Avviso di sicurezza del 24/06/2022

Segnalazione di campagna malevola a tema “spedizione bloccata presso il corriere”

Gent.Utenti,

pubblichiamo questo avviso per segnalare una campagna malevola a tema “Una spedizione postale è bloccata”. La campagna mira a convincere l’utente ad effettuare un piccolo pagamento tramite carta di credito.

La campagna può essere riconosciuta come malevola dalle seguenti caratteristiche:

- La mail non proviene da un dominio riferibile ad il corriere indicato
- Il mittente e/o l’oggetto della mail contiene inserimenti/sostituzioni di caratteri con lo scopo di sviare gli algoritmi di analisi anti-virus, es: *_Sp3dizi0ne* al posto di *Spedizione*
- Il link proposto non è riferibile al corriere (solitamente si può avere la preview del link soffermandocisi sopra per alcuni secondi)
- Il destinatario del pagamento non è riferibile al corriere.

Vi chiediamo di verificare autonomamente sul portale del corriere indicato l’effettiva esistenza di spedizioni in atto e vi chiediamo di avere la massima prudenza nell’effettuare pagamenti elettronici verificando sempre il soggetto a cui il pagamento sarà diretto. Di seguito potete trovare il dettaglio della campagna malevola.

Ricordiamo di mantenere alta la diffidenza rispetto a richieste inusuali soprattutto se di tipo economico.

Grazie per l'attenzione.

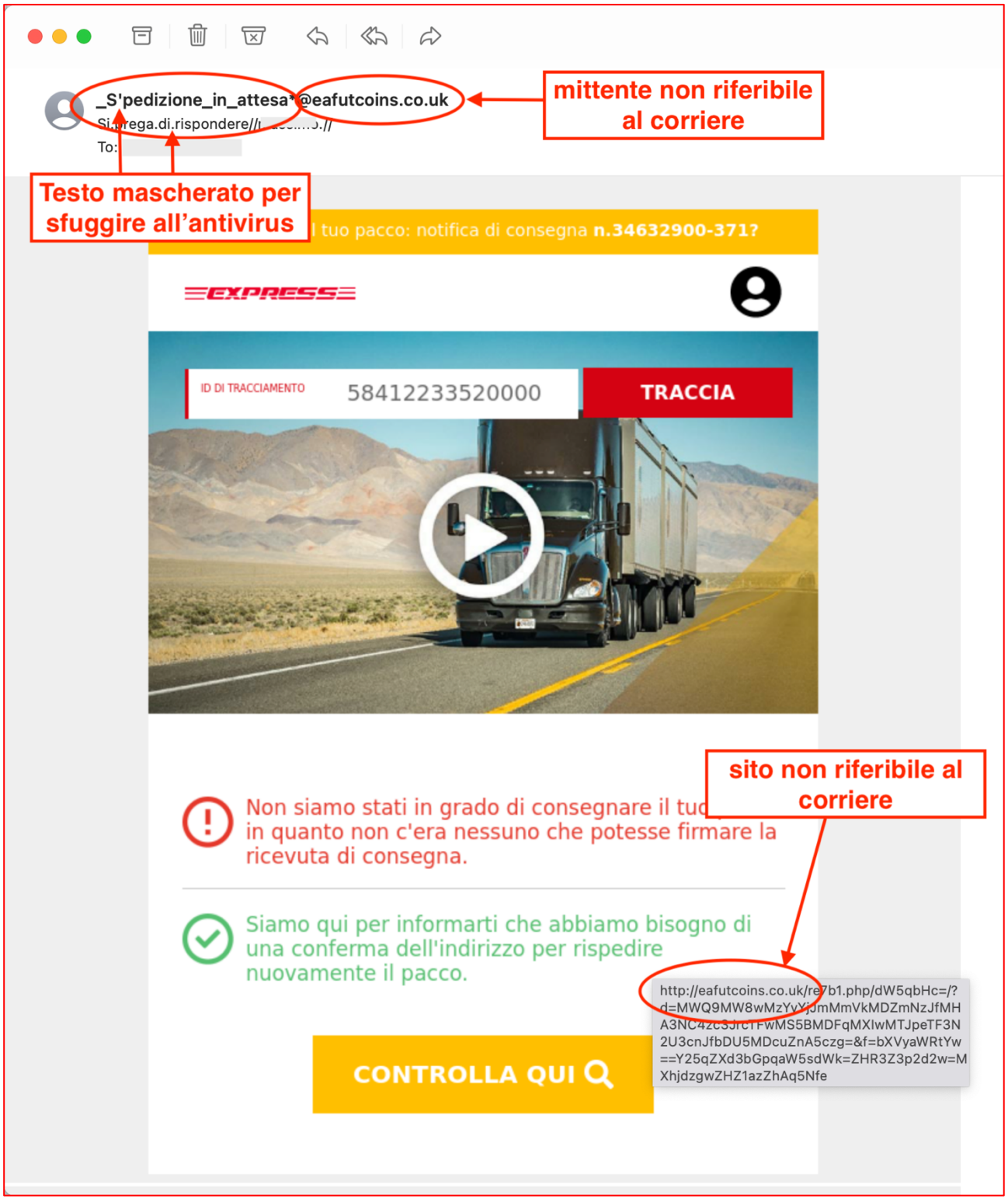
I più cordiali saluti.

Settore Cybersecurity, Protezione Dati e Conformita' - Direzione ICT
Universita' degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

UNIMI-SOC-202206230000000002 Per favore, non cancellate questa riga
e usate questa mail per ulteriori comunicazioni su questa segnalazione

Dettaglio della campagna malevola

La campagna malevola è veicolata attraverso una mail che segnala un ipotetico problema di consegna di un pacco:



Dall'esame visuale della mail e del link proposto si possono individuare delle caratteristiche anomale:

- La mail non proviene da un dominio riferibile ad il corriere indicato
- Il mittente e/o l'oggetto della mail contiene inserimenti/sostituzioni di caratteri con lo scopo di sviare gli algoritmi di analisi anti-virus, es: *_Sp3dizi0ne* al posto di *Spedizione*
- Il link proposto non è riferibile al corriere.

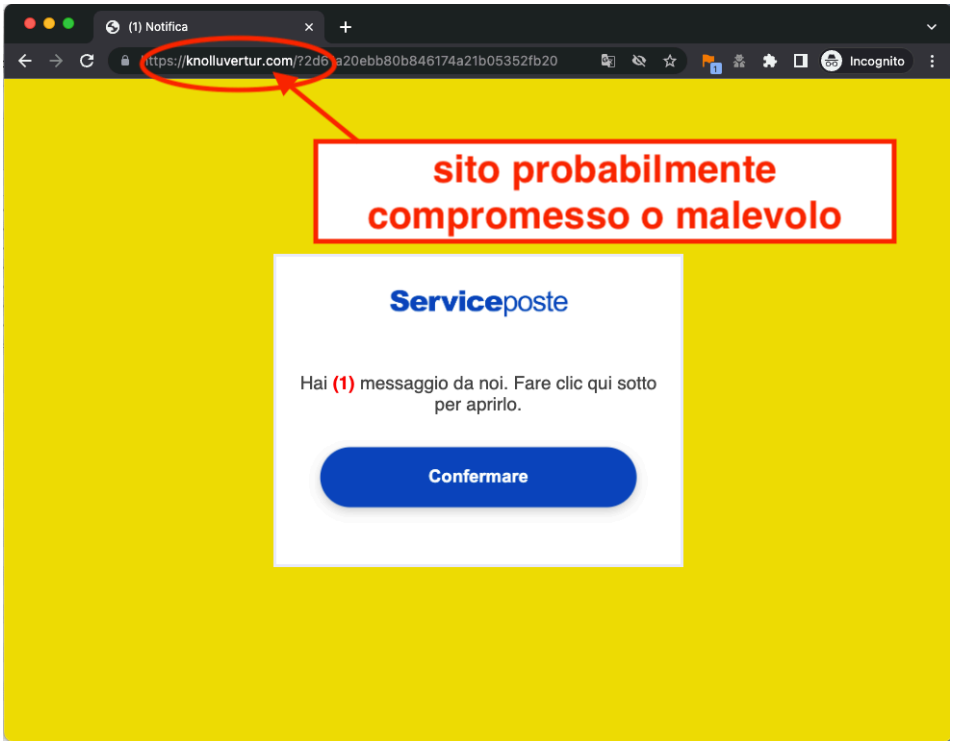
E'possibile anche analizzare l'header nascosto della mail seguendo le indicazioni della guida scaricabile al link:

https://work.unimi.it/filepub/sicurezza_ict/DICT_IO_GuidaPraticaAnalisiMail_rev.3del16062021.pdf

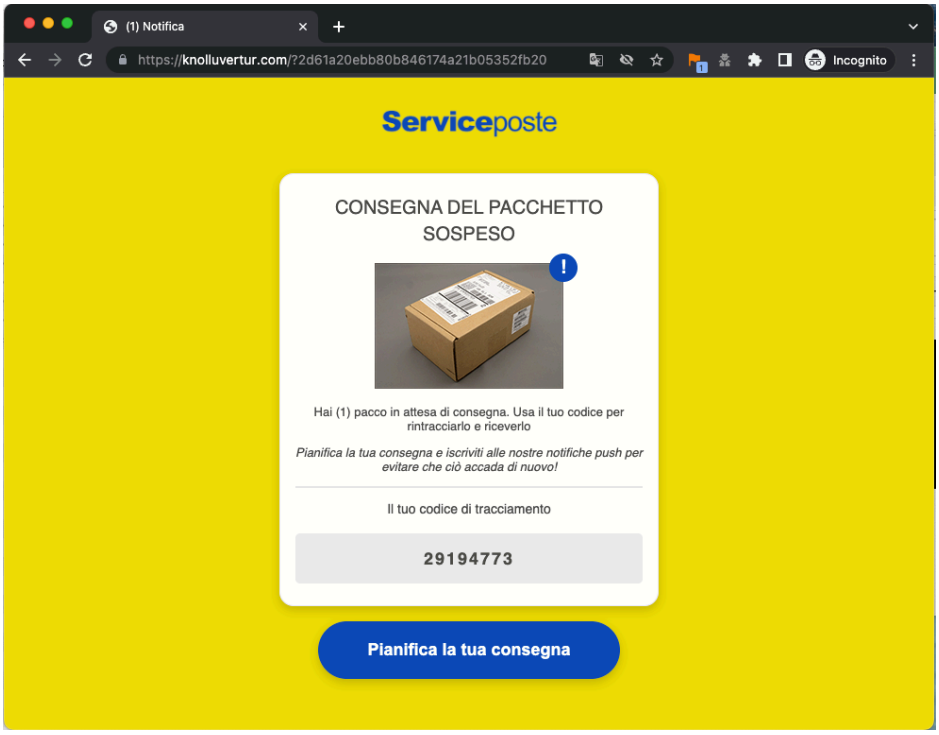
```
Received: by 2002:a05:6....
...lts: i=1; mx.google.com;
       dkim=pass header.i=@eaf..
       ..:03 -0700 (PDT)
Received-SPF: pass (google.com: domain of return@eafutcoins.co.uk designates .....80.202;
Authentication-Results: mx.google..
..FOdTWPjYCsnHV97IzBqzdr8jsiMOCRvyn7YKW93mZH0Uc
   bPXTIwnecovT7IWHQpU=
DomainKey-Signature: a=rsa-sha1; c=nof..
..5060530307506186370 60@eafutcoins.co.uk>
Return-Path: ">" _S'pedizione_in_attesa*@eafutcoins.co.uk>
To: <......>
In-Reply-To: <......>

Sender: _S'pedizione_in_attesa*@eafutcoins.co.uk

Auto-Submitted: auto-generated
x-mid: 424054902953129431258641896878
X-SES-Outgoing: __SmtpDate 27.255.80.202

From:  _S'pedizione_in_attesa*@eafutcoins.co.uk
X-NFM-EmailParse-FWD: __SmtpDate
X-Mailer: Phpmailer
Date: __SmtpDate
X-Originating-IP: 27.255.80.202
Content-Type: multipart/digest; boundary="-__=__VMS2__QifMbIg3....sZjBPHOdY31Q3ldr=?"
Mime-Version: 1.0
```

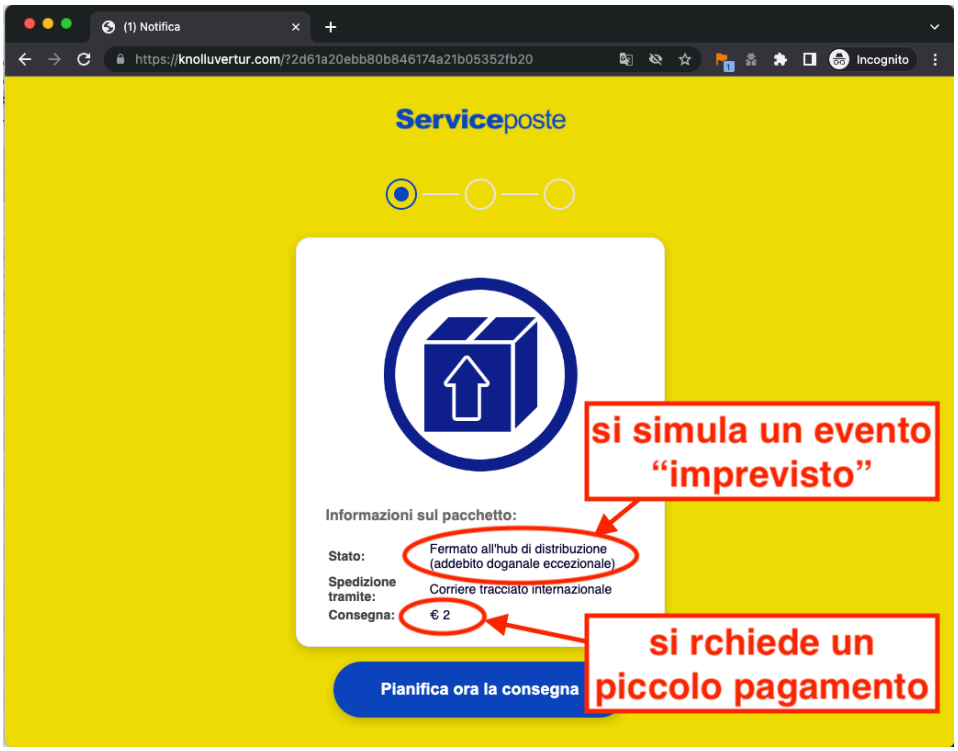
Dall'analisi dell'header si può individuare il mittente effettivo "eafutcoins.co.uk" che non è riferibile al corriere.

Se erroneamente si procede cliccando il link proposto si raggiunge, dopo una redirezione automatica, il sito malevolo vero e proprio che simula il portale del corriere:

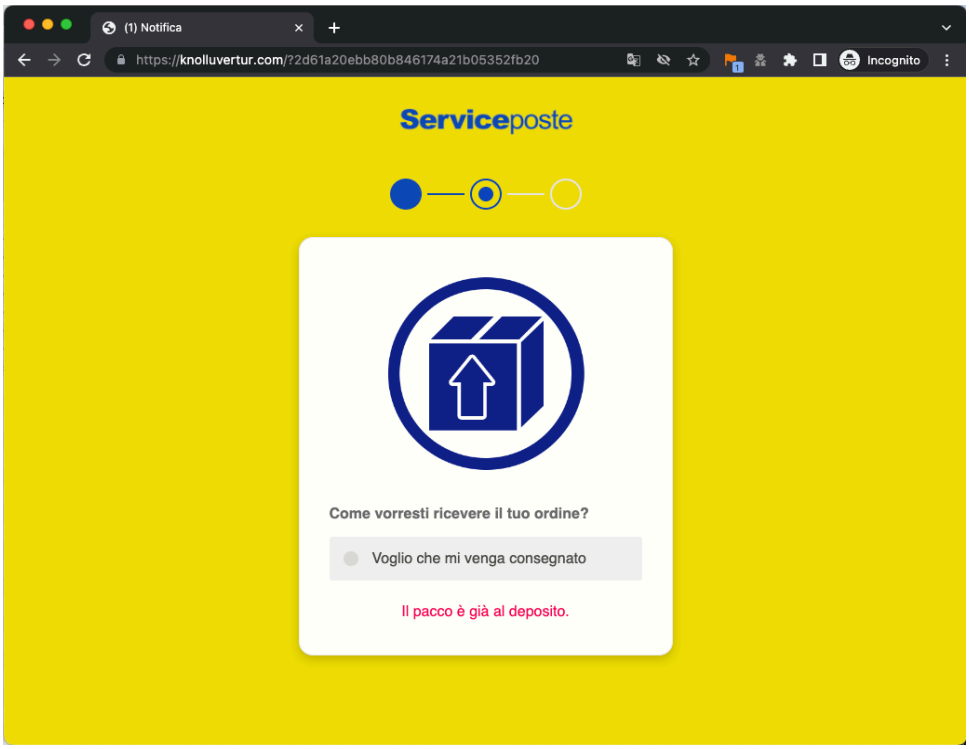


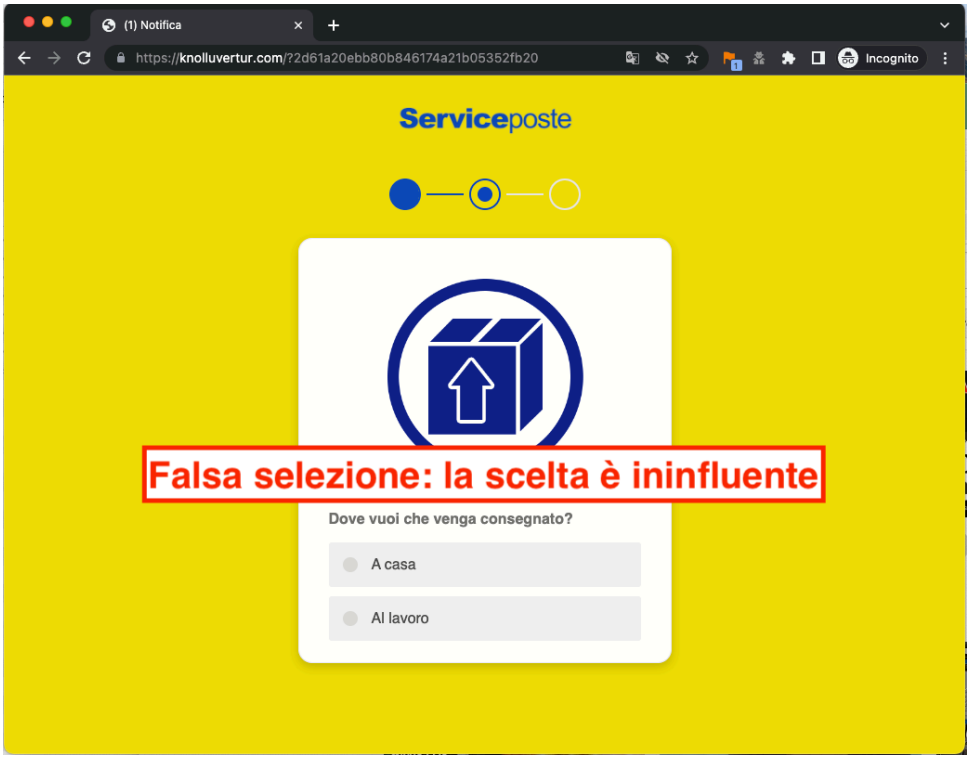
Se la vittima procede nella sequenza di schermate si viene diretti inevitabilmente verso la pagina di phishing dei dati personali ed il form di pagamento:

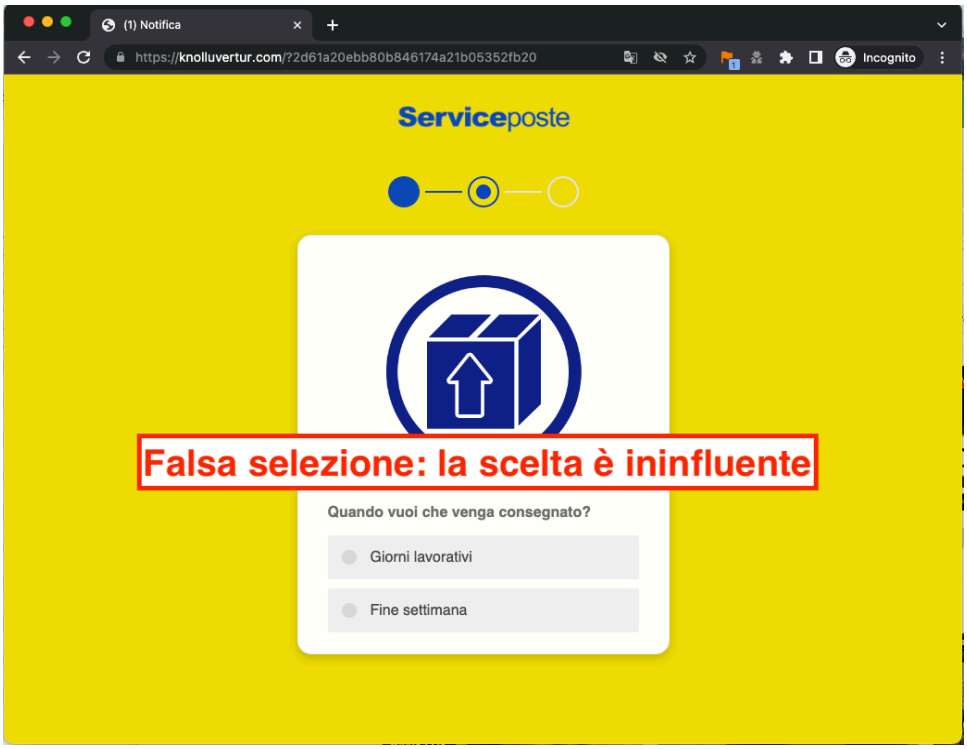


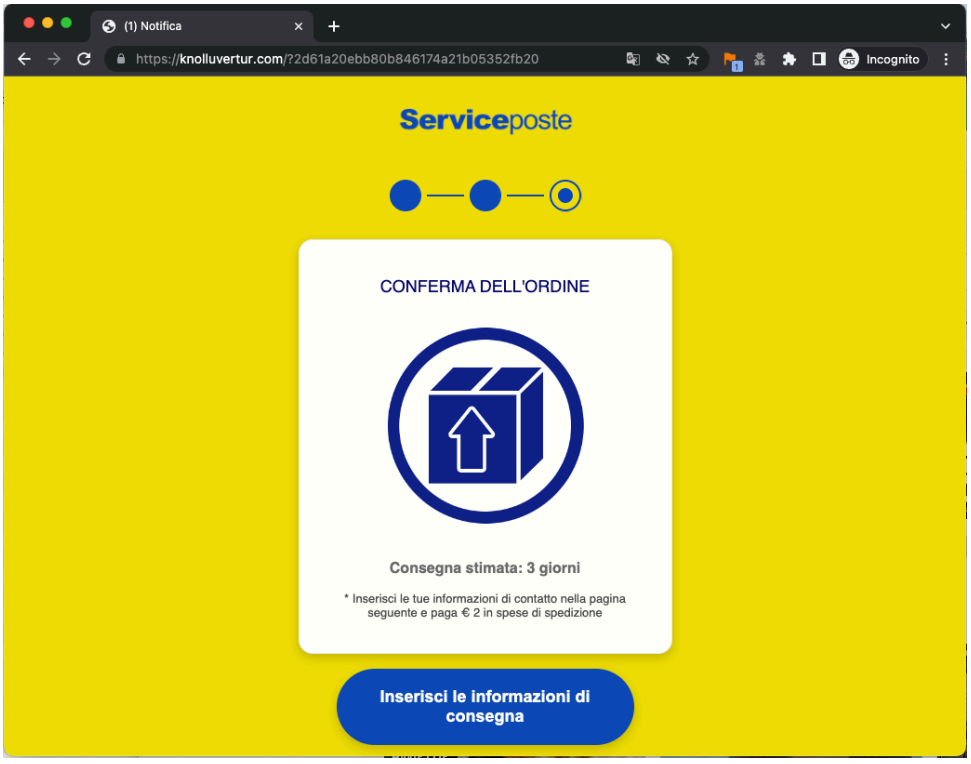

(1) Notifica
https://knolluvertur.com/?2d61a20ebb80b846174a21b05352fb20
Incognito
Serviceposte
si simula un evento "imprevisto"
Informazioni sul pacchetto:
Stato:
Fermato all'hub di distribuzione (addebito doganale eccezionale)
Spedizione tramite:
Corriere tracciato internazionale
Consegna:
€ 2
si rchiede un piccolo pagamento
Pianifica ora la consegna


(1) Notifica
https://knolluvertur.com/?2d61a20ebb80b846174a21b05352fb20
Incognito
Serviceposte
Finto passaggio di selezione: questa scelta è finta
Come vorresti ricevere il tuo ordine?
Voglio che mi venga consegnato
Vado a prenderlo io stesso
voce non selezionabile

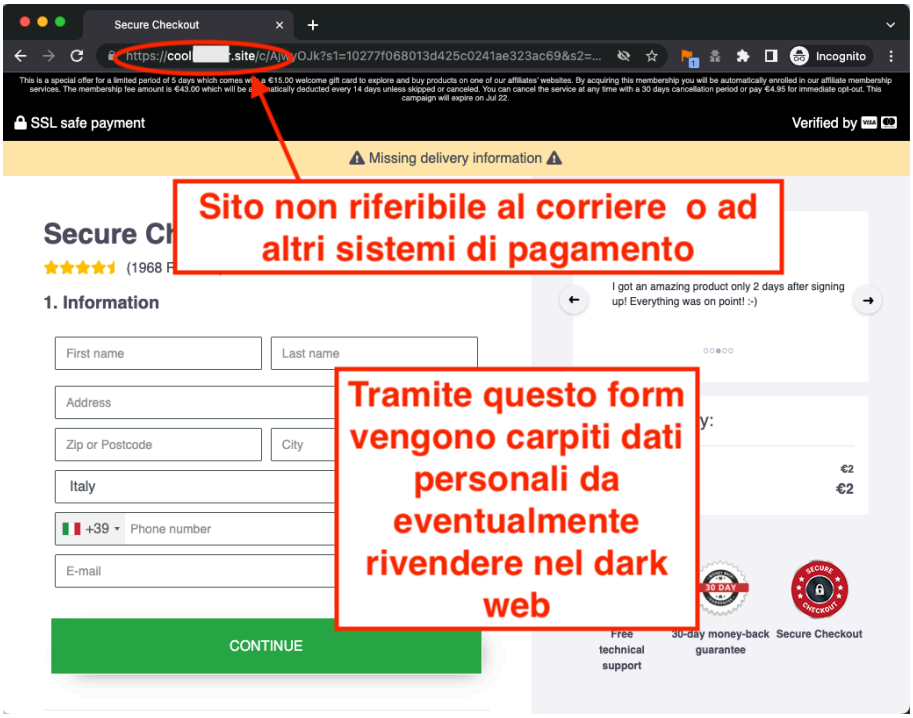

(1) Notifica
https://knolluvertur.com/?2d61a20ebb80b846174a21b05352fb20
Incognito
Serviceposte
Come vorresti ricevere il tuo ordine?
Voglio che mi venga consegnato
Il pacco è già al deposito.

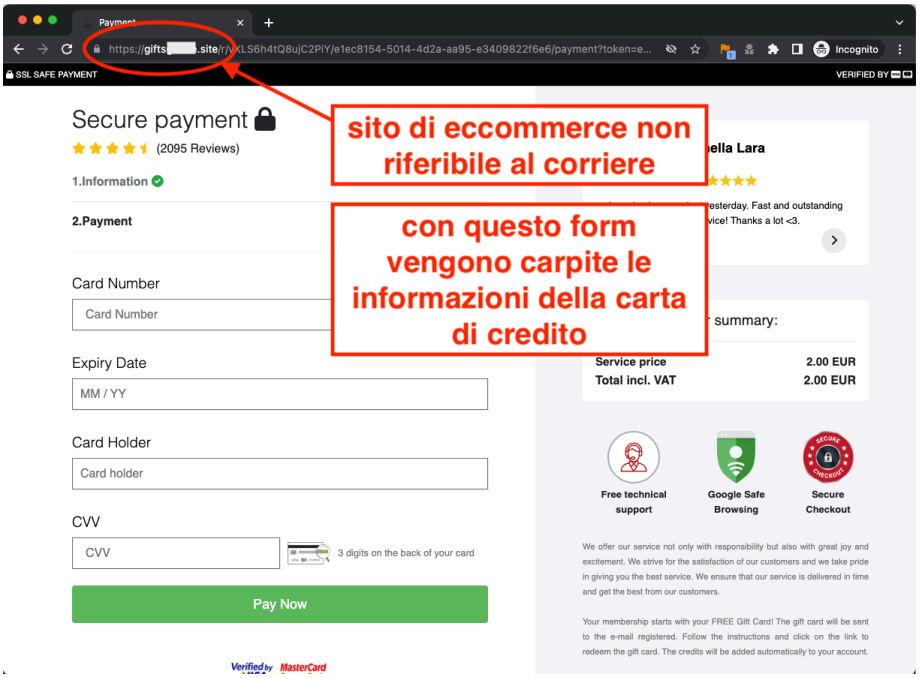

(1) Notifica
https://knolluvertur.com/?2d61a20ebb80b846174a21b05352fb20
Incognito
Serviceposte
Falsa selezione: la scelta è ininfluente
Dove vuoi che venga consegnato?
A casa
Al lavoro


(1) Notifica
https://knolluvertur.com/?2d61a20ebb80b846174a21b05352fb20
Incognito
Serviceposte
Falsa selezione: la scelta è ininfluente
Quando vuoi che venga consegnato?
Giorni lavorativi
Fine settimana

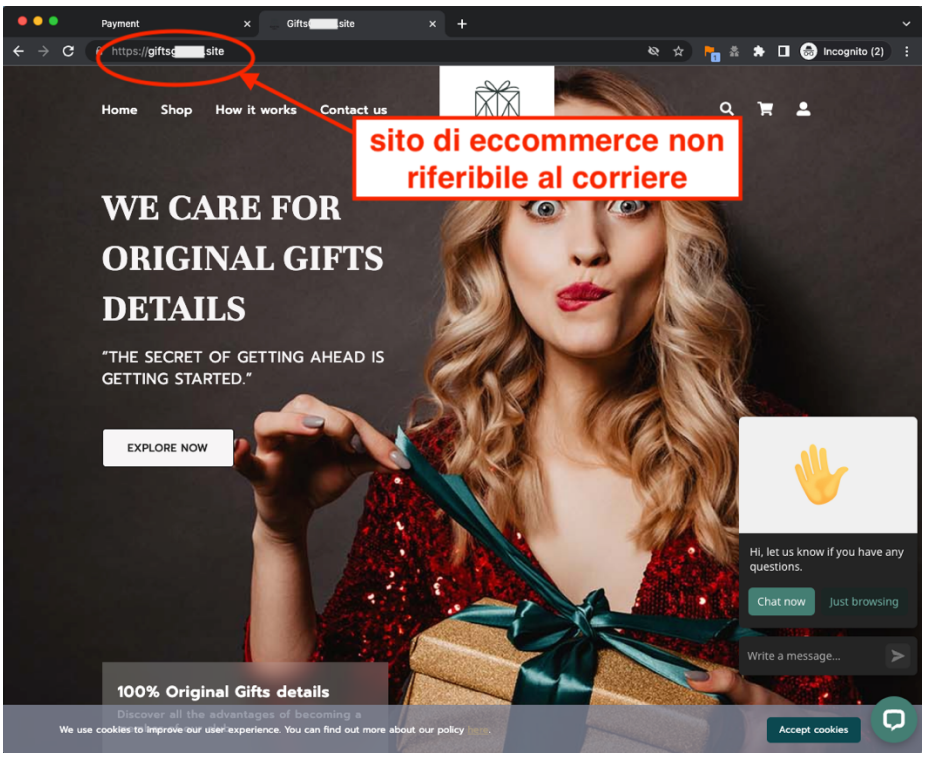

(1) Notifica
https://knolluvertur.com/?2d61a20ebb80b846174a21b05352fb20
Incognito
Serviceposte
CONFERMA DELL'ORDINE
Consegna stimata: 3 giorni
* Inserisci le tue informazioni di contatto nella pagina seguente e paga € 2 in spese di spedizione
Inserisci le informazioni di consegna

Tutti i passaggi fin qui compiuti hanno lo scopo di accreditare la richiesta di informazioni che giunge a questo punto della navigazione e fugare ogni dubbio dalla vittima:





Il sito che ospita la fase di pagamento, non riferibile al corriere:



Contromisure

Nel caso doveste ricevere una mail proveniente da un corriere relativa ad una spedizione, occorre sempre:

- Controllare il mittente della mail e verificare che provenga da un soggetto riferibile al corriere/sito di ecommerce indicato nella mail
- Non cliccare sui link proposti ma connettersi autonomamente al sito del corriere, usando un link preregistrato o cercandolo tramite Google, ed nserendo a mano il codice di spedizione proposto
- Avere sempre estrema diffidenza rispetto a richieste economiche inattese controllando attentamente il sito in cui si stanno introducendo le proprie informazioni.

In caso di dubbio è possibile inoltrare la mail sospetta a sicurezza@unimi.it per un ulteriore controllo.

Grazie per la collaborazione.