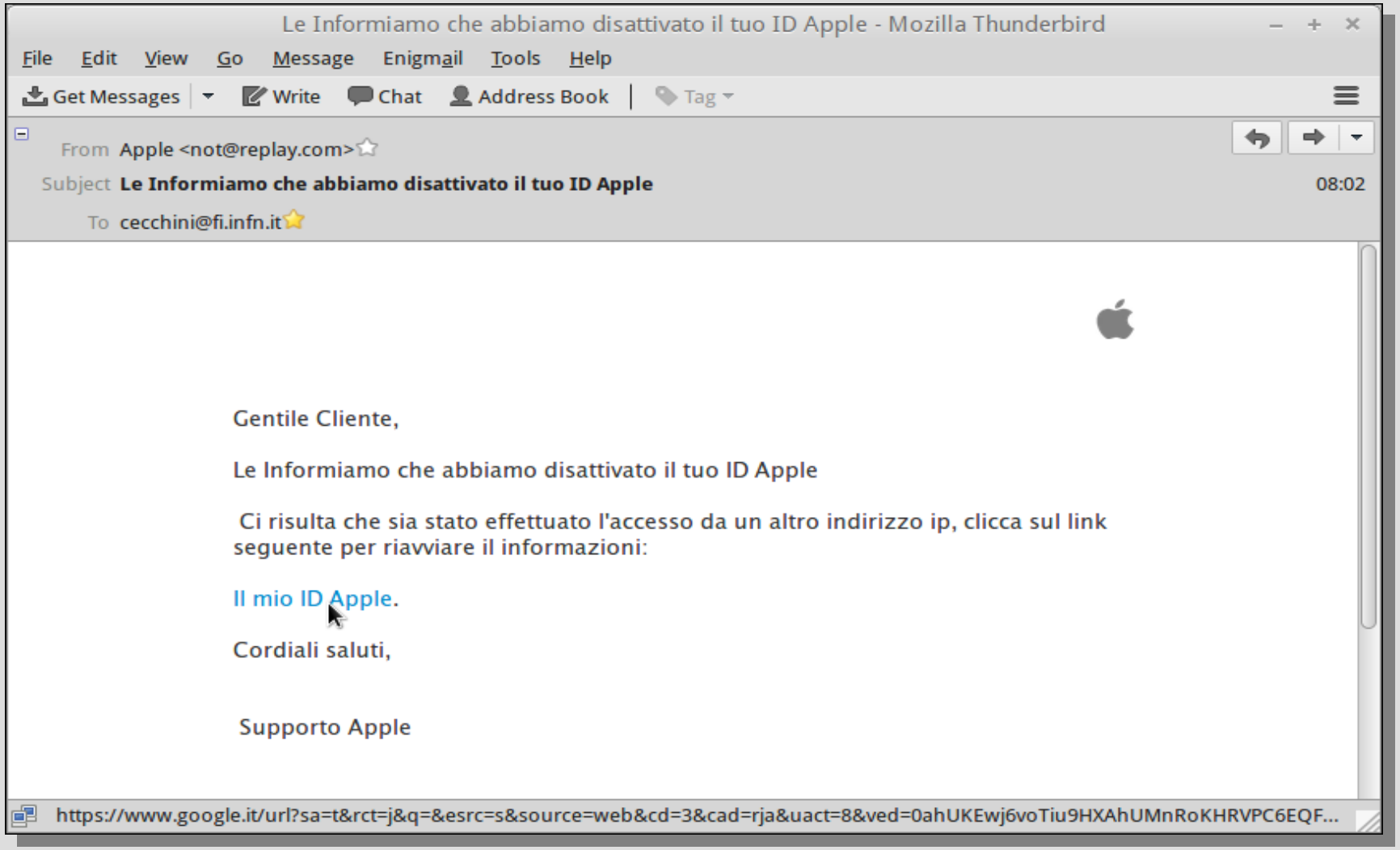
Phishing: esempio 2



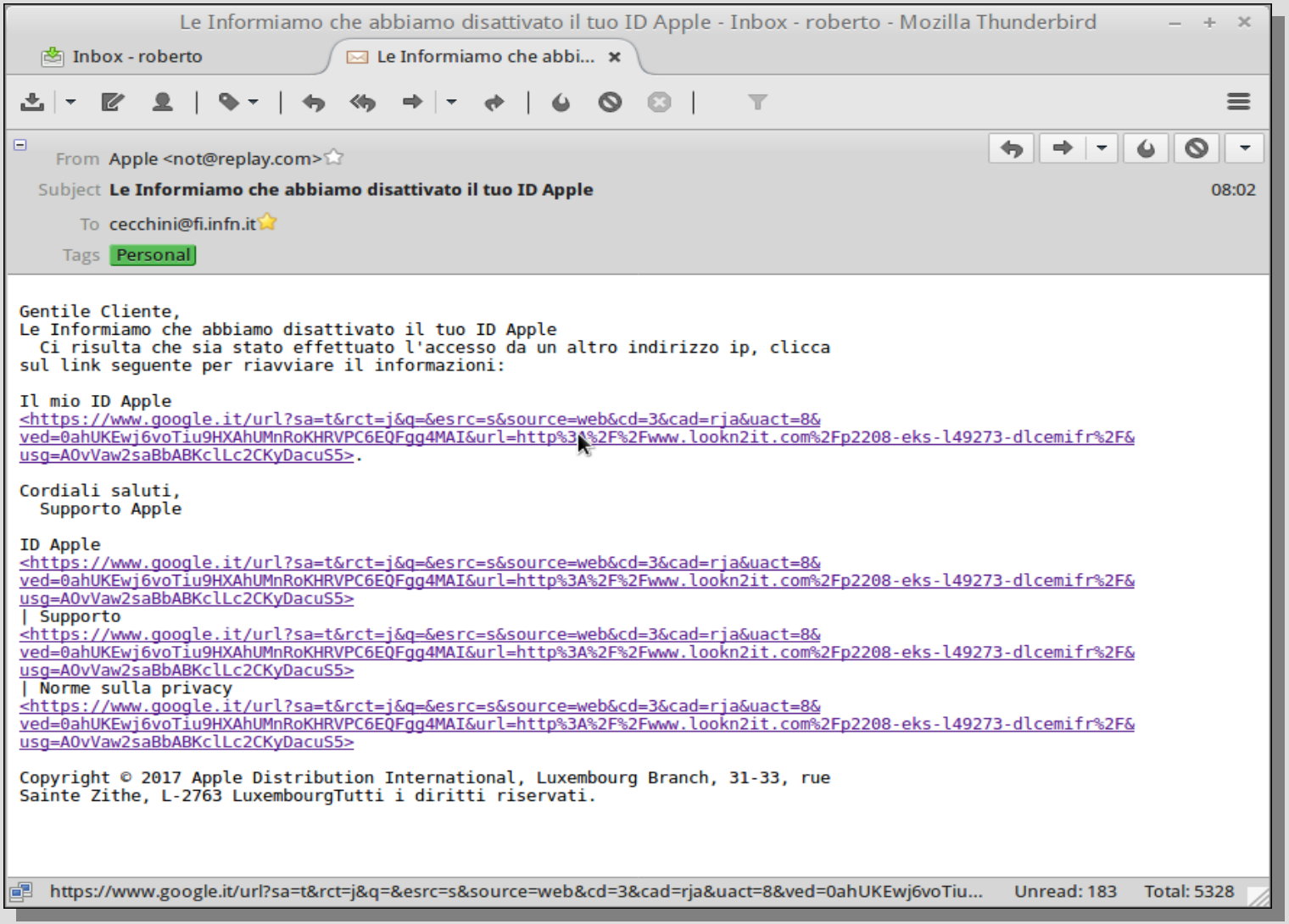
Phising: esempio 2 (segue)



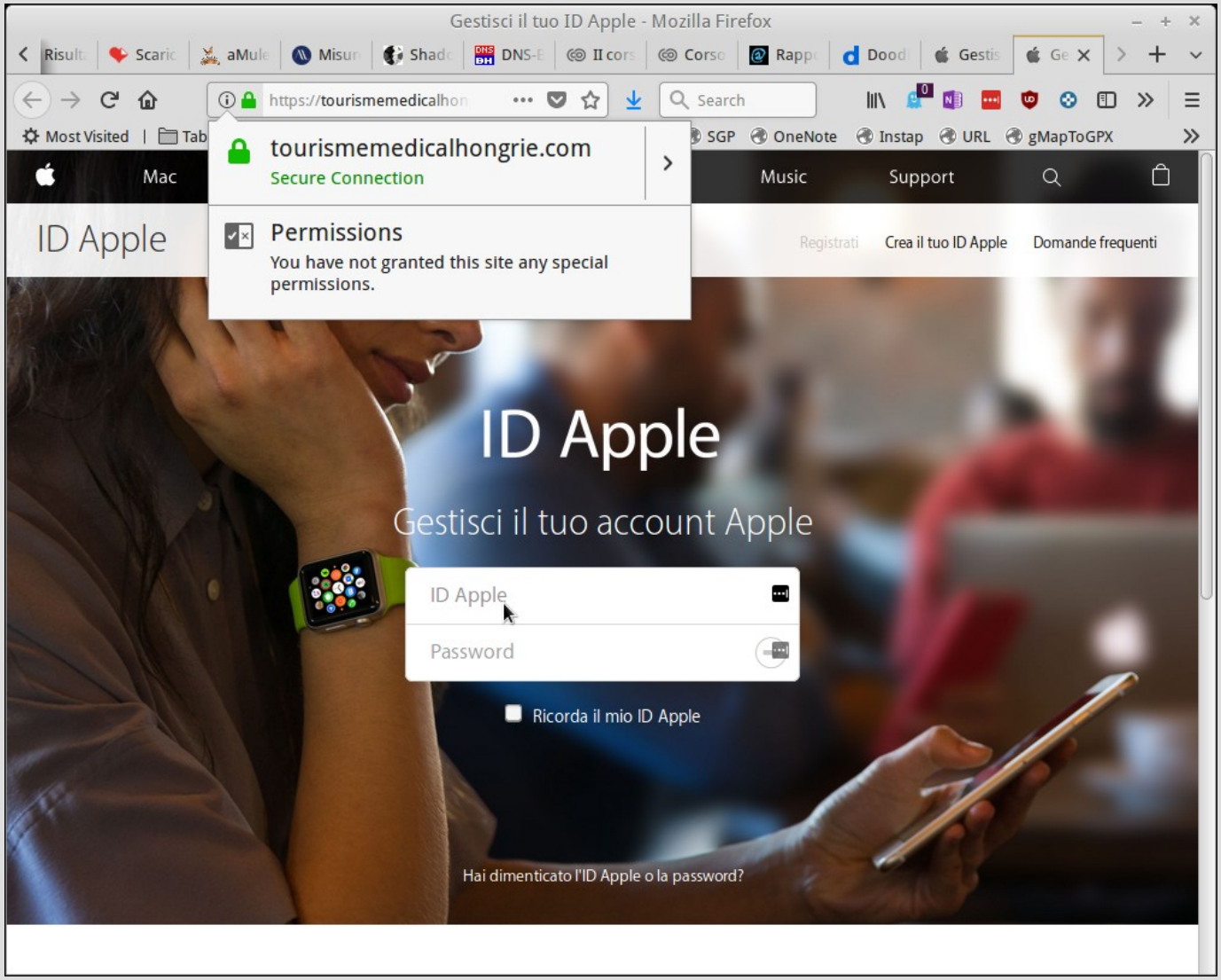
Phishing: esempio 3



Phishing: esempio 3 (segue)



Phishing: esempio 3 (segue)



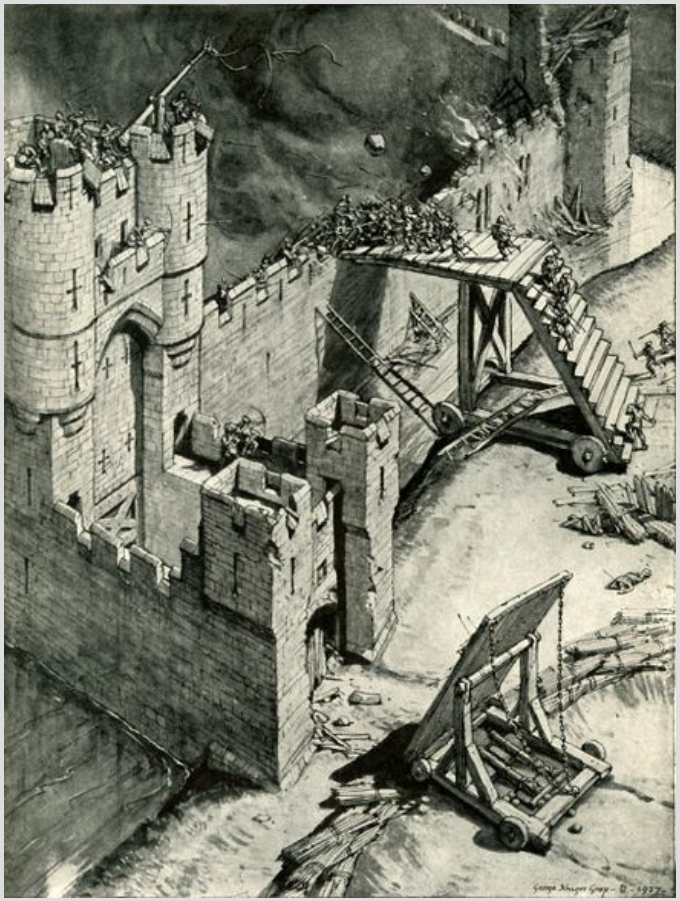
Le “bufale” (Hoax)

- 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:**

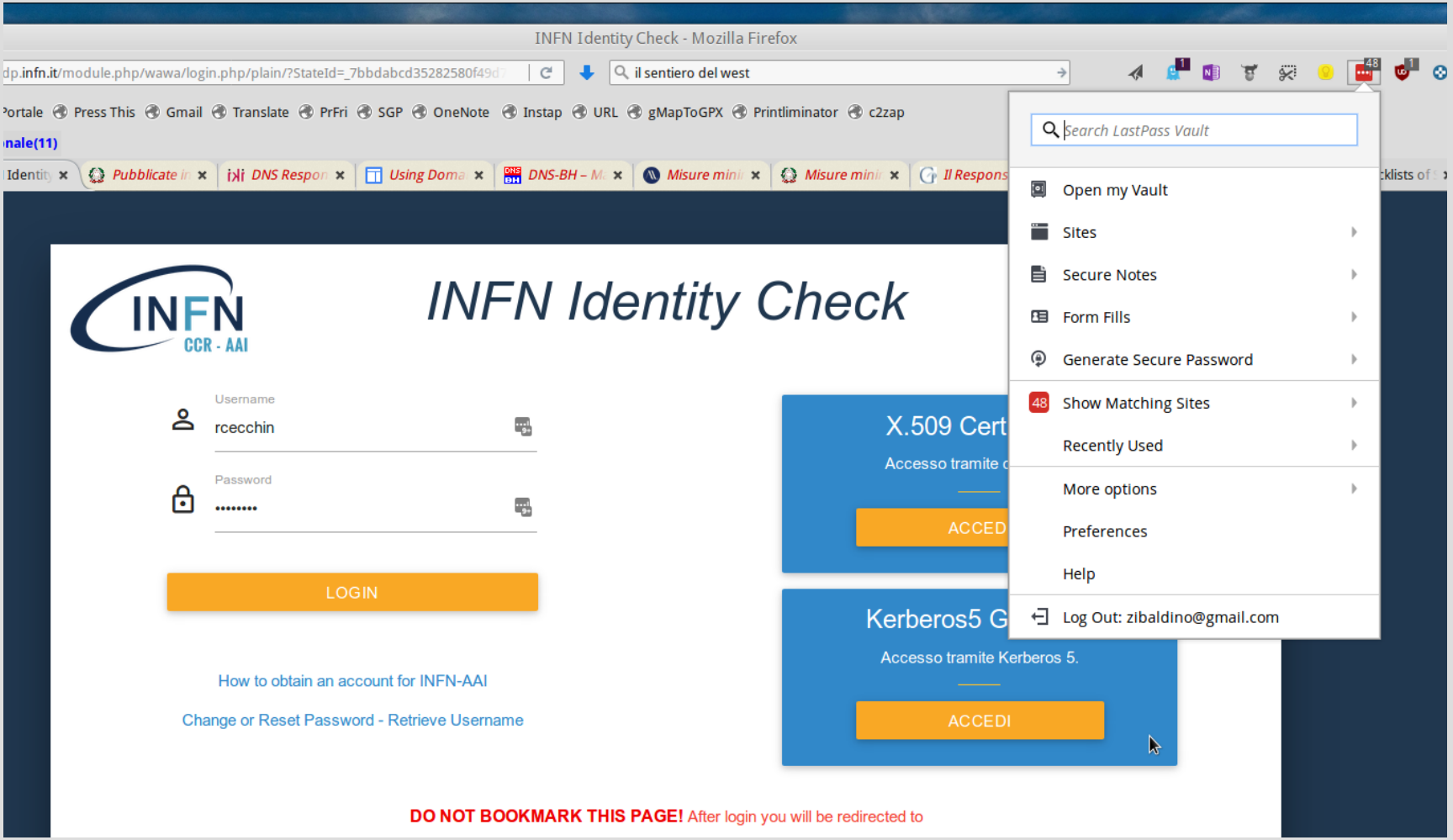
Misure elementari di sicurezza



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)



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

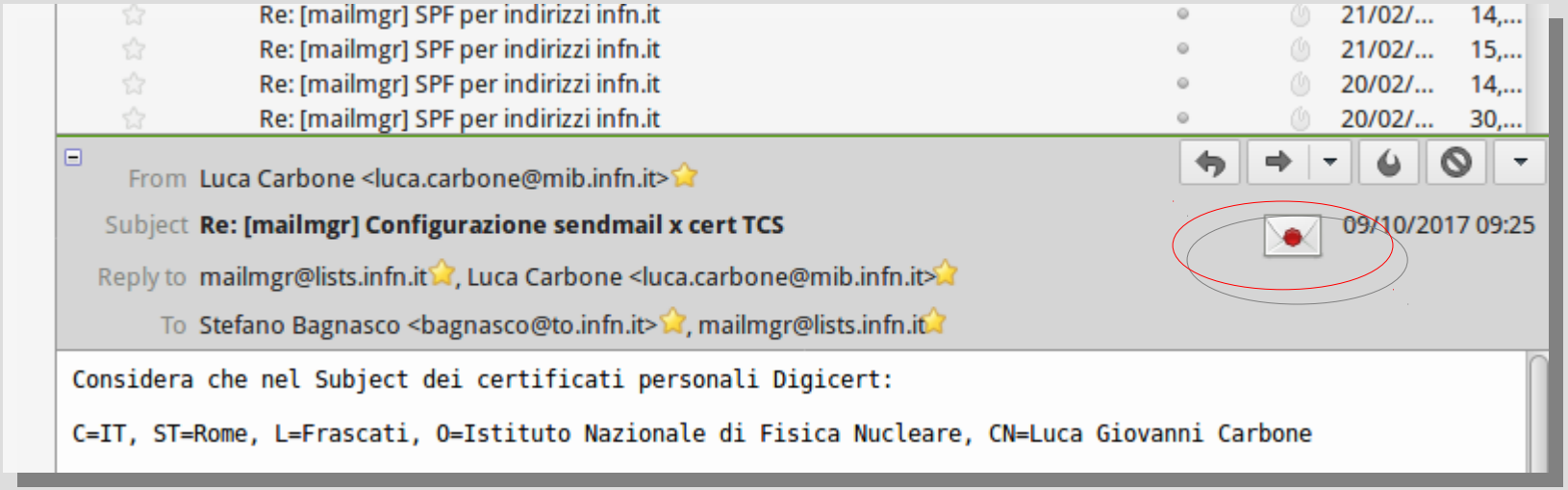
Crittografia

- 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



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?