White Paper

Come riconoscere le email pericolose

INTRODUZIONE 2

RICONOSCERE AL VOLO UNA EMAIL DI PHISHING 3

Caratteristiche di una email di Phishing 4

RICONOSCERE AL VOLO UNA EMAIL DI SPEAR PHISHING 5

Caratteristiche di una email di Spear Phishing 6

EMAIL CHE CONTENGONO CRIPTO-VIRUS O ALTRO MALWARE 8

ANALIZZARE L'HEADER DI UN MESSAGGIO 10

CONCLUSIONI 11

INTRODUZIONE

L'attuale e continua proliferazione di uno strumento come i social media, diventato ormai imprescindibile anche in ambito business, ha sicuramente modificato il modo di comunicare di ognuno di noi, nella vita quotidiana ma anche nel lavoro.

Se pensiamo che fino a qualche anno fa lo strumento più veloce da poter usare era il fax, mentre oggi con un click ognuno di noi è in grado di diffondere a macchia d'olio qualsiasi tipo di informazione, ci rendiamo conto della portata del cambiamento.

Nonostante la tecnologia continui a progredire a un ritmo sorprendente e la velocità media delle connessioni a Internet aumenti di giorno in giorno, sai qual è **lo strumento che viene maggiormente utilizzato per comunicare in ambito business? L'email**.

A questo punto ti verrà da pensare che sia solo una questione di tempo prima che la posta elettronica lasci il posto a uno strumento più moderno.

Ma la realtà è che secondo recenti studi svolti da **Radicati Research** è previsto un ulteriore aumento del numero utenti di posta elettronica in tutto il mondo che nel 2022 ammonterà a oltre 4,2 miliardi.

Quindi la posta elettronica è viva e vegeta e continua ad essere lo strumento di comunicazione preferito in azienda. Immagino che sia così anche nella tua.

Il largo utilizzo che viene fatto dell'email, tuttavia, **ha attirato le attenzioni dei cyber criminali che hanno concentrato le proprie attività illecite attorno a questo strumento**.

Sai che di tutti gli attacchi informatici il 91% nasce da un'email pericolosa? In particolare, la tecnica maggiormente sfruttata è quella del **phishing**.

Il phishing è un **tentativo di frode informatica** che consiste nell'**invio di email contraffatte** con l'obiettivo di impossessarsi dei tuoi dati personali come codici di accesso all'internet banking, numeri di carta di credito, password e altri dati sensibili.

Probabilmente il tuo fornitore di servizi IT sta già facendo un buon lavoro per cercare di proteggerti da questi attacchi attraverso una serie di strumenti in grado di filtrare le email "cattive" e di far arrivare a destinazione solo quelle "buone". Tuttavia, nessuno strumento è perfetto, e **gli hacker continuano a perfezionare gli attacchi di phishing** in modo da renderli sempre più mirati, credibili e di difficile individuazione da parte degli strumenti di sicurezza informatica.

Diventa quindi fondamentale che tu e tutto il personale della tua azienda siate in grado di riconoscere le email pericolose a colpo d'occhio, in modo da evitare di cadere vittima di attacchi che a volte hanno conseguenze devastanti per aziende e privati.

Vediamo insieme come fare.

RICONOSCERE AL VOLO UNA EMAIL DI PHISHING

Fino a qualche anno fa le email di phishing erano facilmente riconoscibili perché presentavano evidenti errori grammaticali o erano assolutamente fuori contesto rispetto al destinatario che le riceveva, **oggi non è più così**.

- Le email di phishing provengono molto spesso da mittenti o brand noti, come un fornitore con cui si collabora, un servizio o un portale online (Microsoft 365 o G Suite, ad esempio) che si usa in azienda o l'istituto di credito di fiducia.
- Spesso c'è un link che porta ad un sito web che è quasi indistinguibile da quello autentico ma che è in grado di carpire le credenziali o i dati bancari immessi dall'utente.
- Queste email, possono presentare dei dati verosimili come il tuo nome, un posto in cui sei stato di recente, un acquisto che hai effettuato, ecc.
- Anche gli errori grammaticali sono stati quasi del tutto azzerati.

Di seguito **riporto alcuni degli esempi più comuni di email di phishing**: fai particolare attenzione quando ti imbatti in questo tipo di messaggi.

Email di phishing più comuni

Finte email a nome della banca

È uno dei più classici tipi di phishing.

Consiste spesso in una **email che sembra inviata dalla banca** nella quale ti viene comunicato che il tuo conto sta per essere bloccato, oppure che è stato utilizzato per operazioni anomale, o ancora come conferma di esecuzione di un'operazione bancaria.

In ogni caso, in tutte queste comunicazioni, ti viene chiesto di cliccare sul link della email per autenticarti e "sistemare" così le cose.

Le banche, in realtà, non comunicano quasi mai per email e ancora più raramente chiedono di svolgere delle azioni all'interno di un messaggio di posta elettronica.

Email da siti di aste online o e-commerce

Il funzionamento è simile a quello delle banche.

Ricevi una email dove **vieni avvisato di aver ricevuto un pagamento per un acquisto, o di aver eseguito un pagamento**.

Anche in questo caso vieni invitato a cliccare sul link per effettuare le verifiche.

L'obiettivo in questo caso è impossessarsi della tua identità e dei numeri di carte di credito che spesso sono memorizzate nel tuo account online del sito di aste o e-commerce.

Offerte di lavoro... troppo allettanti

In questo caso ricevi una email in cui ti **viene proposto un lavoro promettendoti spesso alti guadagni**, poco impegno e ruoli importanti: "dirigente, amministratore delegato...". Si tratta di false società gestite dai truffatori e l'obiettivo è rubare i tuoi dati personali per attività illegali.

Attività di trasferimento denaro

In questo caso i truffatori cercano persone da utilizzare per **attività illegali di riciclaggio** promettendo, anche in questo caso, importanti ricompense.

Di fatto, le persone così reclutate ricevono un bonifico dal truffatore sul proprio conto corrente e a loro volta ricevono istruzioni per trasferire quanto ricevuto su altri conti. Ovviamente si tratta di un'attività illegale.

Caratteristiche di una email di Phishing

Vediamo ora come individuare le email di phishing attraverso alcuni rapidi controlli.

Mittente sospetto

I criminali informatici utilizzano varie tecniche di spoofing per indurre gli utenti a credere che un'email sia legittima. **Controlla attentamente il dominio** per individuare domini simili o non coerenti con la presunta provenienza della email. **Fai attenzione quando leggi l'email sul tuo dispositivo mobile**, poiché è possibile che su questi dispositivi (gli iPhone principalmente) venga visualizzato solo il nome e non l'indirizzo email. Ad esempio, una falsa email a nome della Banca Sella potrebbe riportare un mittente di questo tipo:

- "Risorse umane" risorseumane@sella.it (dominio corretto ma indirizzo inesistente).
- "Mario Guidi" mario.guidi@sellla.it (dominio simile).
- "Mario Guidi" mario.guidi@sella-spa.it (dominio falso).
- "Mario Guidi" alfiomartino1482@gmail.com (email che non ha nulla a che fare con la Banca Sella).

Oggetto

Una email di phishing può usare un **linguaggio accattivante, urgente o minaccioso** per incoraggiare il destinatario ad agire immediatamente. Evocare un senso di curiosità, avidità o paura è una tattica comune tra gli schemi di phishing. Ecco alcuni esempi:

- "Attenzione, il tuo conto è stato bloccato".
- "Richiedi online il tuo preventivo".
- "Problemi di rinnovo".
- "Cambio della password".

Errori

Leggi attentamente l'email: spesso i cyber criminali usano sistemi di traduzione automatica per cui le email **contengono palesi errori grammaticali**. Ci sono poi attacchi più sofisticati per cui la grammatica è corretta ma potrebbero esserci errori più sottili, come problemi di spaziatura o uso di simboli anziché di parole. Ma fa attenzione**: in alcuni casi, non ci saranno errori**.

Allegati

Diffidare di email che includono allegati. Le email di phishing possono includere un collegamento in un allegato, anziché sotto forma di link nel corpo dell'email, per evitare il rilevamento da parte di un filtro email.

Il consiglio è di non scaricare allegati che non ti aspetteresti di ricevere e di farlo solo dopo aver verificato che l'email non presenti caratteristiche tipiche di un'email di phishing.

Immagini

I criminali informatici possono facilmente replicare loghi, immagini e badge di marchi in email e pagine web indistinguibili da quelli reali. Considerare tutti i fattori sopra indicati quando si decide se fare clic.

In caso di dubbi, verificalo. **ISITPHISHING.AI (http://isitphishing.ai/)** è un servizio gratuito che esegue analisi in tempo reale dell'URL e della pagina web per determinare se si tratta di un tentativo di phishing.

RICONOSCERE AL VOLO UNA EMAIL DI SPEAR PHISHING

Lo spear phishing è una variante recente del phishing. **Lo spear phishing prevede l'invio di un'email che sembra provenire da una persona o un'azienda conosciuti**. Lo scopo dello spear phishing spesso è il furto di dati aziendali e il trasferimento di grosse somme di denaro. Lo spear phishing **può iniziare con delle email non pericolose** (non ci sono allegati camuffati o link da cliccare) con lo scopo di instaurare un dialogo con la persona che la riceve per conquistare la sua fiducia.

Nella figura sottostante, due esempi di email di questo tipo. La prima arrivata (apparentemente) a nome di Kevin Beatty (vicedirettore marketing di MDaemon Technologies) e la proveniente (apparentemente) da un amico del destinatario.


venerdì 06/09/2019 16:01

Kevin Beatty <kaain.beatty@altn.com>

Overdue Invoice

A

Greetings,

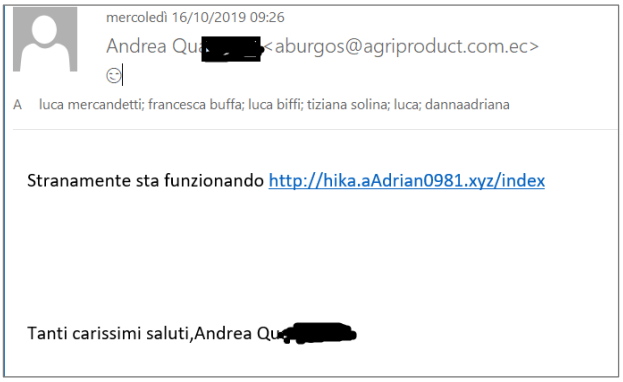
Can you confirm to me the status of your overdue payments if there are any.Please get back to us at the earliest with total amount overdue payment with corresponding due dates and copy of invoices preferably.

Your immediate response will be highly appreciated.

Kevin Beatty
Vice President of Marketing and Business Development
MDaemon Technologies, Ltd.
Address : 4550 State Highway 360, Suite 100
Grapevine, TX 76051
U.S. Toll Free: 866-601-2586
International: 817-601-3222
Fax: 817-601-3223
https://www.altn.com

In questo esempio due sono le cose che devono far sospettare sulla veridicità di questo messaggio:

1. Il **contenuto che parla di pagamenti**. Occorre prestare attenzione ai messaggi che invogliano a versare denaro, fornire numeri di carta di credito a altri dati personali. Peraltro, Kevin si occupa di marketing e non di pagamenti.
2. La **contraffazione del mittente**: in questo caso è sbagliato il nome dell'indirizzo email.



Caratteristiche di una email di Spear Phishing

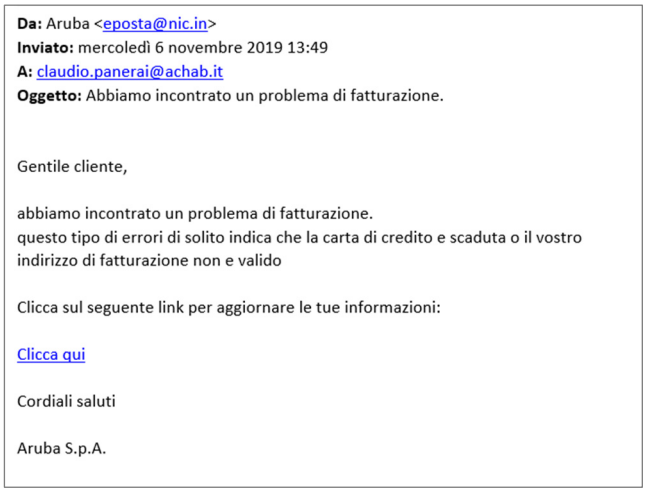
Vediamo ora come a quali elementi occorre prestare attenzione in caso di sospetto attacco di spear phishing.

Mittente

Ci sono diverse varianti di mittenti più o meno alterati che si possono incontrare:

- "Human Resources" ur@altn.com (dominio corretto ma indirizzo inesistente).
- "Kevin Beatty" kevin.beatty@altn.com (indirizzo e nome corretti).
- "Kevin Beatty" kevin.beatty@altm.com (dominio alterato ma molto simile a quello vero).
- "Kevin Beatty" kevin.beatty@altn-inc.com (dominio alterato ma molto simile a quello vero).
- "Kevin Beatty" random@gmail.com (indirizzo email è completamente diverso).

È importante quindi, quando si apre un messaggio sospetto o se ne visualizza l'anteprima, controllare il mittente del messaggio e verificare se nome e indirizzo email sono coerenti con la provenienza dichiarata dal messaggio stesso.
L'esempio seguente rientra nella quarta tipologia (indirizzo email completamente slegato dal nome):



Oggetto

Una email di spear phishing può usare un **linguaggio accattivante, urgente o minaccioso** per incoraggiare il destinatario ad agire immediatamente o per catturare l'attenzione dell'utente. L'oggetto di queste email può contenere termini commerciali e finanziari, come "ordine", "fattura", "pagamento", "purchase," "invoice," "direct deposit," ecc.

Contenuti

Il corpo della email spesso è rapido e puntuale e **include quasi sempre una richiesta finanziaria**. Gli hackeri in questi casi usano spesso un linguaggio progettato per far sentire la vittima come l'unica persona che può completare la richiesta e che non farlo in modo tempestivo potrebbe essere dannoso per l'azienda.

Pre-attacco

Il pre-attacco è una forma di ingegneria sociale in cui un criminale informatico **coinvolge una vittima nel corso di una o più email per ottenere la sua fiducia**. Sulla base delle informazioni che ha scoperto sulla vittima, l'attaccante lancia una piccola chiacchierata con la vittima per abbassare la guardia, come "Come sono andate le vacanze?" O "Congratulazioni per la promozione".

Firma

I cyber criminali spesso includono **una riga aggiuntiva nella firma che indica che il messaggio è stato composto su un telefono cellulare o tablet**. Questo aiuta a rafforzare la natura urgente del messaggio, crea una scusa per inviare l'email da un indirizzo email personale e presenta una copertura per eventuali errori grammaticali o stilistici nell'email.

EMAIL CHE CONTENGONO CRIPTO-VIRUS O ALTRO MALWARE

Le email che veicolano cripto-virus o altro malware spesso, per superare i controlli, sono composte da **poche righe di testo e un allegato o un link pericoloso**. Se aperto l'allegato o cliccato il link ha inizio l'infezione che può provocare il blocco del proprio PC e/o la contaminazione delle altre macchine della rete aziendale.

L'antivirus locale non sempre è in grado di bloccare questi malware per cui occorre prestare molta attenzione alle email che contengono allegati e link, anche se provengono da mittenti conosciuti. Occorre in particolare prestare **attenzione alle email con allegati documenti di office** (.doc, .docx, .xls e .xlsx), **immagini, pdf e zip**. Chi riceve una email con un allegato di questo tipo, prima di aprirlo, deve:

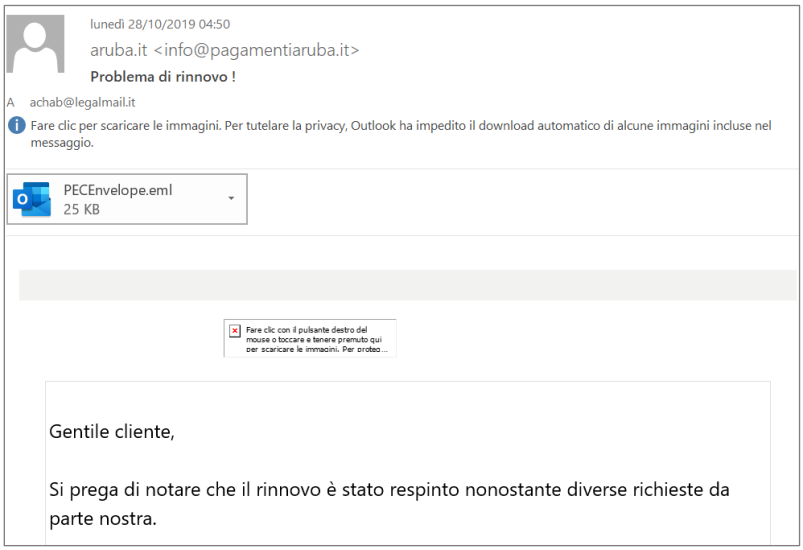
1. **Analizzare il mittente** del messaggio per capire se il mittente stesso è un mittente conosciuto e affidabile e non "falsificato" (vedi sezioni **Mittente** dei paragrafi precedenti).
2. **Leggere attentamente il testo** del messaggio per capire se si tratta di contenuti affidabili; ad esempio in una mail che cita "accettazione ordine n°…", il numero dell'ordine deve essere compatibile con la numerazione usata dall'azienda.
3. Se la mail cita una persona, **verificare che il testo sia coerente con le mansioni svolte dalla persona;** nell'esempio di Kevin Beatty del paragrafo precedente, Kevin si occupa di marketing e non di pagamenti come cita invece il testo del messaggio.

Email di spam e phishing purtroppo arrivano anche via PEC, per cui occorre non abbassare la guardia pensando che le email PEC siano immuni da questo tipo di abusi.

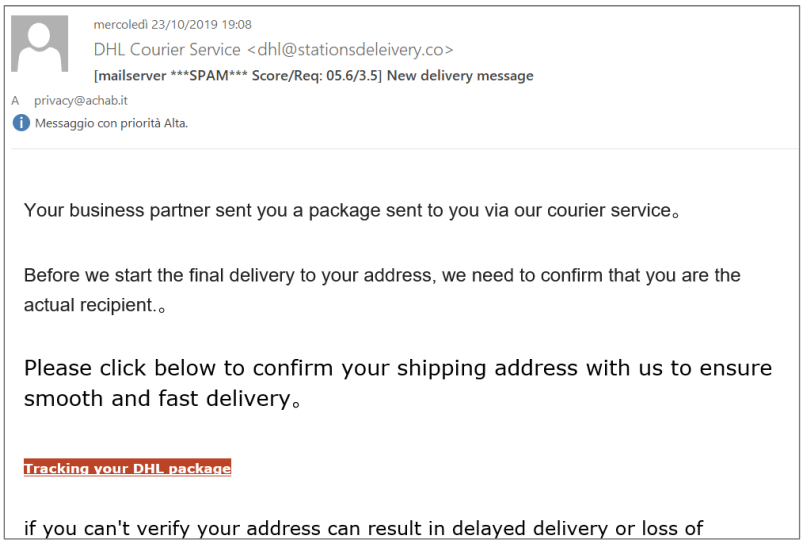
Attenzione poi, che alcune email possono sembrare delle PEC per la presenza di un allegato PECEnvelope.eml che assomiglia molto all'allegato postacert.eml presente nelle PEC vere.

Di seguito alcuni esempi di email pericolose.

Falsa PEC:



Email con link pericoloso:



mercoledì 23/10/2019 19:08

DHL Courier Service <dhl@stationsdeleivery.co>

[mailserver ***SPAM* Score/Req: 05.6/3.5] New delivery message**

A privacy@achab.it

Messaggio con priorità Alta.

Your business partner sent you a package sent to you via our courier service。

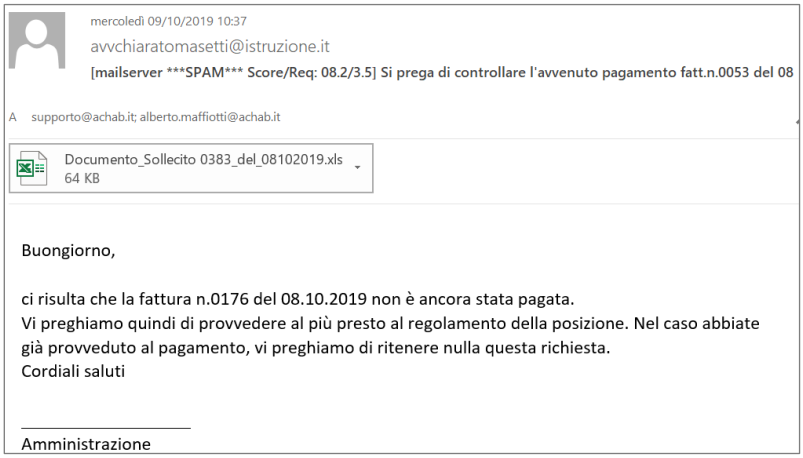
Before we start the final delivery to your address, we need to confirm that you are the actual recipient.。

Please click below to confirm your shipping address with us to ensure smooth and fast delivery。

Tracking your DHL package

if you can't verify your address can result in delayed delivery or loss of

Email con allegato pericoloso:



mercoledì 09/10/2019 10:37

avvchiaratomasetti@istruzione.it

[mailserver ***SPAM* Score/Req: 08.2/3.5] Si prega di controllare l'avvenuto pagamento fatt.n.0053 del 08**

A supporto@achab.it; alberto.maffiotti@achab.it

Documento_Sollecito 0383_del_08102019.xls
64 KB

Buongiorno,

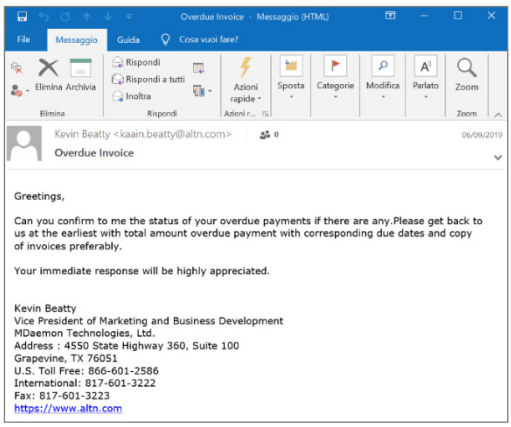
ci risulta che la fattura n.0176 del 08.10.2019 non è ancora stata pagata.
Vi preghiamo quindi di provvedere al più presto al regolamento della posizione. Nel caso abbiate già provveduto al pagamento, vi preghiamo di ritenere nulla questa richiesta.
Cordiali saluti

Amministrazione

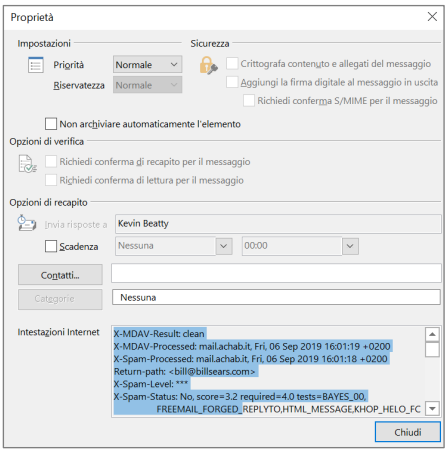
ANALIZZARE L'HEADER DI UN MESSAGGIO

Se si hanno ancora dubbi sulla provenienza effettiva del messaggio, si può analizzare l'header del messaggio ricevuto. In Outlook, ad esempio, questo si può fare con questi passi:

1. Aprire il messaggio e selezionare il menu **File**, in alto a sinistra e poi il bottone Proprietà.



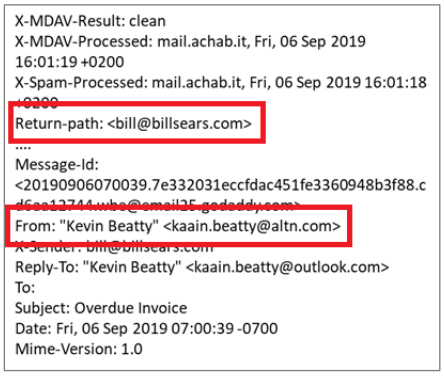
2. Nel popup che appare, nella sezione **Intestazioni Internet**, selezionare tutto il testo contenuto nella text area e poi tasto destro -> Copia



3. Incollare il testo copiato nel blocco note di Windows

```
X-MDAV-Result: clean
X-MDAV-Processed: mail.achab.it, Fri, 06 Sep 2019
16:01:19 +0200
X-Spam-Processed: mail.achab.it, Fri, 06 Sep 2019 16:01:18
+0200
Return-path: <bill@billsears.com>
....
Message-Id:
<20190906070039.7e332031eccfdac451fe3360948b3f88.c
d6aa12744.wbe@email25.godaddy.com>
From: "Kevin Beatty" <kaain.beatty@altn.com>
X-Sender: bill@billsears.com
Reply-To: "Kevin Beatty" <kaain.beatty@outlook.com>
To:
Subject: Overdue Invoice
Date: Fri, 06 Sep 2019 07:00:39 -0700
Mime-Version: 1.0
```

4. Confrontare il valore dell'header **Return-path** (il reale mittente che ha spedito) con il valore dell'header **From** (il mittente dichiarato da chi ha spedito). Se sono diversi, il messaggio è sospetto.



CONCLUSIONI

L'email è uno strumento estremamente utile sul lavoro, ma anche molto pericoloso. Seguendo i consigli riportati in questo documento sarai in grado di riconoscere le email pericolose più comuni, ma attenzione: se dovessi avere dei dubbi chiedi sempre consiglio al tuo fornitore di servizi IT, lui saprà sempre consigliarti al meglio.

Glossario

Spoofing – Tipo di attacco informatico che impiega in varie maniere la falsificazione dell'identità (spoof).

Cripto-virus – Tipologia di virus in grado di rendere illeggibili i dati presenti su una macchina o su una serie di macchine collegate alla stessa rete. Il ransomware è una variante di cripto-virus che richiede il pagamento di un riscatto da parte della vittima con il fine di rendere nuovamente leggibili i dati.

Dominio email – Si tratta della parte dell'indirizzo email posto dopo il simbolo @.

Header email – Si tratta dell'intestazione di un'email e contiene le informazioni relative alla "vita" del messaggio, dal momento in cui viene inviato alla ricezione, oltre alle informazioni che riguardano l'autore dell'email.