



# International Phishing Campaign Impersonating Postal Institutions: Analysis

## Introduction:

This report presents the results of our latest CTI analysis of a particularly malicious phishing campaign targeting traditional mail users around the world. The campaign was characterized by sophistication and large scale, with attackers targeting countries such as Poland, Bolivia, Norway, Portugal, Kuwait, Estonia and many others.

The most disturbing aspect of this campaign was its specificity: the attackers impersonated various trusted postal institutions in order to mislead users and steal their cash. The criminals sent messages informing about alleged shipping problems, containing a link to a fake website. Users who clicked on the link were redirected to a page that looked identical to the real post office website, where they were asked to enter their payment card details.

Through our analysis, however, we were able to identify the infrastructure used by the attackers in this campaign, including server locations, domains and IP addresses. Moreover, we were able to uncover the administrative panels used by the attackers to monitor and manage their attacks. These discoveries have enabled us to gain a deeper understanding of the strategies and tactics used by the attackers, and have provided valuable information that can help counter such attacks in the future.

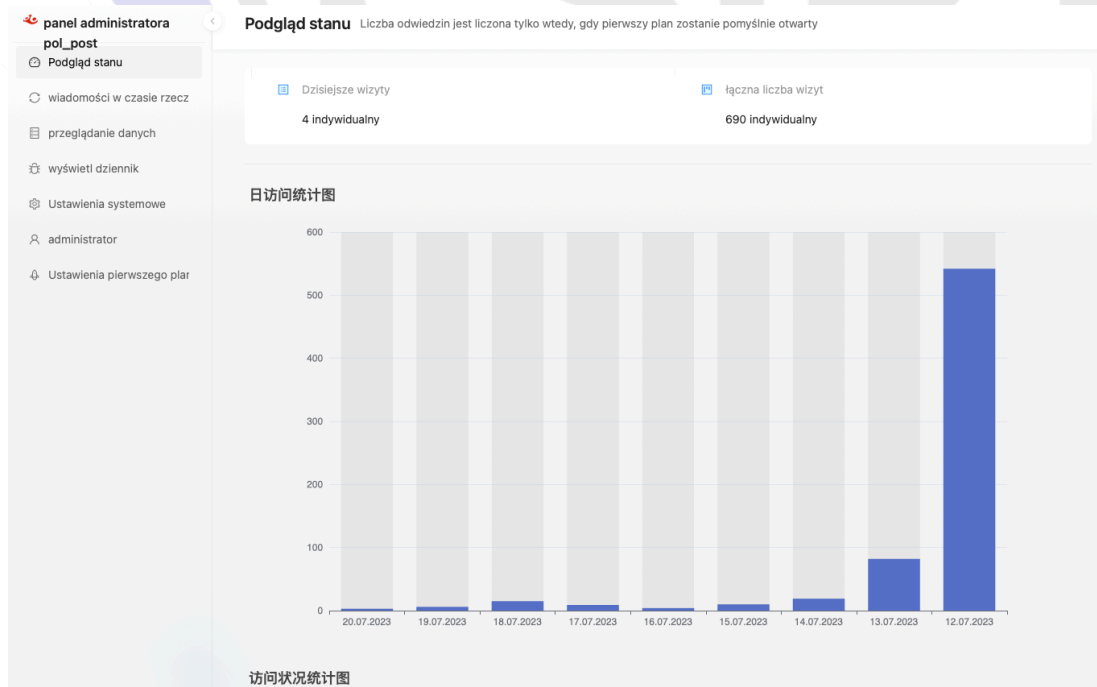


Figure 1 - Admin panel for a phishing campaign on: Post Office.

## Analysis:

### Statistics:

The infrastructure used in the phishing campaign in question was complex and extensive, once again highlighting the elaborate nature of this type of attack. The attackers used a variety of domains and IP addresses, indicating the wide reach and complex nature of their operations.

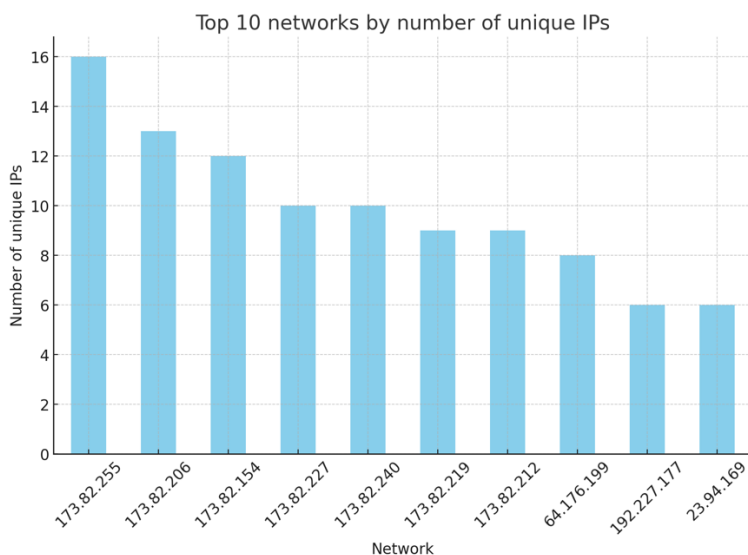


Figure 2 - Top 10 IP networks used in attacks.

Our analysis identified unique domains that were used as part of this campaign. Among them, domains with suffixes such as .top, .xyz, .buzz were particularly common, which may suggest the attackers' preference for specific types of domains.

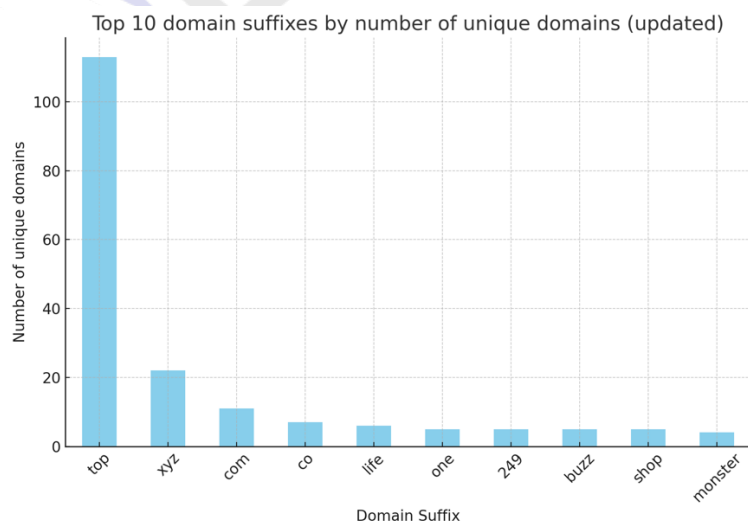


Figure 3 - Top 10 domains used in attacks.

In addition, thanks to the ASN information, we were able to identify organizations that were often used as launching points for attacks. These organizations came from different countries, which shows how global the scope of this campaign was.

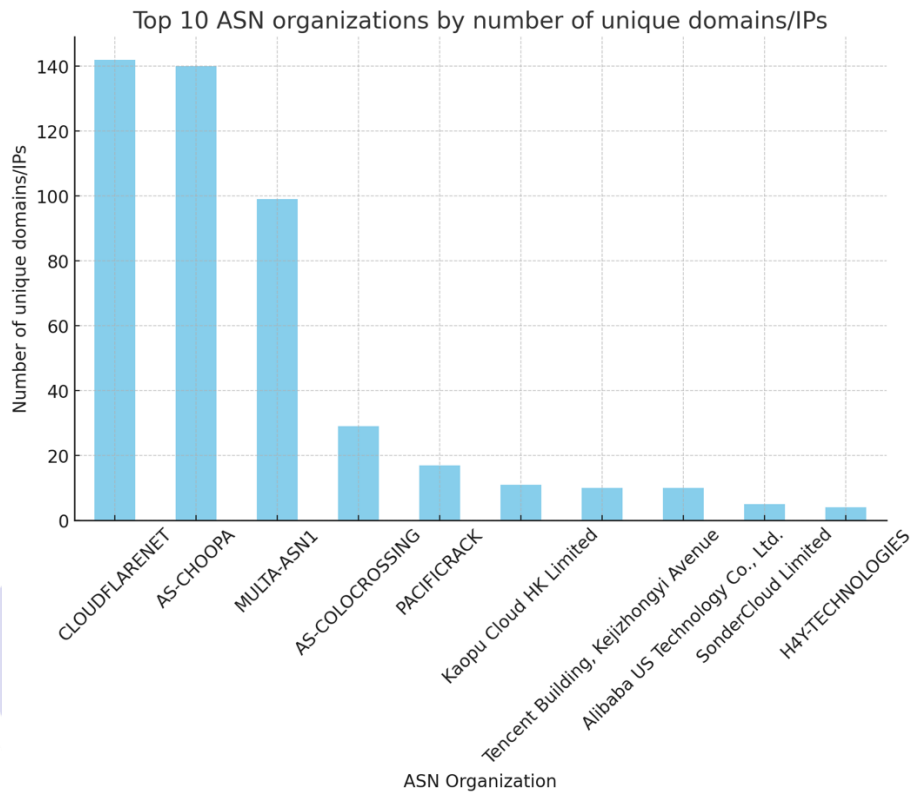


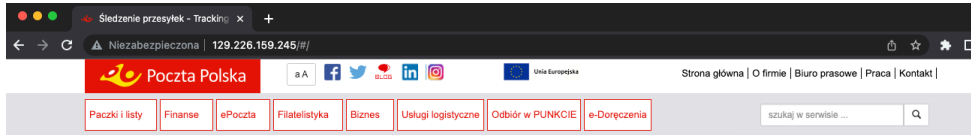
Figure 4 - Top 10 ASNs used in attacks.

## Infrastructure tracking:

The address of the fake site impersonating the Polish Post Office: *poczta-polskad[.]top*

IP address: *129.226.159[.]245*

mmh3 favicon hash: *1797175259*



Strona główna > Współpraca > Śledzenie przesyłek - Tracking

### Status przesyłki

Twój numer pakietu: 856704565

**Zawiadomienie o porażce dostawy**

- Ponieważ adres dostawy nie jest jasny, pakiet nie jest dostarczany
- Twój pakiet powrócił do naszego centrum operacyjnego
- Zaktualizuj swój adres, wysłamy ponownie w 21.07.2023

[Kontynuować](#)

## Passive DNS:

- postal-polskad[.]top
- omnivai[.]xyz
- trojan.zohocloud[.]xyz

URL:  
https://poczta-polskad.top

Device type:  
Desktop

User agent:  
Chrome Android

[Szukaj](#)

Scanning URL: https://poczta-polskad.top  
Adres IP: 129.226.159.245  
 Oznacz IP jako niebezpieczne

Serwisy:

[Shodan](#) [GreyNoise](#) [VirusTotal](#) [Censys](#) [CriminallP](#) [URLScan](#)

Powiązane domeny (50):

LP.	DOMAIN	DATA AKTUALIZACJI	DATA UTWORZENIA
1.	poczta-polskad.top	2023-07-20 11:46:21	2023-07-20 09:50:18
2.	omnivai.xyz	2023-07-17 08:00:22	2023-07-15 11:04:34
3.	trojan.zohocloud.xyz	2021-11-22 11:30:38	2020-10-27 14:34:12

**FOFA.info:**

Query: ip="129.226.159.245"

9 results ( 1 unique IP ), 94 ms, Keyword Search.

Nearly year results, click to view all results.

No	Host/Fid	IP	Port/Protocol	Domain	Lastupdate time
1	129.226.159.245:22	129.226.159.245	22 ssh	-	2023-07-17
2	https://129.226.159.245	129.226.159.245	443 https	-	2023-07-16
3	https://129.226.159.245	129.226.159.245	443 https	-	2023-07-16
4	129.226.159.245	129.226.159.245	80 http	-	2023-07-16
5	129.226.159.245	129.226.159.245	80 http	-	2023-07-16
6	www.omnival.xyz	129.226.159.245	80 http	omnival.x	2023-07-15
7	https://www.omnival.xyz	129.226.159.245	443 https	omnival.x	2023-07-15
8	omnival.xyz	129.226.159.245	80 http	omnival.x	2023-07-15
9	https://omnival.xyz	129.226.159.245	443 https	omnival.x	2023-07-15

**FOFA.info FID:**

Query: fid="mwPk6F0j6G0YSMxscpiQbg=="

610 results ( 399 unique IP ), 252 ms, Keyword Search.

Nearly year results, click to view all results.

No	Host/Fid	IP	Port/Protocol	Domain	Lastupdate time
1	https://tr-ptlgovtr.top	172.67.174.223	443 https	tr-ptlgovtr	2023-07-20
2	https://correos-zl.net	104.21.70.151	443 https	correos-zl	2023-07-20
3	https://www.resubmito...	173.82.206.249	443 https	resubmito	2023-07-20
4	https://www.open-rich.top	173.82.206.126	443 https	open-rich	2023-07-20
5	https://173.82.206.126	173.82.206.126	443 https	-	2023-07-20
6	https://23.94.169.116	23.94.169.116	443 https	-	2023-07-20
7	https://45.32.152.87	45.32.152.87	443 https	-	2023-07-20
8	https://georgianpost.top	23.94.169.116	443 https	georgianp	2023-07-20
9	https://israelpostoffice.t...	45.32.152.87	443 https	israelpost	2023-07-20
10	https://resubmito.top	173.82.206.249	443 https	resubmito	2023-07-20

Favicon:



Identified and active phishing sites as of 20.07.2023:

South Korea - hxxps://epost-go-kr[.]xyz/#/

The screenshots show a phishing website designed to look like the official South Korean postal service website (www.epost.go.kr). The site is hosted on a domain that appears to be a typo-squatting attempt: hxxps://epost-go-kr[.]xyz/#/.

**First Screenshot: Payment Page**  
 The page displays a payment form for a service. The text at the top reads: "온라인 결제 서비스를 위해 일부 서비스 수수료를 부과해야 합니다. 패키지는 결제 후 다시 배송됩니다. 일시불: 389,600₩". Below this, there are input fields for "카드 소지자" (Cardholder), "카드 번호" (Card number, pre-filled with 0000 0000 0000 0000), "만료일" (Expiration date, MM/YY), "보안 코드 (CV)" (Security code, pre-filled with 1234), and "주민등록번호" (Residential registration number). A yellow "계속하다" (Continue) button is at the bottom.

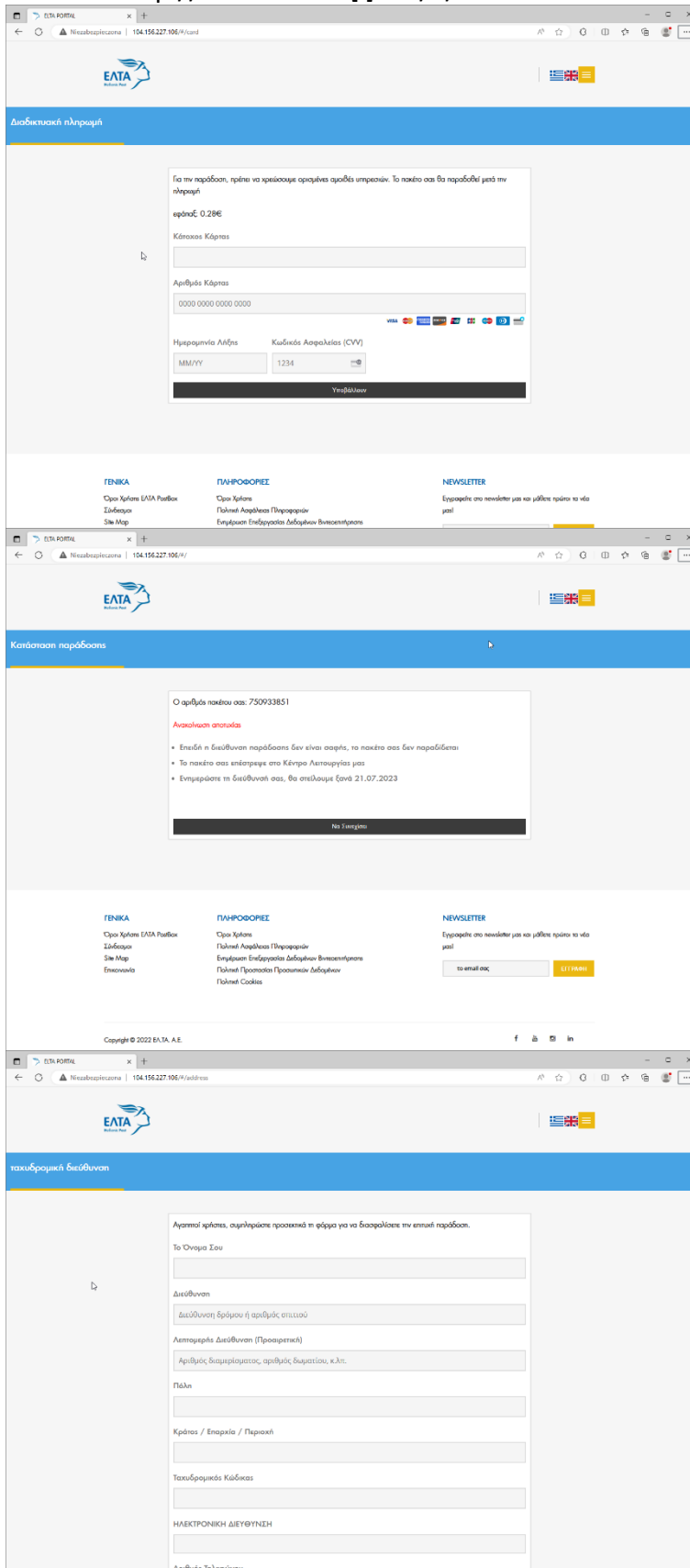
**Second Screenshot: Delivery Status Page**  
 The page shows a "배송 상황" (Delivery Status) notification. The text reads: "패키지 번호: 983493976", "배송 실패 통지" (Delivery failure notice), "배송 주소가 명확하지 않기 때문에 패키지가 전달되지 않습니다. 귀하의 패키지가 운영 센터로 돌아 왔습니다. 주소를 업데이트하십시오. 21.07.2023에 다시 배송합니다." A yellow "계속하다" (Continue) button is at the bottom.

**Third Screenshot: Address Form Page**  
 The page prompts the user to provide their address for delivery. The text reads: "우편 주소 안내하는 사용자 여러분, 성공적인 배송을 위해 양식을 신중하게 작성하십시오." Below this, there are several input fields: "당신의 이름" (Your name), "주소" (Address), "가리 주소 또는 주택 번호" (Apartment address or house number), "자세한 주소 (선택 사항)" (Detailed address (optional)), "이피브 번호, 객실 번호 등" (EPIB number, room number, etc.), "도시" (City), "주/지방/지역" (Province/Region/City), "우편 번호" (Postal code), "이메일" (Email), and "전화 번호" (Phone number). A yellow "즉시 업데이트하십시오" (Update immediately) button is at the bottom.

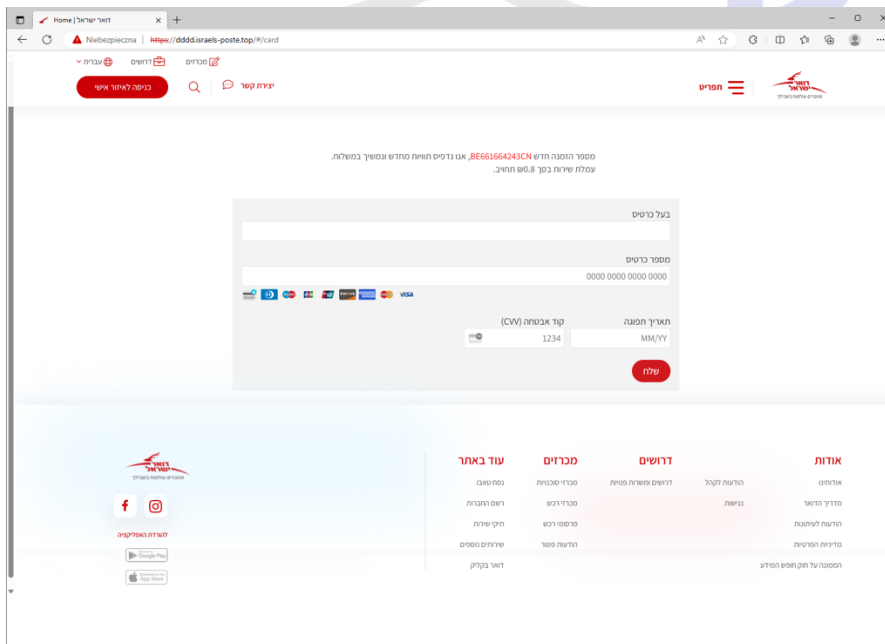
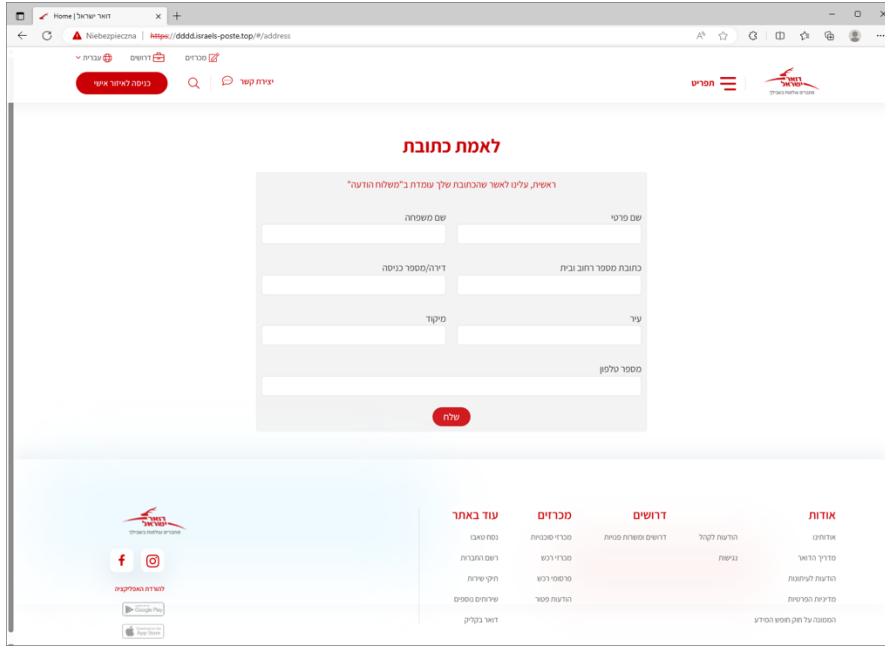




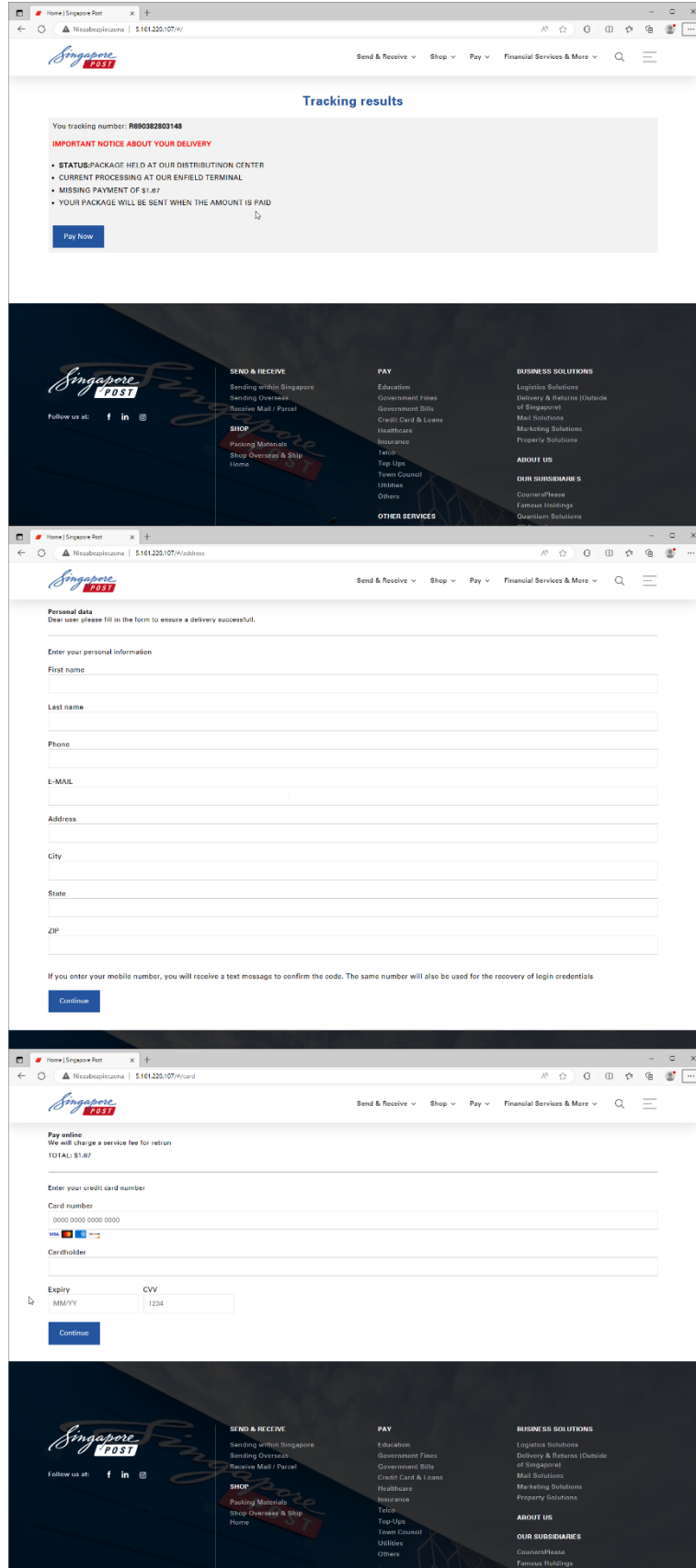
Greece - hxxp://104.156.227[.]106/#/.



### Israel - hxxps://dddd.israels-poste[.]top/#/



### Singapore - hxxp://5.161.220[.]107/#/



KNF  
IRT

Spain - hxxp://149.248.62[.]119/#/.

The image displays three sequential screenshots of the Correos.es website interface. Each screenshot shows the top navigation bar with the logo, 'Particular' and 'Empresa' tabs, a search bar, and an 'INICIAR SESIÓN' button. The first screenshot, titled 'Estado de entrega', shows a delivery status for package number 104890006. It features a red 'Aviso de falla de entrega' (Delivery failure notice) with the following details: 'Debido a que la dirección de entrega no está clara, su paquete no se entrega' (Due to unclear delivery address, your package is not delivered), 'Su paquete ha regresado a nuestro centro de operaciones' (Your package has returned to our operations center), and 'Actualice su dirección, enviaremos nuevamente en 21.07.2023' (Update your address, we will re-ship on 21.07.2023). A yellow 'Continuar' button is visible. The second screenshot, titled 'Dirección de envío' (Shipping address), contains a form with fields for 'Su Nombre', 'DIRECCIÓN', 'Dirección Detallada (Opciones)', 'Ciudad', 'Estado / Provincia / Región', 'Código Postal', 'Correo Electrónico', and 'Número De Teléfono'. A yellow 'Actualizar inmediatamente' button is at the bottom. The third screenshot, titled 'Pago en línea' (Online payment), shows a payment section with a total amount of 0.22€. It includes fields for 'Titular De La Tarjeta', 'Número De Tarjeta', 'Fecha De Expiración', and 'Código De Seguridad (CVV)'. A yellow 'Enviar' button is at the bottom. All three screenshots also feature a sidebar with 'Para ti', 'Para tu empresa', and 'Para tu interés' sections, and social media icons.



### Bolivia - hxxps://posta-hr[.]top/#/

The image displays three screenshots of the AGBC National Tracking Service website. The top screenshot shows the 'Estado de entrega' (Delivery Status) page for package number 403167761. It features the MIENCOMIENDA logo and a map of Bolivia. A red warning message states: 'Aviso de falla de entrega' (Delivery failure notice). The reasons listed are: 'Debido a que la dirección de entrega no está clara, su paquete no se entrega' (Due to unclear delivery address, your package is not delivered), 'Su paquete ha regresado a nuestro centro de operaciones' (Your package has returned to our operations center), and 'Actualice su dirección, enviaremos nuevamente en 21.07.2023' (Update your address, we will resend on 21.07.2023). A 'Continuar' button is visible.

The middle screenshot shows the 'Dirección de envío' (Shipping Address) form. It includes a header with the AGBC logo and social media icons. The form contains several input fields: 'Su Nombre', 'DIRECCIÓN', 'Dirección Detallada (Opcional)', 'Ciudad', 'Estado / Provincia / Región', 'Código Postal', 'Correo Electrónico', and 'Número De Teléfono'. A blue 'Actualizar inmediatamente' button is at the bottom.

The bottom screenshot shows the 'Pago en línea' (Online Payment) page. It features the MIENCOMIENDA logo and a map of Bolivia. A warning message reads: 'ATENCIÓN AMIGOS ESTO ES UN INTENTO DE ESTAFA, POR FAVOR NO COMPLETE TUS DATOS REALES; GRACIAS POR SU ATENCIÓN ESTA PAGINA VA HA SIDO DESMANTELADA -D' (ATTENTION FRIENDS THIS IS A SCAM ATTEMPT, PLEASE DO NOT ENTER YOUR REAL DATA; THANKS FOR YOUR ATTENTION THIS PAGE HAS BEEN DISMANTELED -D). Below this, there are input fields for 'Titular De La Tarjeta', 'Número De tarjeta', 'Fecha De Expiración', and 'Código De Seguridad (CVV)'. A 'Pagar' button is at the bottom.

KNF  
IRT

### DHL Germany - hxxp://208.85.22[.]235/#/

The image displays three sequential screenshots of the DHL Germany website interface. Each screenshot shows the top navigation bar with the DHL logo, 'auch mit!' banner, and links for 'Pakete versenden', 'Pakete empfangen', and 'Hilfe und Kontakt'. The browser address bar consistently shows 'hxxp://208.85.22[.]235/#/'.

- Top Screenshot:** The main content area is titled 'Lieferstatus' (Delivery Status). It displays 'Ihre Paketnummer: 217449142' and a 'Verpackungsweis der Lieferung' (Packaging instructions) section with three bullet points: 'Da die Lieferadresse nicht klar ist, wird ihr Paket nicht geliefert', 'Ihr Paket ist in unser Operation Center zurückschickst', and 'Bitte aktualisieren Sie Ihre Adresse, wir wenden wieder in 31.07.2023 versenden'. A red 'Weitermachen' button is at the bottom.
- Middle Screenshot:** The main content area is titled 'Postanschrift' (Post Address). It includes a warning: 'Sehr geehrte Benutzer, bitte füllen Sie das Formular sorgfältig aus, um die erfolgreiche Lieferung zu gewährleisten.' Below are input fields for 'Ihrer Name', 'Adresse', 'Detaillierte Adresse (Optional)', 'Stadt', 'Stadt / Provinz / Region', 'Postleitzahl', 'Email', and 'Telefonnummer'. A red 'Sofort Aktualisieren' button is at the bottom.
- Bottom Screenshot:** The main content area is titled 'Onlinebezahlung' (Online Payment). It states: 'Für die erneute Lieferung müssen wir einige Servicegebühren erheben. Ihr Paket wird nach Zahlungseingang erneut zugestellt.' Below is a 'Passchaltbep: 0.18' and a 'Kartenzahlung' form with fields for 'Kartenzahl', 'Kartennummer', 'Gültig bis', and 'OW'. A red 'Einzahlen' button is at the bottom.

Each screenshot also features a footer with navigation links for 'Privatkunden', 'Geschäftskunden', 'Unternehmen', and 'Wissenslager', along with a 'Social' section.

KNF  
IRT

DPD Hungary - hxxp://208.85.19[.]234/#/.

The image shows three sequential screenshots of the DPD Hungary website. The top screenshot displays the main page with a navigation menu on the left and a central banner featuring a DPD delivery van and a driver. Below the banner is the 'Kiszállítás állapota' (Delivery status) section, which includes a red 'További' (More) button. The middle screenshot shows a form for tracking or delivery status, with fields for 'Cím' (Address), 'Beküldési cím' (Pickup address), 'Város' (City), 'Állam / Province / Megye' (Country/Province/County), 'Helység' (Locality), 'Email', and 'Telefonszám' (Phone number). The bottom screenshot shows the 'Online fizetés' (Online payment) section, which includes a 'Kártyatartó' (Cardholder) field, a 'Kártyaszám' (Card number) field, a 'Lejárt dátuma' (Expiration date) field, and a 'Biztonsági kód (CVV)' (Security code) field. A red 'Fizetés' (Payment) button is visible at the bottom of this section.

KNF  
IRT

Italy - hxxp://64.176.189[.]221/#/

The screenshot shows three sequential steps of a user's interaction with the Posteitaliane website:

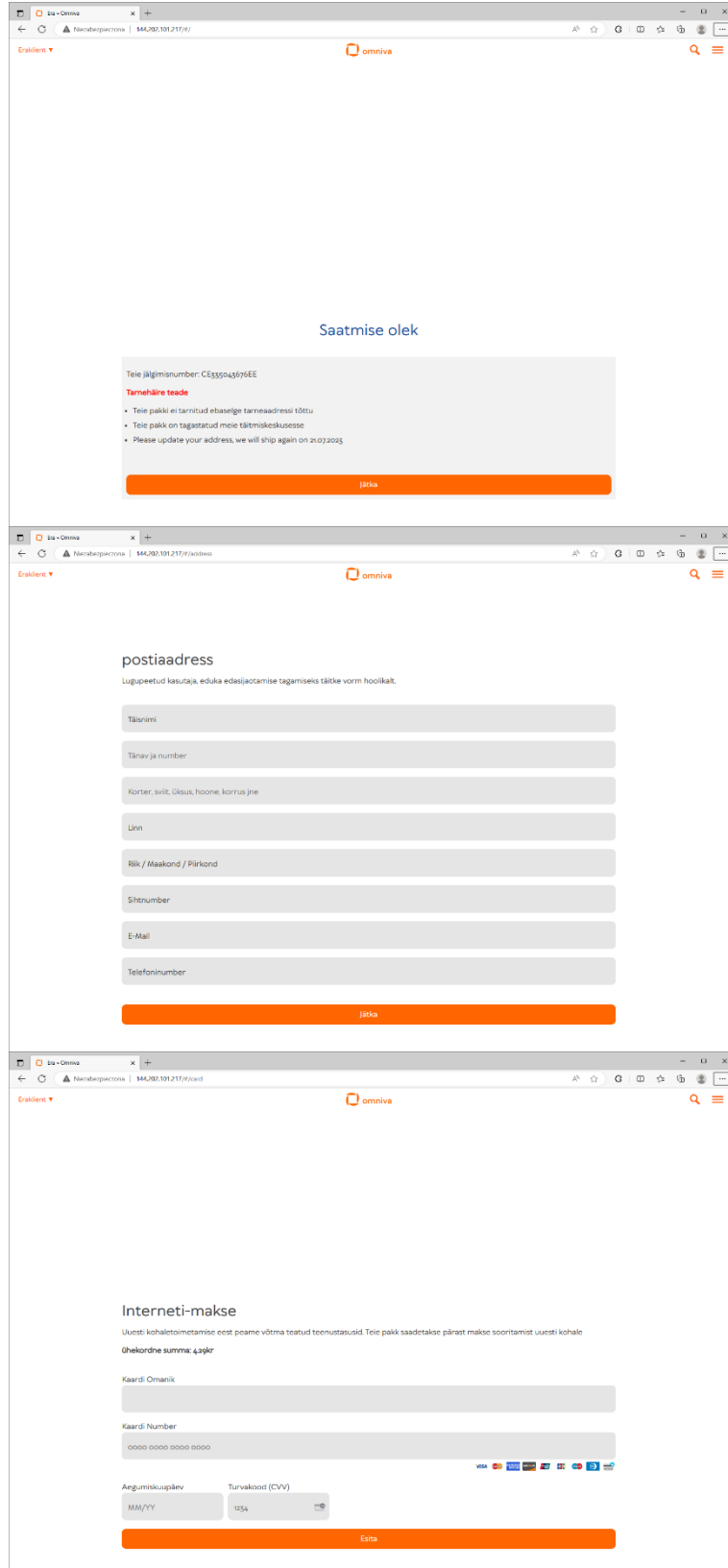
- Step 1: Tracking Search**
  - Search bar: "Cerca Spedizioni"
  - Tracking ID: "XA733227828IT"
  - Service: "POSTEDELIVERY EXPRESS"
  - Status: "stato non disponibile" (status not available)
  - Message: "Se c'è un errore durante il processo di consegna, il destinatario deve essere specificato e l'indirizzo deve essere comunicato e restituito"
  - Progress: "Preso in carico" (checked), "In transito", "In consegna", "Consegnata"
  - Details: "17072023 Presa in carico da Ufficio Postale 0102", "Ufficio Postale Roma 90 di Via Pietro Beloni 130, 00169"
- Step 2: Anagraphic Data Form**
  - Section: "Dati Anagrafici"
  - Instruction: "GENTILE UTENTE, SI PREGA DI COMPILARE IL MODULO PER GARANTIRE UNA CONSEGNA DI SUCCESSO."
  - Fields: "NOME", "COGNOME", "CELLULARE", "E-MAIL", "INDIRIZZO", "CITTA", "PROVINCIA", "POST CODICE"
  - Note: "Se inserisci il tuo numero di cellulare, riceverai un messaggio di testo per confermare il codice. Lo stesso numero verrà utilizzato anche per il recupero delle credenziali di accesso"
  - Button: "PROSEGUI"
- Step 3: Payment Form**
  - Section: "Paga in linea"
  - Text: "PER LA RICONSEGNA, ADDEBITEREMO UNA COMMISSIONE DI SERVIZIO"
  - Total: "TOTALE: €5,90"
  - Fields: "NUMERO DI CARTA", "TITOLARE DELLA CARTA", "DATA DI SCADENZA", "CVV"
  - Button: "PROSEGUI"

The footer of the website includes categories: "OGGETTI DEDICATI", "AREA PERSONALE", "ASSISTENZA", "SERVIZI ONLINE", "LAZIENDA", and "ACCESSIBILITÀ".

KNF  
IRT



## Estonia - hxxp://144.202.101[.]217/#/.



The image displays three sequential screenshots of the Omniva website interface, showing a shipping status page, an address form, and a payment section.

**Top Screenshot: Saamise olek**

Teie jälgimisnumber: CE532043676EE

**Tarnehäire teade**

- Teie pakki ei tarnitud ebaselge tarneaadressi tõttu
- Teie pakki on tagastatud meie täitmiskeskusesse
- Please update your address, we will ship again on 21.07.2023

Jätka

**Middle Screenshot: postiaadress**

Lugupidetud kasutaja, eduka edasijätkamise tagamiseks täitke vorm hoolikalt.

Täisnimi  
Tänav ja number  
Korteri, süliti, üksus, hoone, korrus jne  
Linn  
Riik / Maakond / Piirkond  
Sihtnumber  
E-Mail  
Telefoninumber

Jätka

**Bottom Screenshot: Interneti-makse**

Uuesti kohaletoimetamise eest peame võtma teatud teenustasusid. Teie pakki saadetakse pärast makse sooritamist uuesti kohale

Gheloordne summa: 4,39kr

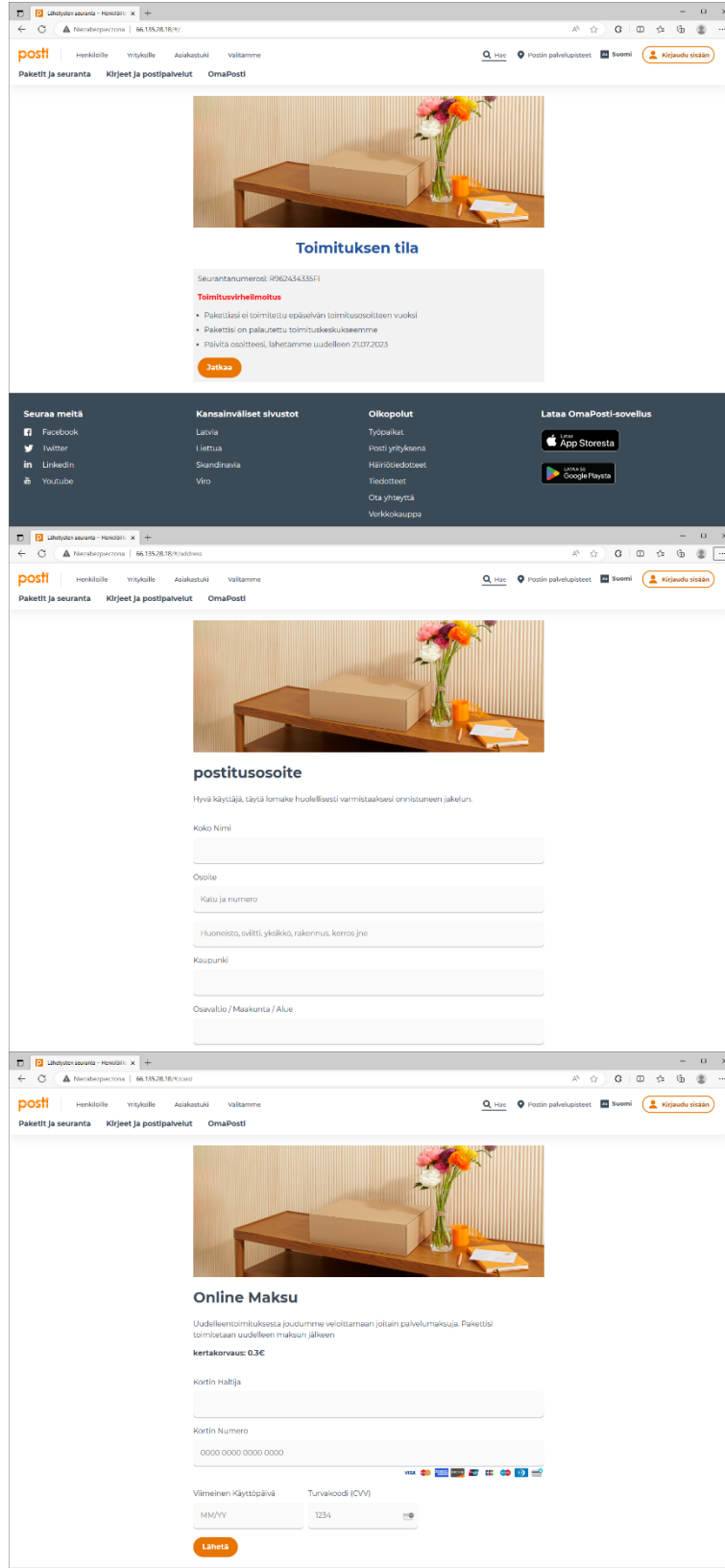
Kaardi Omanik  
Kaardi Number  
0000 0000 0000 0000

Argumisküpslev Turvakood (CVV)  
MM/YY USA

Esita

KNF  
IRT

## Finland - hxxp://66.135.28[.]18/#/



**posti** | Henkilöille | Yrityksille | Asiakastuki | Valittu

Paketti ja seuranta | Kirjeet ja postipalvelut | OmaPosti

### Toimituksen tila

Seurantamääritys: R062434335F1

**Toimitusvirhe ilmoitus**

- Pakettiasi ei toimitettu epäselvään toimitusosoitteeseen vuoksi
- Paketti on palautettu toimituskeskukseemme
- Päivitä osoitteesi, lähettämme uudelleen 21.07.2023

[Jatka](#)

**Seuraa meitä**

- Facebook
- Twitter
- LinkedIn
- YouTube

**Kansainväliset sivustot**

- Latvia
- Iittua
- Skandinavia
- Viro

**Olkopolut**

- Työpaikat
- Posti yrityksenä
- Häiriöilmoitukset
- Tiedotteet
- Ota yhteyttä
- Verkkokauppa

**Lataa OmaPosti-sovellus**

Lataa App Storesta

Lataa Google Playsta

---

**postitusosoite**

Hyvä käyttää, täytä lomake huolellisesti varmistaksesi onnistuneen jakelun.

Koko nimi

Osoite

Katu ja numero

Huoneisto, silityt, yksikkö, rakennus, kerros jne

Kaupunki

Osa-alue / Maakunta / Alue

---

**Online Maksu**

Uudelleen toimituksia joudumme veloittamaan joltain palvelumaksuista. Paketti toimitetaan uudelleen maksun jälkeen.

**hertakorvaus: 0,3€**

Kortin haltija

Kortin Numero

0000 0000 0000 0000

Viimeinen käyttöpäivä: MM/YY | Turvakoodi (CVV): 1234

[Lähetä](#)

KNF  
IRT

# France - hxxps://frpost[.]fr/#/

**Statut de livraison**

Votre numéro de package: 304489740

**Acte de livraison de défaillance**

- Parce que l'adresse de livraison n'est pas claire, votre colis a été refusé
- Votre colis est renvoyé à notre centre d'opérations
- Veuillez mettre à jour votre adresse, nous espérons le recevoir à 21.07.2023

Continuer

**Nos Engagements**

- Proche de vous: Localiser un bureau de poste
- Priorité neutralité carbone
- Paiements 100% sécurisés
- Livraison offerte dès 21€ d'achat: Nos produits marketplace

**Applications la Poste** Trouvez nos applications

**Restons connectés**

**Nos Services**  
Envoyer sans vous déplacer  
Envois importants  
Déménagement, Absence

**Nos Produits**  
Enveloppes  
Timbres  
Emballages

**Nos Tarifs**  
Comparateur de tarifs  
Tarifs postaux 2023 | Catalogue intégral  
Grille de tarifs Courier

**La Poste vous accompagne**  
Aides et contact  
Les avantages de Mon compte La Poste  
Espace sourds et malentendants

**Adresse postale**

Cher utilisateur, veuillez remplir soigneusement le formulaire pour assurer la réussite de la livraison.

Votre Nom

Prénom

Adresse de rue ou numéro de maison

Adresse D'appoint (Optionnel)  
Numéro d'appartement, numéro de chambre, etc.

Ville

Etat / Province / Région

Code Postal

E-Mail

Numéro De Téléphone

Mettez à jour l'attachement

**Paiement en ligne**

Pour une nouvelle livraison, nous devons facturer des frais de service. Votre colis vous sera livré après paiement

montant forfaitaire: 0,27€

Titulaire De La Carte

Numéro De Carte  
0000 0000 0000 0000

Date D'expiration  
MM/YY

Code De Sécurité (CVV)  
1234

Soumettre

**Nos Engagements**

- Proche de vous: Localiser un bureau de poste
- Priorité neutralité carbone
- Paiements 100% sécurisés
- Livraison offerte dès 21€ d'achat: Nos produits marketplace

**Applications la Poste** Trouvez nos applications

**Restons connectés**

**Nos Services**  
Envoyer sans vous déplacer  
Envois importants  
Déménagement, Absence

**Nos Produits**  
Enveloppes  
Timbres  
Emballages

**Nos Tarifs**  
Comparateur de tarifs  
Tarifs postaux 2023 | Catalogue intégral  
Grille de tarifs Courier

**La Poste vous accompagne**  
Aides et contact  
Les avantages de Mon compte La Poste  
Espace sourds et malentendants

### Kuwait - hxxp://208.167.242[.]249/#/.

The image displays three sequential screenshots of the Kuwait Post website (www.kuwaitpost.gov.kw) accessed via a browser. The browser's address bar shows the URL: hxxp://208.167.242[.]249/#/.

- Top Screenshot (Landing Page):** Shows the main navigation menu with links for 'الرئيسية' (Home), 'الخدمات' (Services), 'عن بريد الكويت' (About Kuwait Post), and 'القسمة الثالثة' (Third Quarter). A central banner features a yellow button labeled 'رابط طلب الخدمة' (Service Request Link). Below the banner, there are sections for 'كيف هي خدمتنا؟' (How is our service?), 'خدمات البريد الوارد' (Inbound Mail Services), 'روابط مهمة' (Important Links), and 'البريد الصادر' (Outbound Mail). The Kuwait Post logo and '© بريد الكويت 2023' are visible at the bottom.
- Middle Screenshot (Registration Form):** Titled 'العنوان البريدي' (Postal Address), it contains a form with fields for: 'اسم' (Name), 'عنوان' (Address), 'عنوان الشارع أو رقم الشارع' (Street name or number), 'عنوان مكتب (اختياري)' (Optional office address), 'رقم التذاوير أو الخدمة وما يرتكبه' (Postage number or service and related), 'بلد' (Country), 'البريد الإلكتروني / هاتف' (Email / Phone), 'عنوان بريدي' (Postal address), 'بريد الكويت' (Kuwait Post), and 'رقم هاتف' (Phone number). A yellow 'تسجيل على الموقع' (Register on the site) button is at the bottom.
- Bottom Screenshot (Payment Page):** Titled 'الدفع الإلكتروني' (Online Payment), it shows a form for 'مبلغ الخدمة' (Service amount) with a value of 0.21KD. Below this are fields for 'رقم البطاقة' (Card number) and 'تاريخ الانتهاء' (Expiration date). A yellow 'دفع' (Pay) button is present. The footer includes the Kuwait Post logo and '© بريد الكويت 2023'.



## Luxembourg - hxxp://64.176.192[.]239/#/

# Paraguay - hxxp://155.138.129[.]182/#/.

The image displays three sequential screenshots of the Paraguayan National Post Office website (Direccion Nacional de Correos del Paraguay). The website features a dark blue header with the national coat of arms and the slogan "Paraguay de la gente".

- Top Screenshot:** Shows the "Rastreo de Envíos Internacionales" (International Shipments Tracking) page. It displays the "Estado de entrega" (Delivery Status) for a specific package (number 56510736). The status indicates a delivery failure: "Aviso de falta de entrega" (Notice of missing delivery). The text explains that the delivery address is unclear and the package is not being delivered. It notes that the package has returned to the sender's control and provides the date of the last update: 21.07.2023. A "Continuar" (Continue) button is visible.
- Middle Screenshot:** Shows the "Dirección de envío" (Shipping Address) form. It includes fields for "Su Nombre" (Your Name), "DIRECCIÓN" (Address), "Dirección Detallada (Opcional)" (Detailed Address - optional), "Ciudad" (City), "Estado / Provincia / Región" (State/Province/Region), "Código Postal" (Postal Code), "Correo Electrónico" (Email), and "Número De Teléfono" (Phone Number). A "Notificación Inmediatamente" (Notify Immediately) button is at the bottom.
- Bottom Screenshot:** Shows the "Pago en línea" (Online Payment) section. It states that for the service, users must pay some fees. The total amount is "Pago Único: Gs2178.83". It includes fields for "Titular De La Tarjeta" (Cardholder Name), "Número De Tarjeta" (Card Number), "Fecha De Expiración" (Expiration Date), and "Código De Seguridad (CVV)" (Security Code). A "Comprar" (Buy) button is at the bottom.

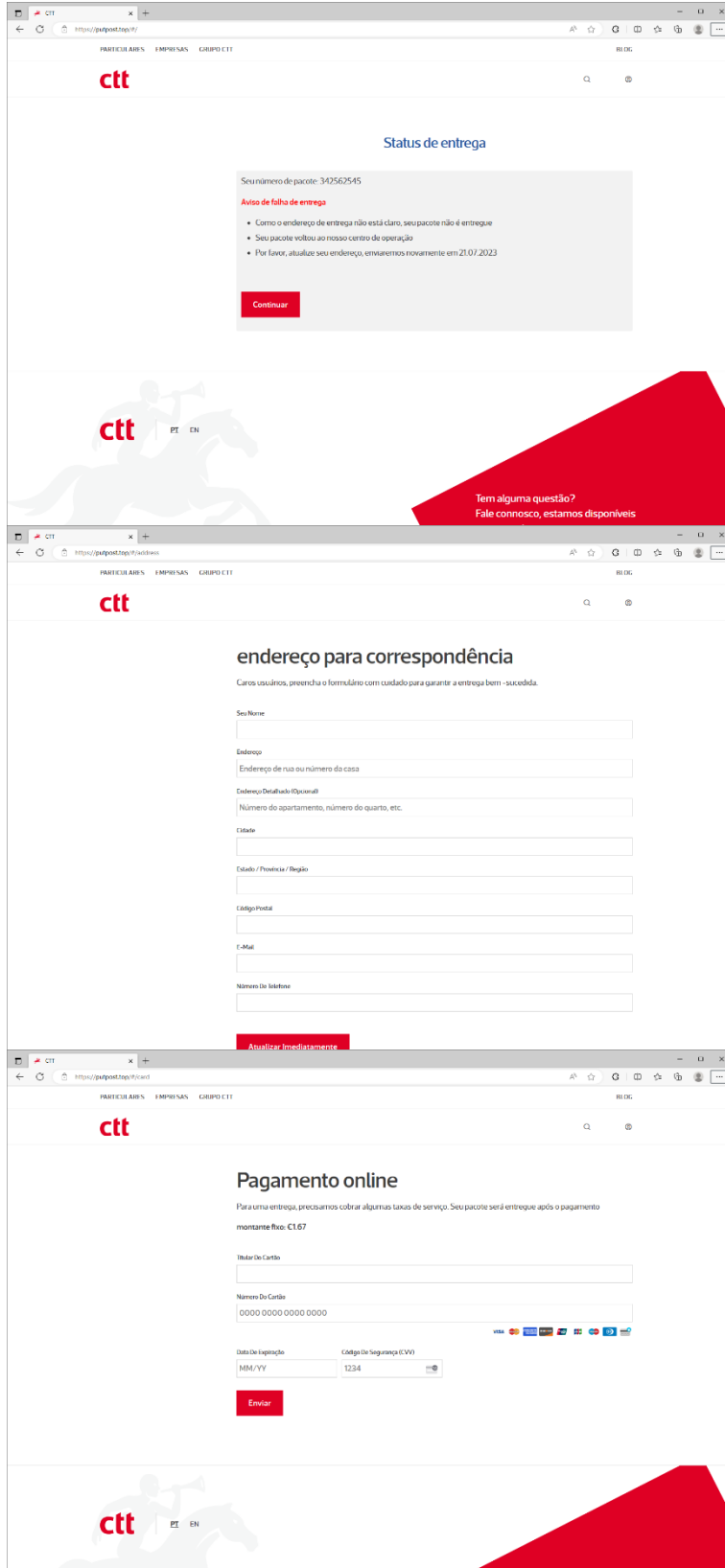
Each screenshot also features a footer with "Enlaces de Interés" (Links of Interest) to various Paraguayan government institutions, including the Secretariat of Social Action (SAS), National Institute of Forestry (INFORNA), National Institute of Information and Communication (SICOM), National Institute of Culture and Arts (INACSA), National Institute of Indigenous Affairs (INAI), National Institute of Statistics and Censuses (INEC), National Institute of Rural Development and Land (INIA), Ministry of Industry and Commerce (MIC), Ministry of Health (MH), and National Institute of Sports (INE).



Poland - hxxps://129.226.159[.]245/#/.



### Portugal - hxxps://www.putpost[.]top/#/





Slovenia - hxxp://137.220.55[.]113/#/

The image displays three sequential screenshots of the Slovenian Post website (Pošta Slovenije) in a browser window. The browser's address bar shows the URL: hxxp://137.220.55[.]113/#/.

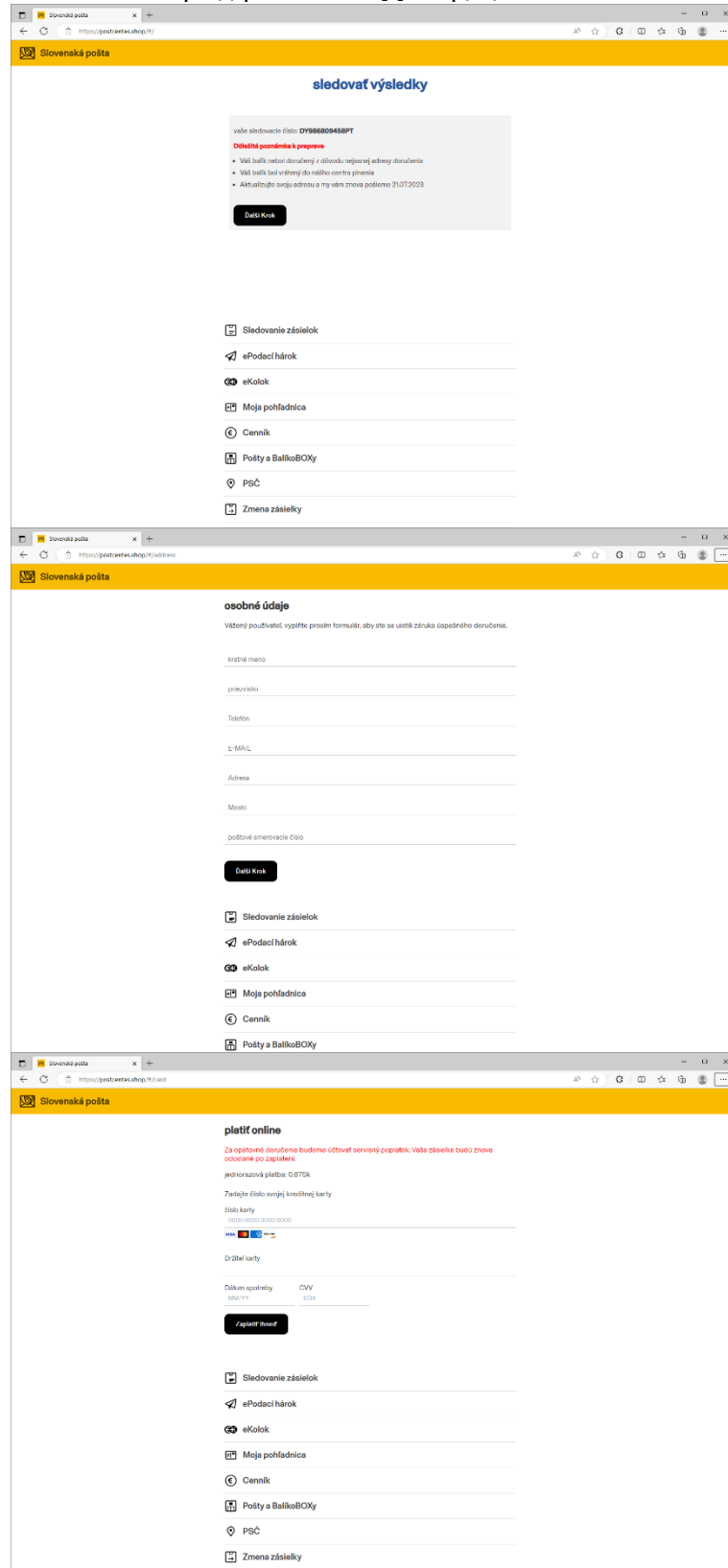
**Top Screenshot:** Shows a notification banner for a parcel (VAŠA SLOVENSKA PAKETA) with a status of 'Čakavostno o napaki o dostavi'. Below the notification is a navigation menu with categories like 'DOMOV', 'POŠTNE STORITVE', 'DENARNE STORITVE', etc. A footer menu includes 'Zasebno', 'Poslovno', 'O nas', and 'Prilpomočki in orodja'.

**Middle Screenshot:** Displays the 'poštni naslov' (mail address) form. It includes fields for 'Tvoje ime', 'Nagovor', 'Podrobni Naslov (Neobvezno)', 'Mesto', 'Zvezna Održava / Provincas / Regija', 'Poštna Štavelka', 'E-Naslov', and 'Telefonska Štavelka'. A 'Takoj Posodobiti' button is at the bottom.

**Bottom Screenshot:** Shows the 'Spletno plačilo' (online payment) form. It includes fields for 'Imetnik Kartice', 'Štavelka Kartice', 'Rok Uporabe', and 'Varnostna Koda (CVV)'. A 'Plačaj' button is at the bottom.



## Slovakia - hxxps://postcentes[.]shop/#/



The image displays three sequential screenshots of the 'Slovenská pošta' website interface, accessed via a browser at the URL https://postcentes.shop/#/.

**Top Screenshot: sledovať výsledky**  
 This section shows tracking information for a specific parcel with ID **DY98680468PT**. A red warning message states: **Dôležitá poznámka k prepravu**. Below the message, there are three bullet points:
 

- Všet balík netočí doručení z dôvodu neznanej adresy doručenia
- Všet balík bol vrátený do nášho centra príjmu
- Aktualizujte svoju adresu a my vám znovu pošleme 21.07.2023

 A **Daťi Knok** button is visible below the text.

**Middle Screenshot: osobné údaje**  
 This section is titled 'osobné údaje' and includes a note: 'Všetny pouzivat, vyplyte prosim formulár, aby ste sa uistili zhrka úspedného doručenia.' Below this, there are several input fields for:
 

- krasné meno
- prírodnisko
- Telefón
- E-MAIL
- Adresa
- Mesto
- poštové smerovacie číslo

 A **Daťi Knok** button is located at the bottom of the form.

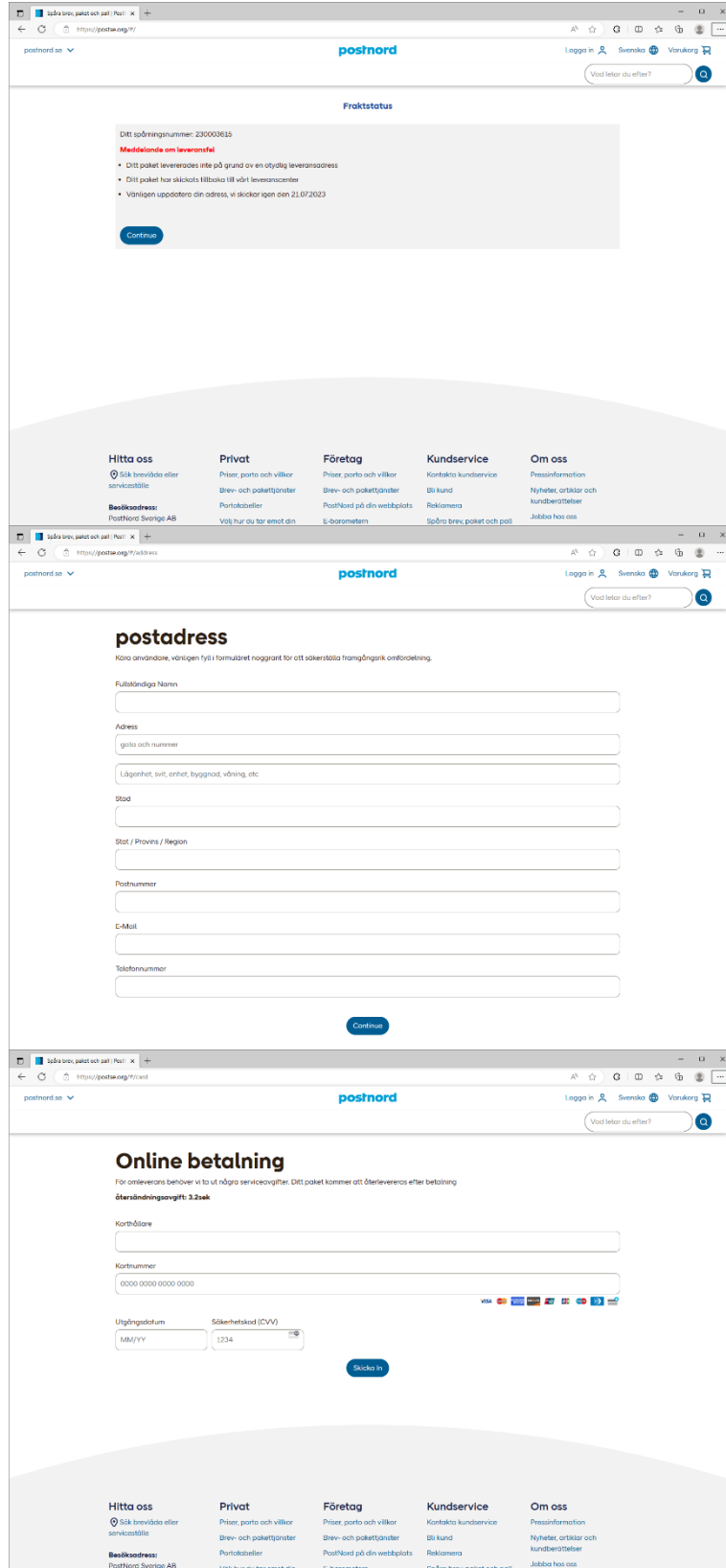
**Bottom Screenshot: platiť online**  
 This section is titled 'platiť online' and contains a red warning: 'Za opoždné doručenie budeme účtovať servisný poplatok. Všet zásielka budú znovu odošlané po zaplášení.' Below this, it shows a one-time payment of **0,975€**. There are fields for:
 

- Zaplášte číslo svojej kreditnej karty
- Číslo karty (XXXXXXXXXXXX)
- Držitel karty
- Dátum spolehlivy (MM/YY) and CVV (ECS)

 A **Zaplášť online** button is at the bottom.

KNF  
IRT

Sweden - hxxps://postse[.]org/#/



The image displays three sequential screenshots of the PostNord website interface:

- Top Screenshot (Fraktstatus):** Shows a shipping status page for order number 230003615. It includes a "Meddelande om leveransfel" (Delivery error message) stating that the package was not delivered due to an incorrect address and will be returned to the sender. A "Continue" button is visible.
- Middle Screenshot (postadress):** Shows a form for entering a postal address. The form includes fields for full name, address (street and number), apartment/unit/building/floor, city, state/province/region, postal code, email, and phone number. A "Continue" button is at the bottom.
- Bottom Screenshot (Online betalning):** Shows an online payment page. It includes a note about service charges, a "Översändningsavgift: 3,25sek" (Forwarding fee: 3.25 SEK), and a form for card payment with fields for cardholder name, card number, expiration date, and security code (CVV). A "Sicka in" (Submit) button is present.

The website footer, visible in all screenshots, contains navigation links for "Hitta oss", "Privat", "Företag", "Kundservice", and "Om oss".

KNF  
IRT

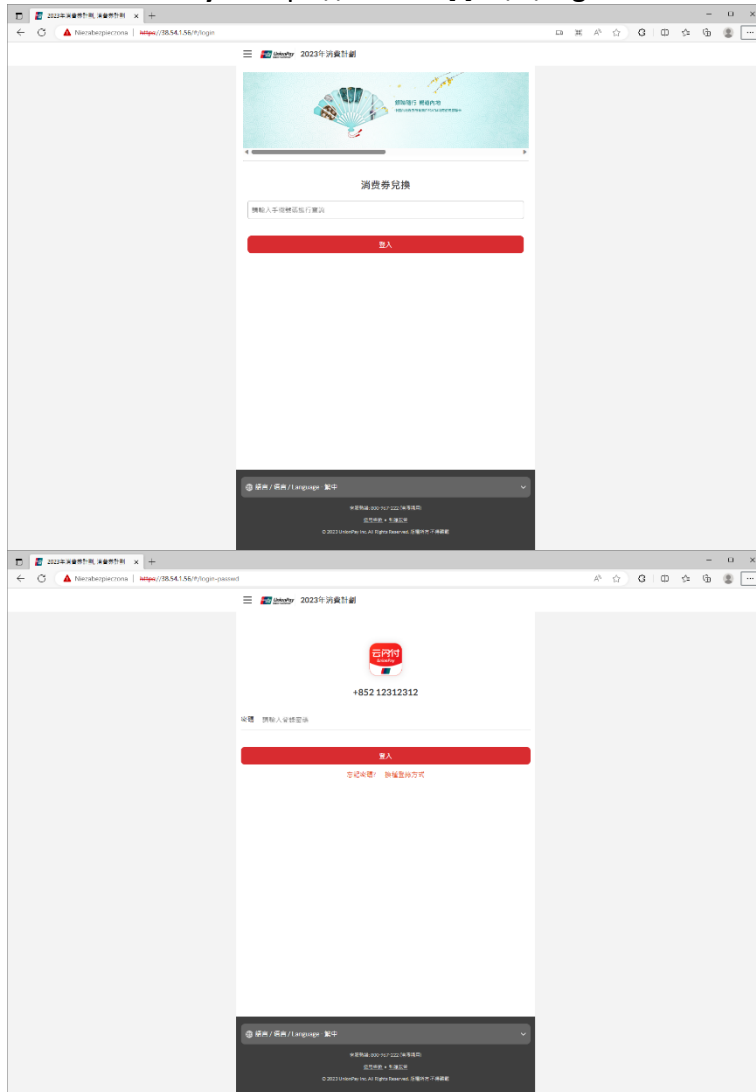
### Turkey - hxxps://45.76.142[.]32/#/

The image shows three sequential screenshots of the PTT Posta Hizmetleri website. The browser address bar in all screenshots is `hxxps://45.76.142.32/#/`.

- Top Screenshot:** Displays the 'Teslim durumu' (Delivery Status) page. It shows a package number '011301965' and a status of 'Teslimat başlandı' (Delivery started). Below this, there are three bullet points: 'Teslimat adresi henüz onaylanmadı, paketlenmiş teslim edilemez', 'Paketiniz Operasyon Merkezi'ne döndü', and 'Lütfen adresinizi güncelleyin, 21.07.2023 de tekrar gönderilecektir'. A 'Detaylı Gör' button is visible.
- Middle Screenshot:** Shows the 'posta adresi' (postal address) form. It includes fields for 'Adınız', 'Adres', 'Ayrıntılı Adres (Bölge - Şehir)', 'Şehir', 'Eyalet / İl / Bölge', 'Posta Kodu', 'E-Posta', and 'İletişim Numarası'. A 'Hemen Gözetle' button is at the bottom.
- Bottom Screenshot:** Shows the 'Online ödeme' (Online payment) section. It states 'Hesabın dağıtım için bakiye hesabını oluşturduktan sonra Paketlenmiş ödeme senaryosunu işlem edebilirsiniz' and 'Tek seferlik ödeme: 7.825'. It features a 'Kart Şanzı' field, a 'Kart Numarası' field with a masked number '0000 0000 0000 0000', and a 'Göndermek' button.

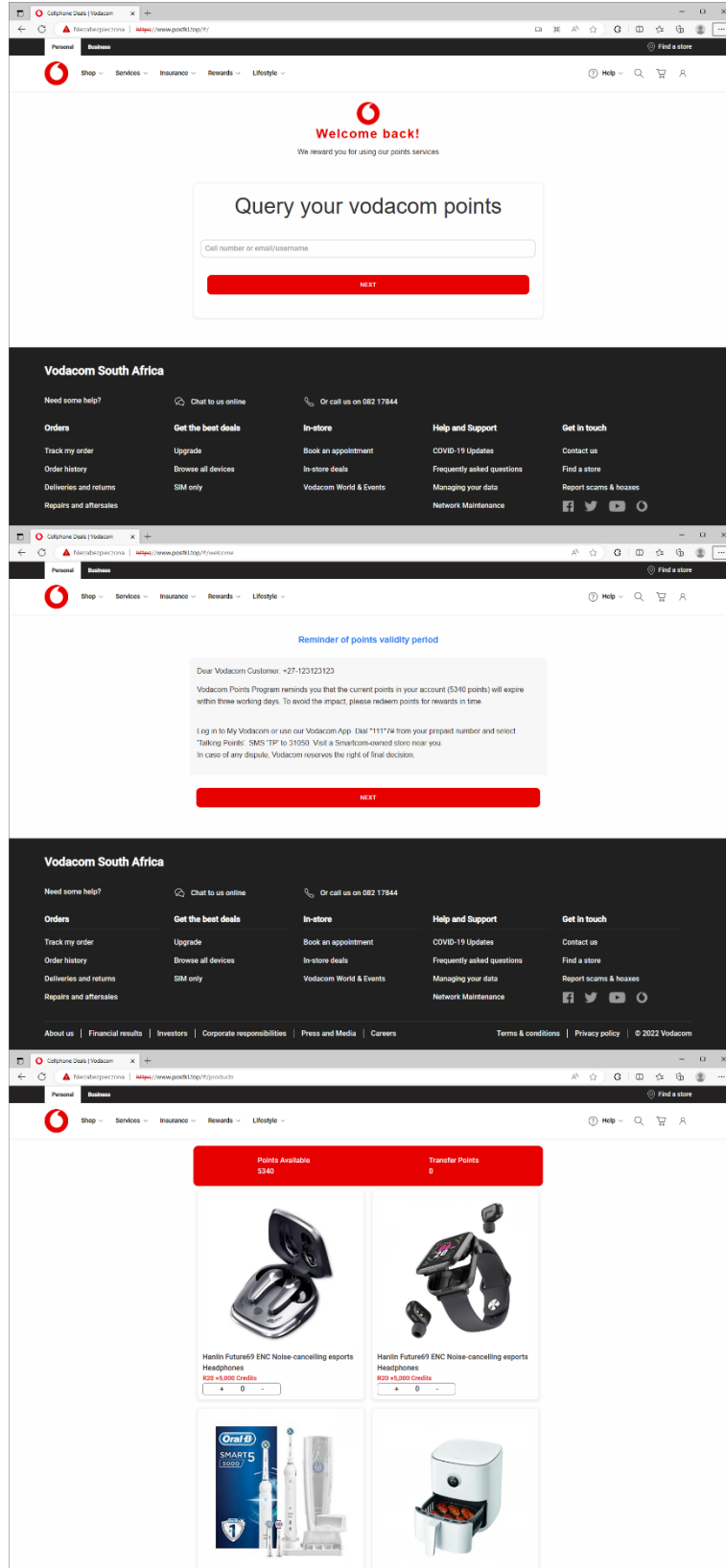


### China UnionPay - hxxps://38.54.1[.]56/#/login

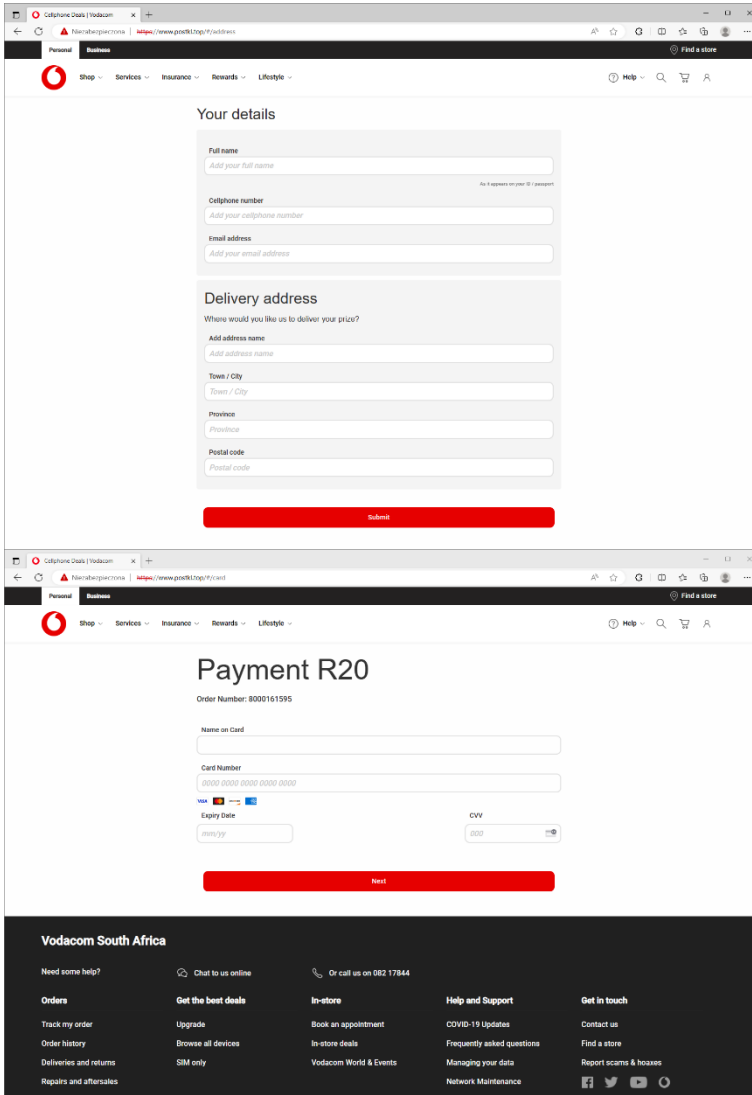


KNF  
IRT

South Africa - hxxps://www.postkl[.]top/#/



KNF  
IRT



C2

IP addresses:

'103.151.111.118',
'103.98.214.162',
'104.129.12.121',
'104.129.5.252',
'104.156.227.106',
'104.156.246.190',
'104.156.249.2',
'104.156.251.78',
'104.156.253.227',
'104.207.128.120',
'104.223.16.73',
'104.238.133.120',
'104.255.175.208',
'104.255.175.222',
'108.61.160.52',
'108.61.33.78',
'114.134.188.253',
'124.223.176.9',
'129.226.159.245',
'137.220.55.113',
'139.180.164.37',
'139.84.226.125',
'139.84.226.99',
'139.84.227.159',
'139.84.233.210',
'139.84.233.31',
'140.82.0.152',
'140.82.30.209',
'140.82.8.101',
'141.164.61.184',
'144.202.0.28',
'144.202.101.217',
'144.202.103.83',
'144.202.114.215',
'144.202.125.124',
'144.202.3.244',
'144.202.4.59',
'144.202.83.235',
'149.248.19.0',

'149.248.62.119',
'149.28.201.221',
'149.28.208.111',
'149.28.226.35',
'149.28.38.126',
'149.28.38.249',
'149.28.43.195',
'149.28.62.146',
'149.28.63.46',
'149.28.71.13',
'149.28.84.225',
'149.28.88.157',
'154.83.13.111',
'154.91.90.199',
'155.138.129.182',
'155.138.139.69',
'155.94.134.184',
'155.94.158.177',
'155.94.177.157',
'155.94.184.138',
'155.94.184.6',
'156.247.14.118',
'156.247.14.86',
'173.82.154.157',
'173.82.154.186',
'173.82.154.189',
'173.82.154.31',
'173.82.154.36',
'173.82.154.72',
'173.82.206.126',
'173.82.206.137',
'173.82.206.196',
'173.82.206.197',
'173.82.206.235',
'173.82.206.249',
'173.82.206.3',
'173.82.206.56',
'173.82.212.178',
'173.82.212.186',



'173.82.212.214',
'173.82.212.215',
'173.82.212.222',
'173.82.212.235',
'173.82.212.252',
'173.82.219.159',
'173.82.219.165',
'173.82.219.213',
'173.82.219.3',
'173.82.219.77',
'173.82.227.117',
'173.82.227.33',
'173.82.232.105',
'173.82.232.212',
'173.82.232.60',
'173.82.235.173',
'173.82.235.191',
'173.82.235.245',
'173.82.240.112',
'173.82.240.130',
'173.82.240.146',
'173.82.240.50',
'173.82.240.87',
'173.82.245.184',
'173.82.245.51',
'173.82.255.152',
'173.82.255.164',
'173.82.255.166',
'173.82.255.167',
'173.82.255.19',
'173.82.255.249',
'173.82.255.43',
'173.82.255.72',
'173.82.255.93',
'192.161.56.19',
'192.227.177.161',
'192.227.177.177',
'192.227.177.179',
'192.227.190.110',
'192.227.190.157',
'195.58.48.175',
'195.58.49.180',
'195.58.49.48',
'198.148.118.153',

'198.148.118.175',
'198.23.174.146',
'198.55.102.75',
'198.55.106.95',
'198.55.122.45',
'204.152.210.108',
'204.44.108.203',
'204.44.108.223',
'204.44.108.224',
'204.44.85.69',
'207.148.28.224',
'207.148.28.49',
'207.246.102.100',
'207.246.105.140',
'207.246.112.85',
'207.246.124.250',
'207.246.126.63',
'207.246.65.116',
'207.246.80.243',
'207.246.94.203',
'207.246.99.46',
'208.167.242.249',
'208.83.236.51',
'208.85.19.234',
'208.85.20.150',
'208.85.22.235',
'208.85.23.97',
'23.94.169.116',
'23.94.169.14',
'23.94.169.144',
'23.94.197.141',
'23.94.199.14',
'23.94.207.106',
'23.94.207.108',
'23.94.207.144',
'23.95.173.174',
'23.95.233.133',
'34.90.241.250',
'38.54.1.56',
'38.54.24.11',
'38.54.27.114',
'38.54.63.125',
'38.54.63.216',
'38.54.94.67',

'38.54.94.83',
'38.60.204.95',
'38.60.216.212',
'38.60.249.15',
'43.130.48.56',
'43.135.178.182',
'43.153.12.103',
'43.157.38.106',
'43.157.39.165',
'45.32.152.87',
'45.32.22.197',
'45.32.55.238',
'45.32.72.244',
'45.32.83.223',
'45.63.14.93',
'45.63.20.123',
'45.63.68.189',
'45.63.71.196',
'45.63.79.223',
'45.63.9.215',
'45.76.13.100',
'45.76.13.243',
'45.76.142.32',
'45.76.2.233',
'45.76.21.156',
'45.76.231.238',
'45.76.253.142',
'45.76.5.187',
'45.76.67.10',
'45.76.70.249',
'45.77.115.221',
'45.77.121.135',
'45.77.158.114',
'45.77.159.65',
'45.77.165.177',
'45.77.165.36',
'45.77.189.75',
'45.77.193.130',
'45.77.194.130',
'45.77.201.71',
'45.77.204.98',
'47.251.16.77',
'47.251.17.155',

'47.254.42.42',
'47.88.106.114',
'47.89.195.232',
'47.89.213.32',
'47.91.67.82',
'5.161.220.107',
'64.112.43.162',
'64.112.43.202',
'64.176.189.221',
'64.176.192.239',
'64.176.192.45',
'64.176.194.62',
'64.176.198.134',
'64.176.199.164',
'64.176.199.196',
'64.176.199.198',
'64.176.199.201',
'64.176.199.205',
'64.176.199.216',
'64.176.199.225',
'64.176.51.66',
'65.20.96.205',
'66.135.10.5',
'66.135.11.84',
'66.135.12.242',
'66.135.13.93',
'66.135.15.90',
'66.135.17.176',
'66.135.18.112',
'66.135.21.194',
'66.135.23.137',
'66.135.25.163',
'66.135.28.18',
'66.135.29.131',
'66.135.29.53',
'66.135.5.56',
'66.135.7.245',
'66.42.105.67',
'66.42.107.46',
'66.42.127.93',
'67.219.97.186',
'95.179.224.112'

**Domains:**

'an-post.xyz',
'anpost-track.top',
'atpost.pro',
'ausposts.net',
'autopase.top',
'autopass-no.cc',
'autopass.bio',
'autopassno-top.top',
'autopassno.top',
'avantrawr.shop',
'bahrainpost.top',
'bpost-be.top',
'bpost.vip',
'ceskaposta.top',
'chl-correos.top',
'chl-pose-server.top',
'chl-poster-track.top',
'chl-postese-track.top',
'chl-postets-track.top',
'chl-postse-track.top',
'coles--au.shop',
'coles-au.co',
'coleş.com',
'correo.monster',
'correos-cl.cc',
'correos-cl.services',
'correos-cr.top',
'correos-es.mom',
'correos-help.xyz',
'correos-poster.xyz',
'correos-zl.net',
'correos.boats',
'correos.pics',
'correos.wang',
'correosbolivia.top',
'correosccc.top',
'correoscl.buzz',
'correosclo.top',
'correosgob.buzz',
'correogocr.co',
'correoso.top',
'correoss.online',

'cri-poste-server.top',
'cri-poster-track.top',
'cypruspost-post.services',
'de-posts-dhl.top',
'dhighpu.xyz',
'dpd-hu.top',
'e1t5bpf2.com',
'eeporstee.com',
'eeposte.net',
'elta-help.top',
'elta-new.top',
'elta-news.top',
'elta-post.top',
'eltagr.monster',
'eltagr.one',
'eltagr.top',
'enposta.top',
'epost-go-kr.xyz',
'etc-jp-nexco-etc.top',
'foodnew.top',
'foodpandatw.top',
'frpost.fr',
'georgianpost.top',
'govuk.top',
'grupoice.vip',
'hellotoby.top',
'hk-shell.top',
'hrpost.co',
'ias516fb.com',
'idme.red',
'instanthq.com',
'israeipost.top',
'israel-posts.top',
'israele-posts.top',
'israelp-post.top',
'israelpostoffice.top',
'israels-poste.top',
'jordanpost.top',
'kaz-kazpster.top',
'kddi-au.top',
'krtopaes.top',
'krtopasoet.top',

'krtopeote-track.top',
'krtopessoe-track.top',
'kuwaitpost.top',
'luhg8p7a.com',
'moc-gov.world',
'nfipz.top',
'norddk.com',
'norwaypass.co',
'nrod.top',
'omniva.top',
'omnivaee.top',
'omnivaee.xyz',
'omnivai.xyz',
'open-rice-serice.top',
'open-rich.top',
'package-tracking.top',
'plpsc.top',
'mail-poland.one',
'polskapl.top',
'posindonesia.top',
'posnaf.top',
'post-ag.live',
'post-at.art',
'post-en.top',
'post-hr.top',
'post-news.top',
'post-office.life',
'post-server.top',
'post-t.ink',
'post-t.wiki',
'post-track-at.top',
'posta-hr.co',
'posta-hr.top',
'posta-hu.xyz',
'posta-romana.vip',
'posta-server.top',
'posta-service.top',
'posta-tracking.top',
'posta.cyou',
'posta.wang',
'postag.ws',
'postahr.buzz',
'postahu.top',
'postalparcel.info',

'postask.buzz',
'postasw.xyz',
'postcentes.cyou',
'postcentes.icu',
'postcentes.shop',
'postcentes.xyz',
'postcentres.cloud',
'postcentres.pw',
'postcentres.shop',
'postcolombia.co',
'postcorihu.top',
'postcorihu.xyz',
'poste-at.top',
'post-it.services',
'poste-server.top',
'poste-track.top',
'poste-tracking.top',
'poste-tracks.top',
'postea-si.top',
'postea-track.top',
'poster-track.xyz',
'postifi.life',
'postifi.top',
'postkl.top',
'postlu.life',
'postnl.cyou',
'postnord-se.xyz',
'postnord.store',
'postnorddk-top.top',
'postof.top',
'postoffice-za.club',
'postoffice.lol',
'postofficeco.one',
'postpy.io',
'posts.cyou',
'postse.org',
'postslovakia.co',
'postta.top',
'postta.xyz',
'pposte-it.xyz',
'pptchek.top',
'psza.life',
'ptt-govtr.com',
'ptt-tr.top',

'ptt.monster',
'pttgovtr.top',
'putpost.top',
'qantaspoints.top',
'resubmito.top',
'scsmhd.com',
'se-postnord.top',
'se-sond.top',
'se-sond.xyz',
'se.postnord.top',
'sgphlpp.com',
'shoppe-verify-login.com',
'shoppeetw.co',
'skpost.shop',
'softbank-payment.com',
'son.postnord.top',
'sonpostnord.se',
'startselects.com',
'streamliner.co',
'sudapost.sd',
'suisseposte.top',
'swisspostpostch.buzz',
'ti-post.co',
'ti-post.top',
'tr-post.xyz',
'traveloka.cyou',
'traveloka.vip',
'tt-posts-track.top',
'ukrposhta.buzz',
'ukrposhta.vip',
'ukrposhta.world',
'ups-us.xyz',
'waws.top',
'wwwpostnordse.top',
'xn--80a7a.com',
'xn--b1alh8a.xn--p1ai',
'xn--b1av.xn--p1ai',
'xn--b1av.xn--80a7a.com',
'xn--d1abj.com',
'xn--d1abj.xn--p1ai',
'xn--d1abj1a.com',
'xn--d1abj1a.xn--p1ai',
'xn--e1akcn.com',
'xn--e1akcn.xn--p1ai',

'xn--k1afg.com',
'xn--k1afg.xn--p1ai',
'xn--k1afg1a.com',
'xn--k1afg1a.xn--p1ai',
'xn--l1adba.xn--p1ai',
'xn--m1aag.com',
'xn--m1aag.xn--p1ai',
'xn--m1adg.com',
'xn--m1adg.xn--p1ai',
'xn--p1ai.xn--80a7a.com',
'xn--p1ai.xn--b1alh8a.xn--p1ai',
'xn--p1ai.xn--b1av.xn--p1ai',
'xn--p1ai.xn--d1abj.com',
'xn--p1ai.xn--d1abj.xn--p1ai',
'xn--p1ai.xn--d1abj1a.com',
'xn--p1ai.xn--d1abj1a.xn--p1ai',
'xn--p1ai.xn--e1akcn.com',
'xn--p1ai.xn--e1akcn.xn--p1ai',
'xn--p1ai.xn--k1afg.com',
'xn--p1ai.xn--k1afg.xn--p1ai',
'xn--p1ai.xn--k1afg1a.com',
'xn--p1ai.xn--k1afg1a.xn--p1ai',
'xn--p1ai.xn--l1adba.xn--p1ai',
'xn--p1ai.xn--m1aag.com',
'xn--p1ai.xn--m1aag.xn--p1ai',
'xn--p1ai.xn--m1adg.com',
'xn--p1ai.xn--m1adg.xn--p1ai',
'yemenpost.top',
'za-post.top',
'za-poste.xyz',
'za-postoffice.xyz',
'za-postserve.xyz'