Report | September 2025

The Postal-Courier Con:

Inside the World's Largest Postal & Courier Scam Campaigns

CTM360®

INDUSTRY
All

COUNTRY
All

REGION
All

DATE
03-09-2025

OVERVIEW :

Global postal and courier phishing scams continue to multiply, exploiting the trust and urgency associated with postal and courier services worldwide. CTM360 actively monitors and detects a wide range of global scam campaigns, including postal and courier scams. **Over the past three months, CTM360 has identified more than 50,000 fraudulent URLs targeting 48 different postal and courier brands worldwide. We continue to record daily detections impacting the top global brands in this sector, underscoring how frequently these scams are being deployed against the industry.**

However, these findings likely represent only the tip of the iceberg. With the scalability of modern phishing kits and the advanced evasion techniques employed by threat actors, the true volume of active scam URLs is far greater. Based on our analysis, we extrapolate that the problem could extend into the hundreds of thousands of scam URLs, highlighting the significant and growing threat faced by postal and courier services globally.

This report breaks down the campaign into two primary categories: International and National Postal & Courier Scams, highlighting the scam stages, distribution channels, templates used, technical observations.

Key Findings

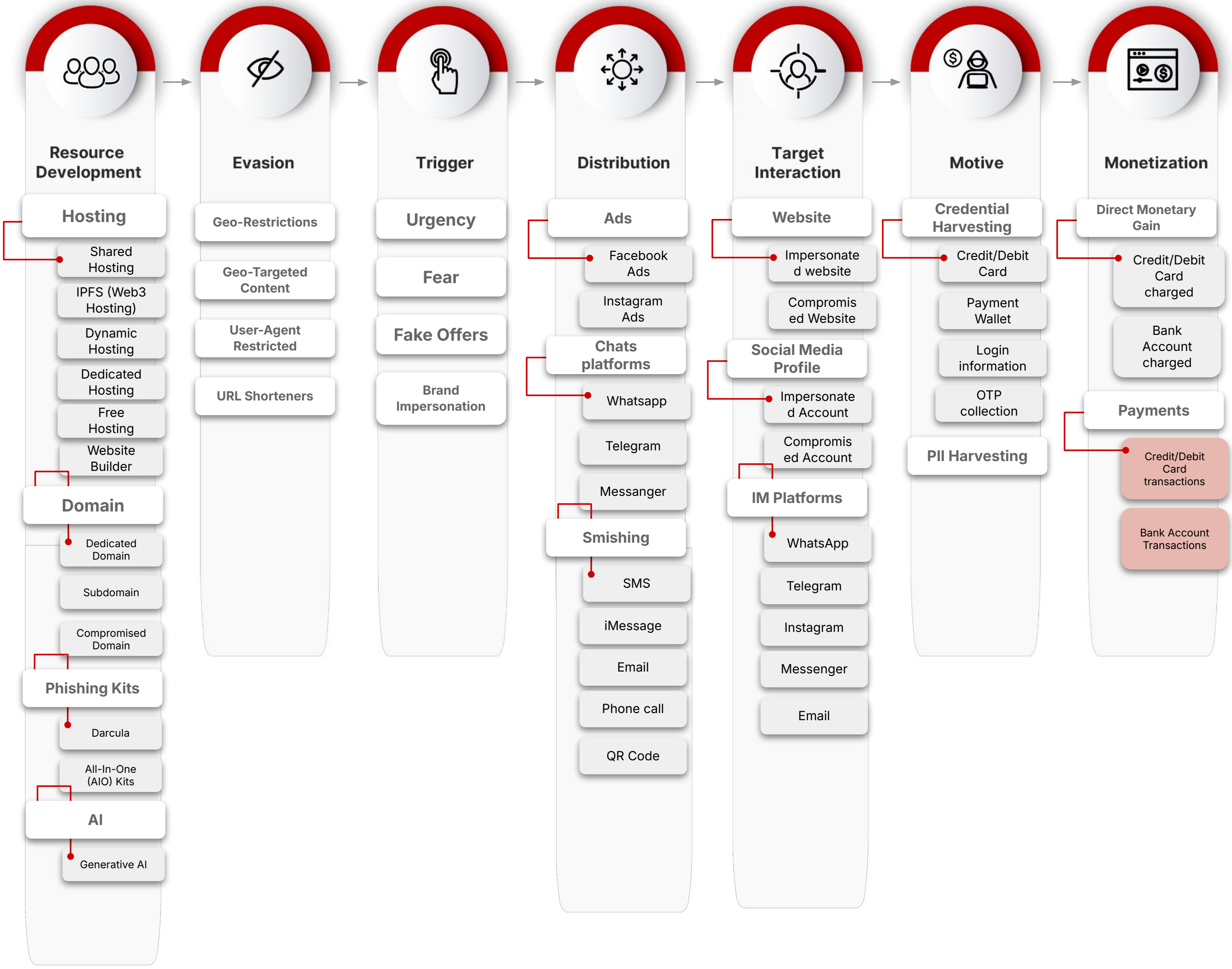
- CTM360 has detected over **50,000+** Global Postal and Courier Scams in the last three months, with nearly equal distribution targeting both international and national brands worldwide.
- Use of **PhaaS platforms like Darcula** significantly lowers the barrier to entry for cybercriminals, enabling mass customization and multi-language phishing forms.
- **Smishing via RCS and iMessage** protocols bypasses traditional SMS filters, enhancing delivery success rates.
- Anti-monitoring techniques (bot redirection, cloaking) and dynamic phishing site updates frustrate takedown efforts.
- International postal & courier brands like DHL, UPS, and Aramex are consistently impersonated. National-level scams are tailored to local languages, postal brands, and users.
- Real-time data exfiltration, cloaking, and GenAI-driven page generation amplify threat effectiveness.

SCAM STAGES:

CTM360 Scam Navigator

CTM360 Scam Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the scam. Scam Navigator is a tool that categorizes common scam techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies seven key stages in a scam: resource development, Evasion, trigger, distribution, target interaction, motive, and monetization. There are commonly 2 phases in the scam, represented as Phase 1 (in grey) & Phase 2 (in light red).

This Scam Navigator has been mapped to this Scam campaign, providing insight into the scam's lifecycle and shedding light on the techniques, entry points, and attack objectives. By breaking down the scam across these stages, the framework enables a clearer understanding of how these campaigns evolve and where defenses can be most effectively applied.



Resource Development
- Hosting
  - Shared Hosting
  - IPFS (Web3 Hosting)
  - Dynamic Hosting
  - Dedicated Hosting
  - Free Hosting
  - Website Builder
- Domain
  - Dedicated Domain
  - Subdomain
  - Compromised Domain
- Phishing Kits
  - Darcula
  - All-In-One (AIO) Kits
- AI
  - Generative AI

Evasion
- Geo-Restrictions
- Geo-Targeted Content
- User-Agent Restricted
- URL Shorteners

Trigger
- Urgency
- Fear
- Fake Offers
- Brand Impersonation

Distribution
- Ads
  - Facebook Ads
  - Instagram Ads
- Chats platforms
  - Whatsapp
  - Telegram
  - Messanger
- Smishing
  - SMS
  - iMessage
  - Email
  - Phone call
  - QR Code

Target Interaction
- Website
  - Impersonated website
  - Compromised Website
- Social Media Profile
  - Impersonated Account
  - Compromised Account
- IM Platforms
  - WhatsApp
  - Telegram
  - Instagram
  - Messenger
  - Email

Motive
- Credential Harvesting
  - Credit/Debit Card
  - Payment Wallet
  - Login information
  - OTP collection
- PII Harvesting

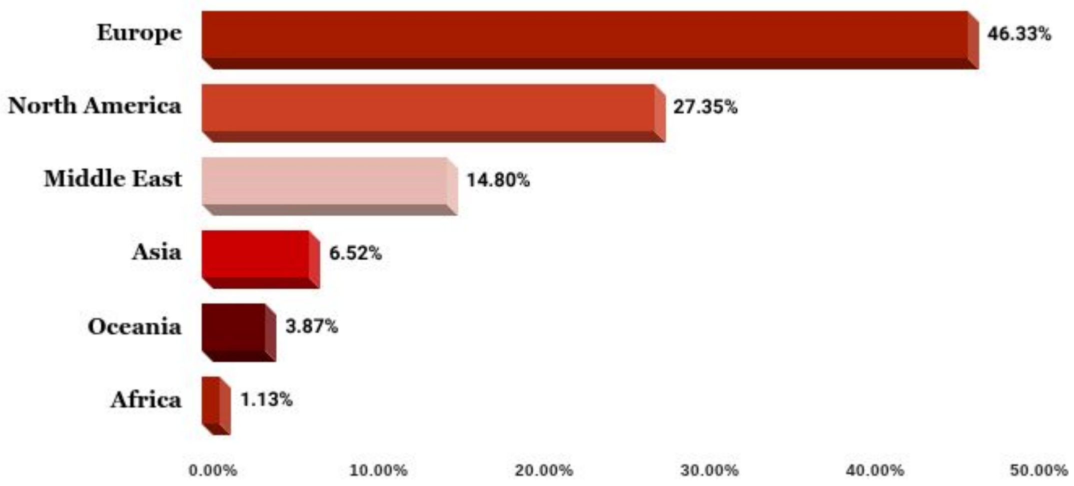
Monetization
- Direct Monetary Gain
  - Credit/Debit Card charged
  - Bank Account charged
- Payments
  - Credit/Debit Card transactions
  - Bank Account Transactions

Targeted Regions Distribution

*The graph below illustrates the **Global Postal and Courier scams** detections by region over the past three months, targeting 48 distinct brands.*

Global Postal & Courier Scam

Breakdown of Postal & Courier Scam Incidents Across Regions



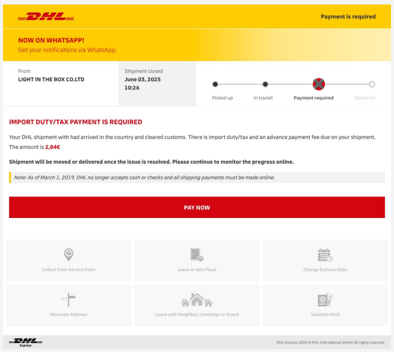
***Note:** The data presented above is approximate, based on current analysis, and is expected to increase over time.*

Top 3 Targeted Postal & Courier Brands (International & National)

International Postal & Courier Brands	National Postal & Courier Brands
DHL Express	USPS
UPS	Australia Post
Aramex	Singapore Post Limited

CTM360 Observations

The screenshots below showcase sample templates of the **international postal & couriers** being targeted globally.



NOW ON WHATSAPP!
Get your notifications via WhatsApp.

From
LIGHT IN THE BOX CO.LTD

Shipment closed
June 03, 2025
10:26

IMPORT DUTY/TAX PAYMENT IS REQUIRED

Your DHL shipment with had arrived in the country and cleared customs. There is import duty/tax and an advance payment fee due on your shipment. The amount is **2,84€**

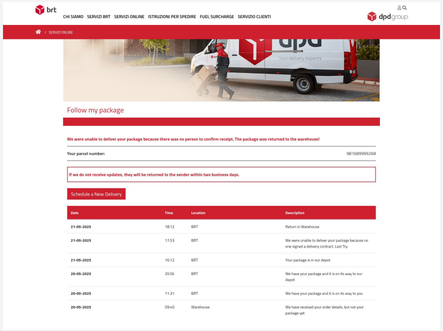
Shipment will be moved or delivered once the issue is resolved. Please continue to monitor the progress online.

Note: As of March 1, 2019, DHL no longer accepts cash or checks and all shipping payments must be made online.

PAY NOW

DHL Express 2025 © DHL International GmbH. All rights reserved.

DHL



Follow my package

We were unable to deliver your package because there was no person to confirm receipt. The package was returned to the warehouse!

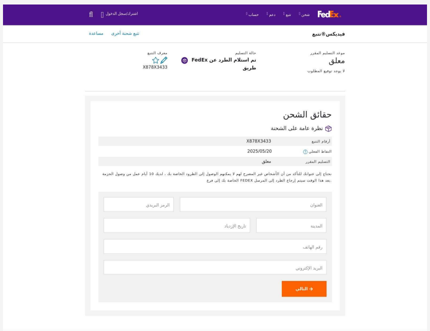
Your parcel number: 981689999268

If we do not receive updates, they will be returned to the sender within two business days.

Schedule a New Delivery

Date	Time	Location	Description
21-05-2025	18:12	BRT	Return in Warehouse
21-05-2025	17:53	BRT	We were unable to deliver your package because no one signed a delivery contract. Last Try.
21-05-2025	16:12	BRT	Your package is in our depot
20-05-2025	20:56	BRT	We have your package and it is on its way to our depot
20-05-2025	11:31	BRT	We have your package and it is on its way to you
20-05-2025	09:40	Warehouse	We have received your order details, but not your package yet

DPD



فيديكس® تتبع

موعد التسليم المقرر
معلق
لا يوجد توقيع المطلوب

حالة التسليم
تم استلام الطرد عن طريق FedEx

معرف التتبع
X878X3433

حقائق الشحن

نظرة عامة على الشحنة

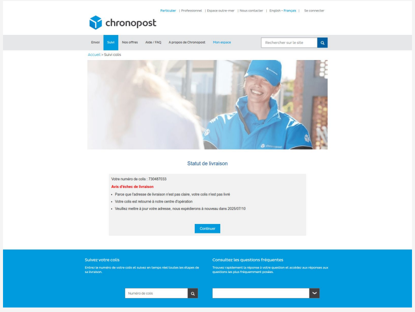
أرقام التتبع	X878X3433
التقاط الفعلي	2025/05/20
التسليم المقرر	معلق

نحتاج إلى عنوانك للتأكد من أن الأشخاص غير المصرح لهم لا يمكنهم الوصول إلى الطرود الخاصة بك ، لديك 10 أيام عمل من وصول الحزمة
.بعد هذا الوقت سيتم إرجاع الطرد إلى المرسل FEDEX الخاصة بك إلى فرع

العنوان
الرمز البريدي
المدينة
تاريخ الإزدياد
رقم الهاتف
البريد الإلكتروني

التالي ←

FedEx



Statut de livraison

Votre numéro de colis : 730487033

Avis d'échec de livraison

- Parce que l'adresse de livraison n'est pas claire, votre colis n'est pas livré
- Votre colis est retourné à notre centre d'opération
- Veuillez mettre à jour votre adresse, nous expédierons à nouveau dans 2025/07/10

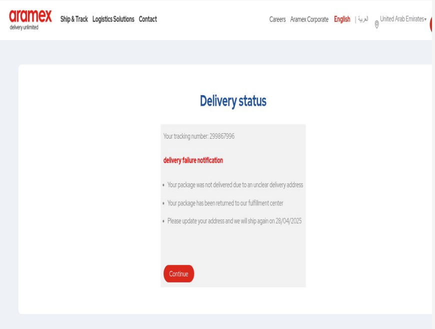
Continuer

Suivez votre colis
Entrez le numéro de votre colis et suivez en temps réel toutes les étapes de sa livraison.

Consultez les questions fréquentes
Trouvez rapidement la réponse à votre question et accédez aux réponses aux questions les plus fréquemment posées.

Numéro de colis

Chronopost



Delivery status

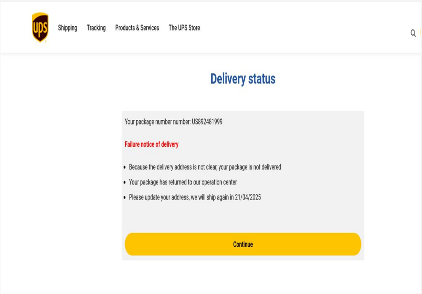
Your tracking number: 299867996

delivery failure notification

- Your package was not delivered due to an unclear delivery address
- Your package has been returned to our fulfillment center
- Please update your address and we will ship again on 28/04/2025

Continue

Aramex



Delivery status

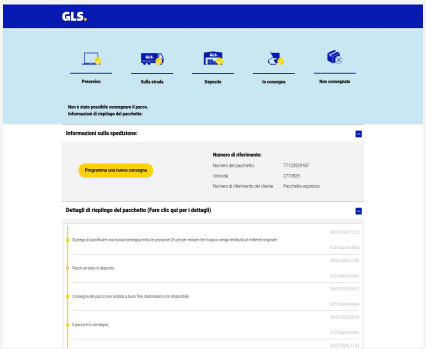
Your package number number: US892481999

Failure notice of delivery

- Because the delivery address is not clear, your package is not delivered
- Your package has returned to our operation center
- Please update your address, we will ship again in 21/04/2025

Continue

UPS



Non è stato possibile consegnare il pacco.
Informazioni di riepilogo del pacchetto:

Informazioni sulla spedizione:

Programma una nuova consegna

Numero di riferimento:

Numero del pacchetto:	77123529187
Unicode:	2773825
Numero di riferimento del cliente:	Pacchetto espresso

Dettagli di riepilogo del pacchetto (Fare clic qui per i dettagli)

28/07/2025 12:25
Si prega di pianificare una nuova consegna entro le prossime 24 ore per evitare che il pacco venga restituito al mittente originale.
GLS Express Italia

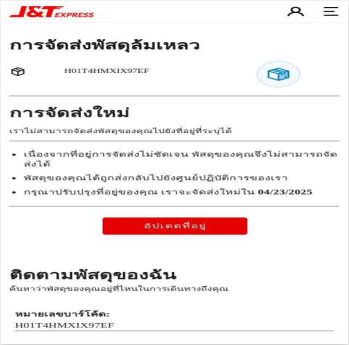
28/07/2025 11:03
Pacco arrivato in deposito.
GLS Express Italia

28/07/2025 09:37
Consegna del pacco non andata a buon fine, destinatario non disponibile.
GLS Express Italia

28/07/2025 08:00
Il pacco è in consegna.
GLS Express Italia

25/07/2025 17:03

GLS



การจัดส่งพัสดุล้มเหลว

H01T4HMXIX97EF

การจัดส่งใหม่

เราไม่สามารถจัดส่งพัสดุของคุณไปยังที่อยู่ที่ระบุได้

- เนื่องจากที่อยู่การจัดส่งไม่ชัดเจน พัสดุของคุณจึงไม่สามารถจัดส่งได้
- พัสดุของคุณได้ถูกส่งกลับไปยังศูนย์ปฏิบัติการของเรา
- กรุณาปรับปรุงที่อยู่ของคุณ เราจะจัดส่งใหม่ใน **04/23/2025**

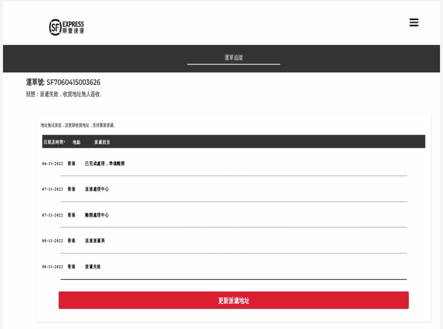
อัปเดตที่อยู่

ติดตามพัสดุของฉัน

ค้นหาว่าพัสดุของคุณอยู่ที่ไหนในการเดินทางถึงคุณ

หมายเลขบาร์โค้ด:
H01T4HMXIX97EF

J&T Express



運單號: SF7060415003626

狀態：派遞失敗，收貨地址無人簽收.

地址無法派送，請更新收貨地址，安排重新派遞。

日期及時間	地點	派遞狀況
06-11-2022	香港	已完成處理，準備離開
07-11-2022	香港	送達處理中心
07-11-2022	香港	離開處理中心
08-11-2022	香港	送達派遞局
08-11-2022	香港	派遞失敗

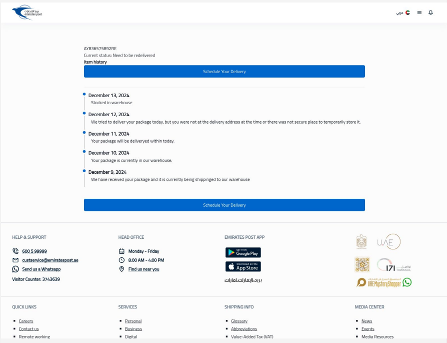
更新派遞地址

SF Express

International Postal & Courier Scam Templates

CTM360 Observations

The screenshots below showcase sample templates of the **national postal & couriers** being targeted globally.



AYB36575892RE
Current status: Need to be redelivered
Item history

Schedule Your Delivery

- December 13, 2024
  Stocked in warehouse
- December 12, 2024
  We tried to deliver your package today, but you were not at the delivery address at the time or there was not secure place to temporarily store it.
- December 11, 2024
  Your package will be deliveryed within today.
- December 10, 2024
  Your package is currently in our warehouse.
- December 9, 2024
  We have received your package and it is currently being shippinged to our warehouse

Schedule Your Delivery

HELP & SUPPORT
600 5 99999
custservice@emiratespost.ae
Send us a Whatsapp
Visitor Counter: 3743639

HEAD OFFICE
Monday - Friday
8:00 AM - 4:00 PM
Find us near you

EMIRATES POST APP
بريد-الإمارات.امارات

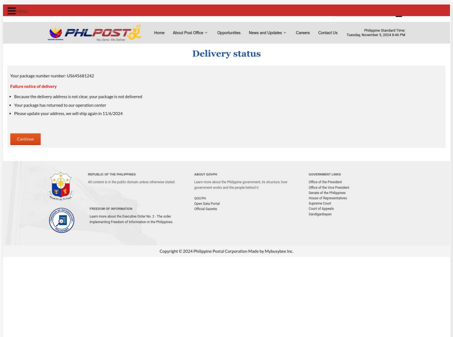
QUICK LINKS
- Careers
- Contact us
- Remote working

SERVICES
- Personal
- Business
- Digital

SHIPPING INFO
- Glossary
- Abbreviations
- Value-Added Tax (VAT)

MEDIA CENTER
- News
- Events
- Media Resources

Emirates Post



MENU
Home | About Post Office | Opportunities | News and Updates | Careers | Contact Us
Philippine Standard Time:
Tuesday, November 5, 2024 8:46 PM

Delivery status

Your package number number: US645681242

Failure notice of delivery
- Because the delivery address is not clear, your package is not delivered
- Your package has returned to our operation center
- Please update your address, we will ship again in 11/6/2024

Continue

REPUBLIC OF THE PHILIPPINES
All content is in the public domain unless otherwise stated.

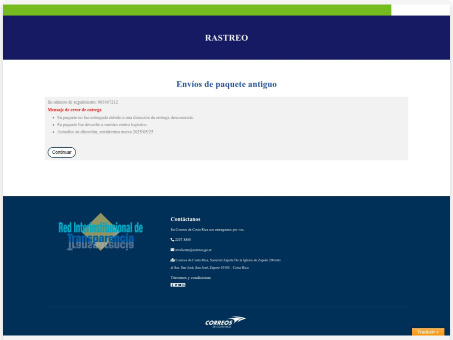
FREEDOM OF INFORMATION
Learn more about the Executive Order No. 2 - The order implementing Freedom of Information in the Philippines.

ABOUT GOVPH
Learn more about the Philippine government, its structure, how government works and the people behind it.
GOV.PH
Open Data Portal
Official Gazette

GOVERNMENT LINKS
Office of the President
Office of the Vice President
Senate of the Philippines
House of Representatives
Supreme Court
Court of Appeals
Sandiganbayan

Copyright © 2024 Philippine Postal Corporation Made by Mybusybee Inc.

Philippine Postal (PHLPost)



RASTREO

Envíos de paquete antiguo

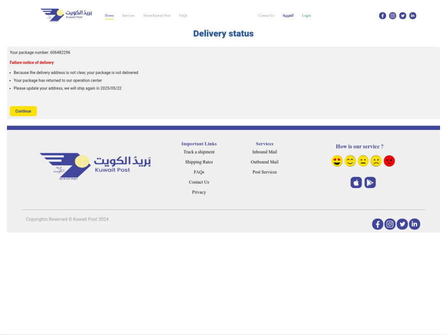
Su número de seguimiento: 003887212
Mensaje de error de entrega
- Su paquete no fue entregado debido a una dirección de entrega desconocida.
- Su paquete fue devuelto a nuestro centro logístico.
- Actualice su dirección, enviáremos nueva 2025/05/25

Continuar

Contáctanos
En Correos de Costa Rica nos entregamos por vos.
2257-8888
srvcliente@correos.go.cr
Correos de Costa Rica, Sucursal Zapote De la Iglesia de Zapote 200 mts al Sur. San José, San José, Zapote 10105 - Costa Rica
Términos y condiciones

Traducir »

Costa Rica



Home Services About Kuwait Post FAQs Contact Us العربية Login

Delivery status

Your package number: 606482296

Failure notice of delivery
- Because the delivery address is not clear, your package is not delivered
- Your package has returned to our operation center
- Please update your address, we will ship again in 2025/05/22

Continue

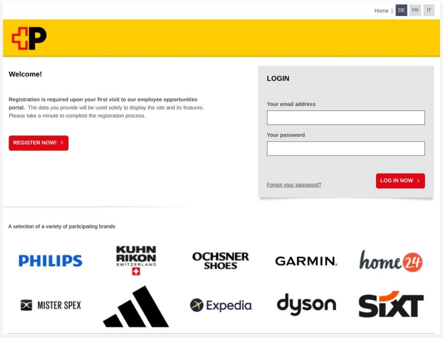
Important Links
Track a shipment
Shipping Rates
FAQs
Contact Us
Privacy

Services
Inbound Mail
Outbound Mail
Post Services

How is our service ?

Copyrights Reserved © Kuwait Post 2024

Kuwait Post



Home | DE FR IT

Welcome!

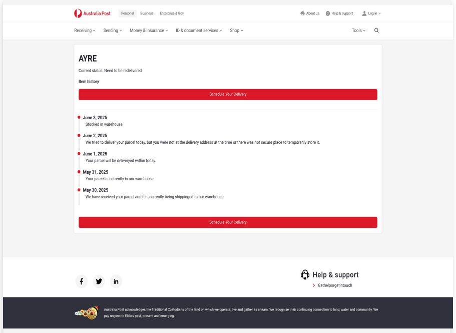
Registration is required upon your first visit to our employee opportunities portal. The data you provide will be used solely to display the site and its features. Please take a minute to complete the registration process.

REGISTER NOW! >

LOGIN
Your email address
Your password
Forgot your password?
LOG IN NOW >

A selection of a variety of participating brands

Swiss Post



Personal Business Enterprise & Gov About us Help & support Log in
Receiving Sending Money & insurance ID & document services Shop Tools

AYRE
Current status: Need to be redelivered
Item history

Schedule Your Delivery

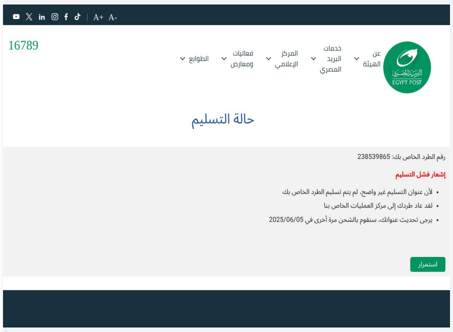
- June 3, 2025
  Stocked in warehouse
- June 2, 2025
  We tried to deliver your parcel today, but you were not at the delivery address at the time or there was not secure place to temporarily store it.
- June 1, 2025
  Your parcel will be deliveryed within today.
- May 31, 2025
  Your parcel is currently in our warehouse.
- May 30, 2025
  We have received your parcel and it is currently being shippinged to our warehouse

Schedule Your Delivery

Help & support
Gethelporgetintouch

Australia Post acknowledges the Traditional Custodians of the land on which we operate, live and gather as a team. We recognise their continuing connection to land, water and community. We pay respect to Elders past, present and emerging.

Australia Post



A+ A-

16789

عن الهيئة | خدمات البريد المصري | المركز الإعلامي | فعاليات ومعارض | الطوابع

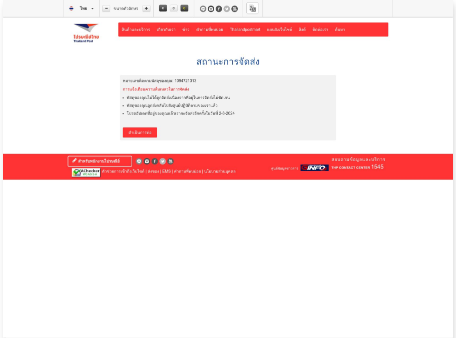
حالة التسليم

رقم الطرد الخاص بك: 238539865

إشعار فشل التسليم
- لأن عنوان التسليم غير واضح، لم يتم تسليم الطرد الخاص بك
- لقد عاد طردك إلى مركز العمليات الخاص بنا
- يرجى تحديث عنوانك، سنقوم بالشحن مرة أخرى في 2025/06/05

استمرار

Egypt Post



ไทย ขนาดตัวอักษร

สินค้าและบริการ | เกี่ยวกับเรา | ข่าว | คำถามที่พบบ่อย | Thailandpostmart | แผนผังเว็บไซต์ | ลิงค์ | ติดต่อเรา | ค้นหา

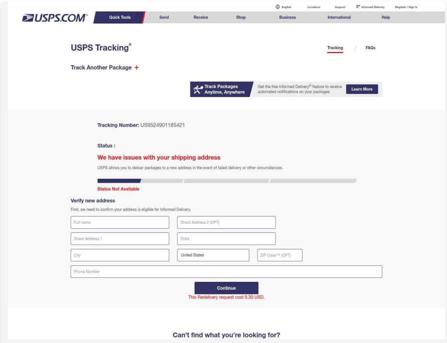
สถานะการจัดส่ง

หมายเลขติดตามพัสดุของคุณ: 1094721313
การแจ้งเตือนความล้มเหลวในการจัดส่ง
- พัสดุของคุณไม่ได้ถูกจัดส่งเนื่องจากที่อยู่ในการจัดส่งไม่ชัดเจน
- พัสดุของคุณถูกส่งกลับไปยังศูนย์ปฏิบัติการของเราแล้ว
- โปรดอัปเดตที่อยู่ของคุณแล้วเราจะจัดส่งอีกครั้งในวันที่ 2-8-2024

ดำเนินการต่อ

สำหรับพนักงานไปรษณีย์
ตัวช่วยการเข้าถึงเว็บไซต์ | ส่งของ | EMS | คำถามที่พบบ่อย | นโยบายส่วนบุคคล
สอบถามข้อมูลและบริการ
ศูนย์ข้อมูลข่าวสาร THP CONTACT CENTER 1545

Thailand Post



English Locations Support Informed Delivery Register / Sign In
USPS.COM Quick Tools Send Receive Shop Business International Help

USPS Tracking®
Tracking / FAQs
Track Another Package +

Track Packages Anytime, Anywhere — Get the free Informed Delivery® feature to receive automated notifications on your packages — Learn More

Tracking Number: US9524901185421

Status :
We have issues with your shipping address
USPS allows you to deliver packages to a new address in the event of failed delivery or other circumstances.

Status Not Available

Verify new address
First, we need to confirm your address is eligible for Informed Delivery.

Full name	Street Address 2 (OPT)	
Street Address 1	State	
City	United States	ZIP Code™ (OPT)
Phone Number		

Continue
This Redelivery request cost 0.30 USD.

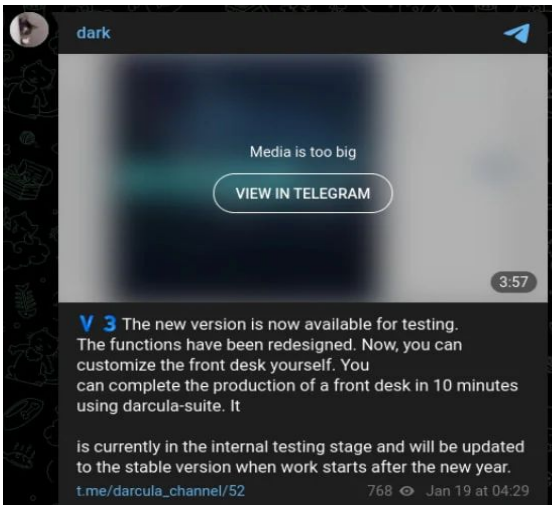
Can't find what you're looking for?

USPS

National Postal & Courier Scam Templates

CTM360 Observations - Resource Development

The foundation of global postal & courier phishing scams is built during the resource development phase, where threat actors develop modular, scalable infrastructure designed for mass-targeted campaigns with minimal friction. Central to this phase is phishing kits and a popular phishing kit used for this scams is the **Darcula Suite**, a phishing-as-a-service (PhaaS) toolkit advertised across Telegram channels. It offers a no-code, drag-and-drop interface enabling even novice users to clone phishing pages for brands like USPS, FedEx, DHL within minutes.



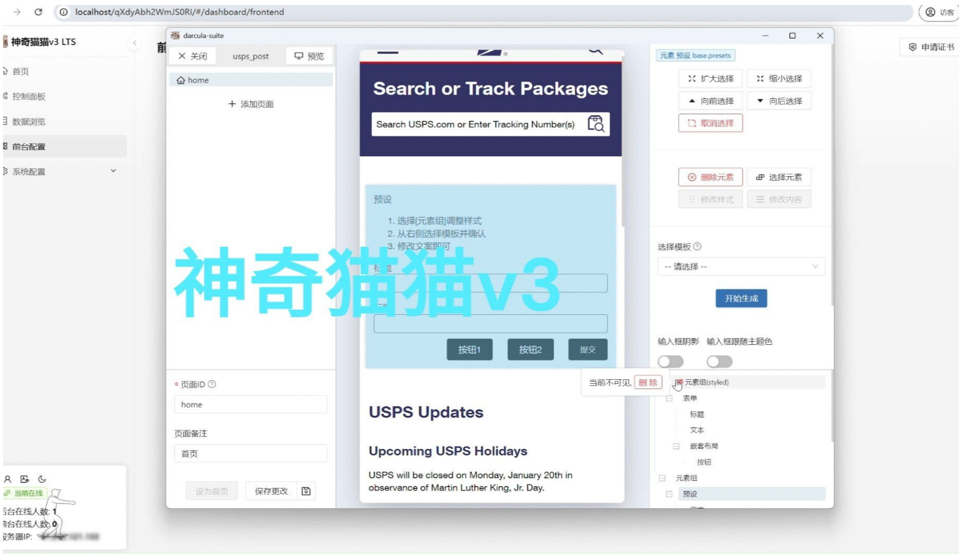
V 3 The new version is now available for testing.
The functions have been redesigned. Now, you can customize the front desk yourself. You
can complete the production of a front desk in 10 minutes using darcula-suite. It

is currently in the internal testing stage and will be updated to the stable version when work starts after the new year.

t.me/darcula_channel/52 768 Jan 19 at 04:29

Darcula V3.0 Telegram Announcement

Actors can fully clone a courier tracking portal and embed credential harvesting forms tailored for desktop, Android, or iOS. Internally, actors test these kits with a level of discipline resembling agile development, often staging edits and refinements before public deployment.



Search or Track Packages

Search USPS.com or Enter Tracking Number(s)

预设

1. 选择[元素组]调整样式
2. 从右侧选择模板并确认
3. 修改文案即可

USPS Updates

Upcoming USPS Holidays

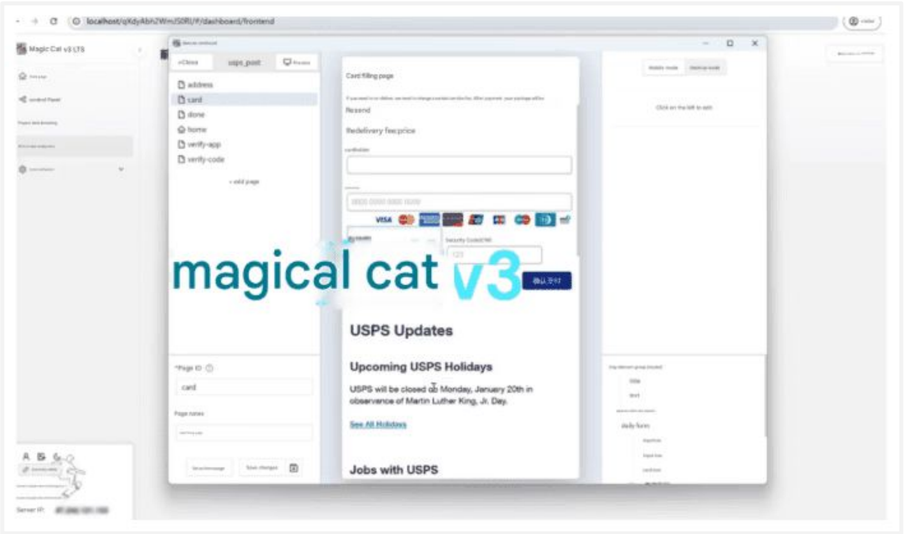
USPS will be closed on Monday, January 20th in observance of Martin Luther King, Jr. Day.

USPS interface in Dracula editor

While Darcula is widely used in **Global Postal Phishing Scams**, its reach extends further. CTM360 has identified its use in other campaigns such as **Pointy Phish and Toll Shark.** Darcula's flexibility allows attackers to seamlessly shift between sectors like Postal, telecom, banking, and government, all while maintaining pixel-perfect impersonation.

CTM360 Observations - Resource Development

To support real-time exploitation, actors embed tools like **Magic Cat v3**, which captures credentials, OTPs, and session cookies live as victims interact with phishing forms, enabling immediate account takeovers or resets.



localhost/qXdyAbh2WmJS0RU/#/dashboard/frontend

Magic Cat v3 LTS

usps_post

- address
- card
- done
- home
- verify-app
- verify-code

+ add page

Card filling page

Resend

Redelivery fee:price

magical cat v3

USPS Updates

Upcoming USPS Holidays

USPS will be closed on Monday, January 20th in observance of Martin Luther King, Jr. Day.

See All Holidays

Jobs with USPS

*Page ID

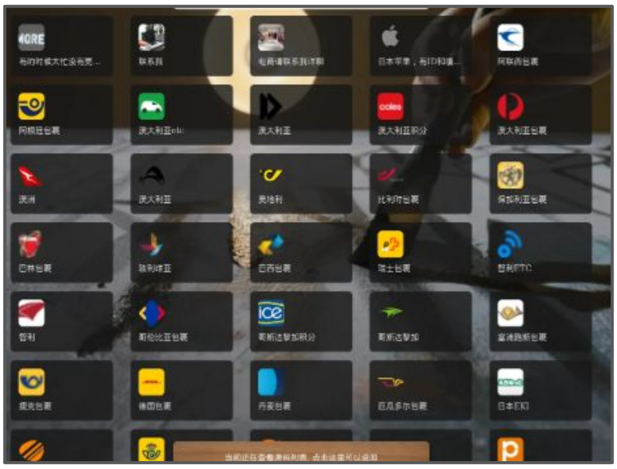
card

Page notes

An injected credit card form, with some of the text machine-translated into English. (Source: Netcraft)

These phishing pages are deployed on domains registered to look convincingly similar to legitimate shipping companies. Threat actors rely on domain shadowing, typosquatting, and homoglyph tricks (e.g., using "**usps.support-track[.]com**" instead of "usps.com") to lure victims.

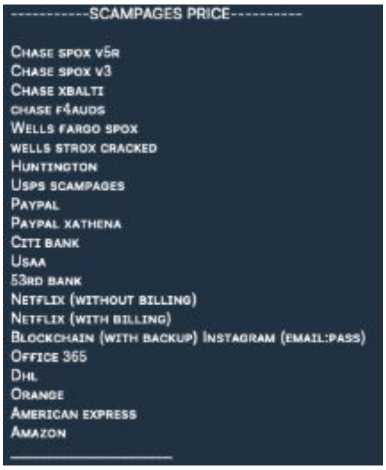
While **Darcula V2** was already effective, it relied on pre-built phishing kits tailored to specific brands, offering over 200 templates across more than 100 countries. The latest version, **Darcula V3**, introduces a more flexible approach, allowing attackers to easily customize and rebrand phishing campaigns to target virtually any organization.



darcula V2 phishing templates (Source: Oshri Kalfon)

CTM360 Observations - Resource Development

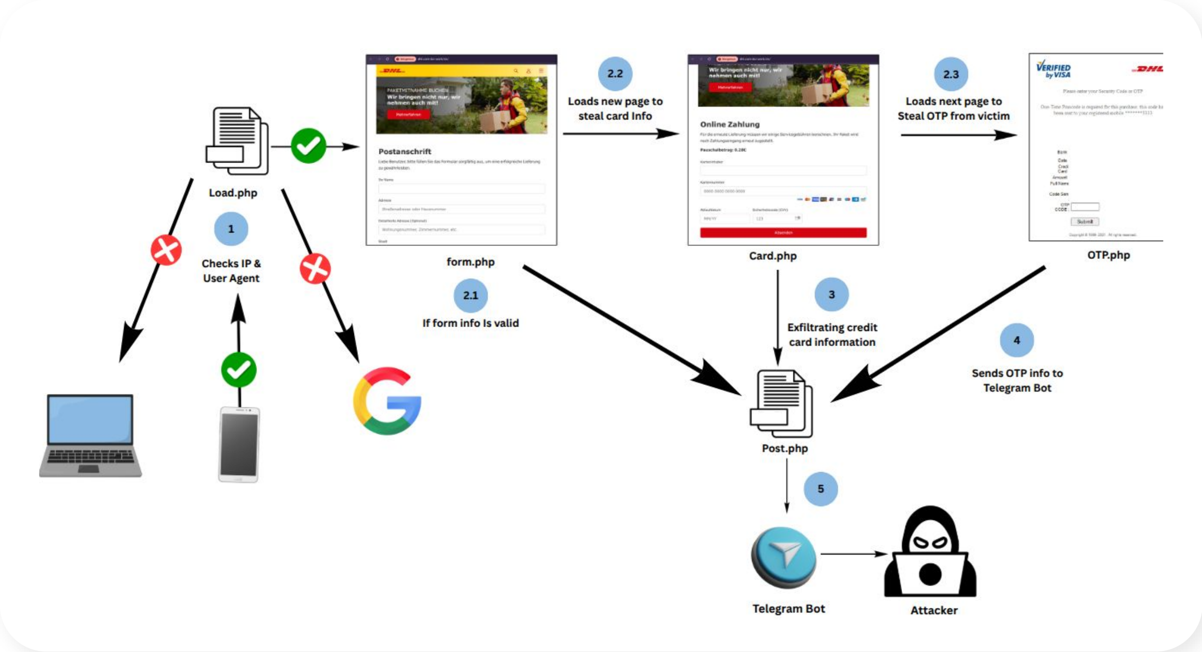
In addition to using Darcula to clone postal services, there are also other prebuilt phishing kits specifically designed for postal scams. While investigating cybercrime marketplaces, we discovered a range of prebuilt phishing kits designed to mimic various organization including postal services. A notable example is a DHL & USPS branded phishing kit, which was actively promoted within Telegram. This particular kit featured a live preview, seemingly aimed at reassuring potential buyers, especially less experienced ones or "script kiddies" about its functionality and effectiveness. We have observed that some of the phishing kits are being shared for free on Telegram and are even available in some public GitHub repositories.



```
-----------SCAMPAGES PRICE----------

Chase spox v5r
Chase spox v3
Chase xbalti
chase f4auds
Wells fargo spox
wells strox cracked
Huntington
Usps scampages
Paypal
Paypal xathena
Citi bank
Usaa
53rd bank
Netflix (without billing)
Netflix (with billing)
Blockchain (with backup) Instagram (email:pass)
Office 365
Dhl
Orange
American express
Amazon
________________________
```

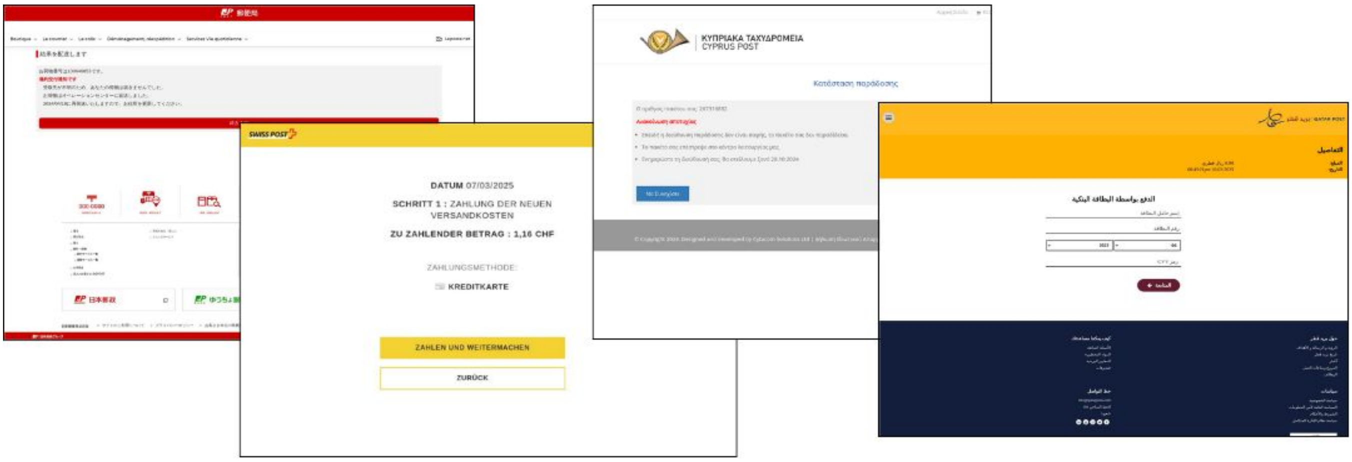
Generic Workflow of The Postal Phishing Kit



These postal phishing kits uses several techniques to avoid detection, including by filtering certain IP addresses or geo location from accessing phishing sites, blocking crawlers from indexing the sites, and blocking device types such as non-mobile devices from viewing the sites. Additionally, most Darcula attacks rely on specific paths, such as /xyz, to access the site, rather than using dedicated subdomains. For national postal scams, these paths are often two-letter country abbreviations corresponding to the targeted nation.

CTM360 Observations - Resource Development

Many campaigns use regional targeting: postal scams are sent in Arabic to Gulf-region numbers, while La Poste and Deutsche Post templates are delivered in French or German respectively. Postal phishing kits supports multiple languages, allowing actors to render phishing pages based on the victim's location or device language, significantly improving believability.



SWISS POST

DATUM 07/03/2025

SCHRITT 1 : ZAHLUNG DER NEUEN VERSANDKOSTEN

ZU ZAHLENDER BETRAG : 1,16 CHF

ZAHLUNGSMETHODE:

KREDITKARTE

ZAHLEN UND WEITERMACHEN

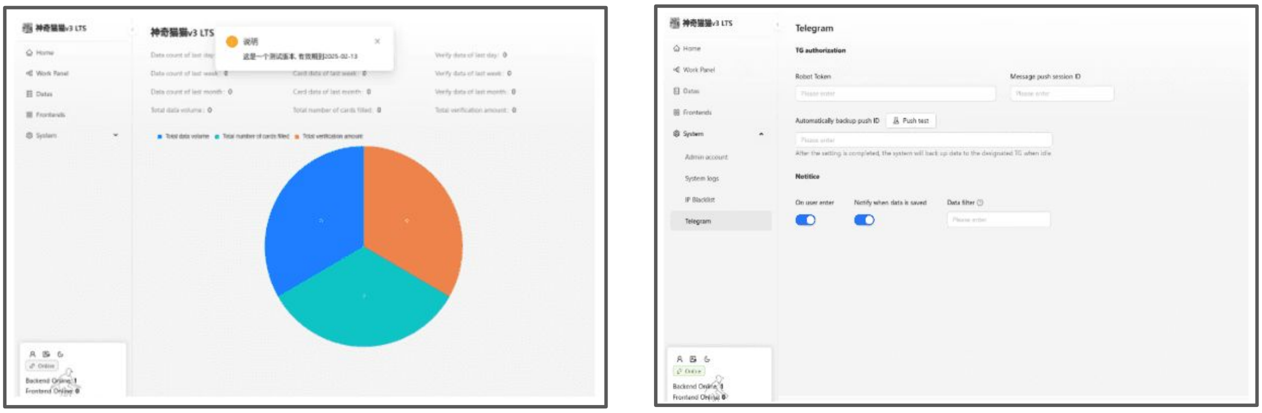
ZURÜCK

ΚΥΠΡΙΑΚΑ ΤΑΧΥΔΡΟΜΕΙΑ
CYPRUS POST

Κατάσταση παράδοσης

Postal scams using different languages to mimic local postal services and appear more credible.

It is common for phishing kits like Darcula-suite to offer an intuitive administrator dashboard that enables users to efficiently manage phishing campaigns. The dashboard aggregates real-time performance statistics, providing a clear view of campaign success. Additionally, threat actors can receive alerts via Telegram when a target becomes a victim of the scam.



神奇猫猫v3 LTS

说明
这是一个测试版本，有效期到2025-02-13

Data count of last week : 0 | Card data of last week : 0 | Verify data of last week : 0
Data count of last month : 0 | Card data of last month : 0 | Verify data of last month : 0
Total data volume : 0 | Total number of cards filled : 0 | Total verification amount : 0

Telegram

TG authorization

Robot Token: Please enter

Message push session ID: Please enter

Automatically backup push ID | Push test

Please enter

After the setting is completed, the system will back up data to the designated TG when idle

Netitice

On user enter ● | Notify when data is saved ● | Data filter: Please enter

On the left: Performance insights via the Darcula-Suite Dashboard. On the right: Seamless Telegram notification integrations for real-time updates. (Source: Netcraft)

CTM360 Observations

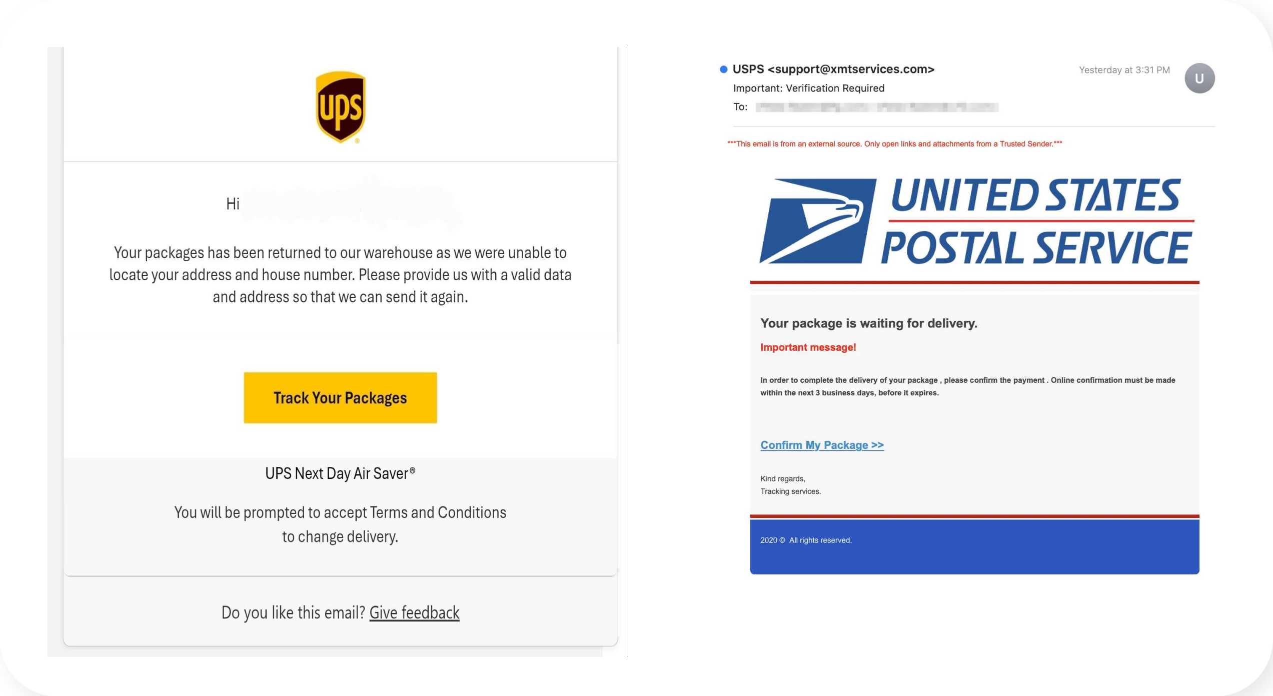
Trigger and Distribution

Scammers exploit **fear, urgency, and impersonation tactics** to initiate delivery scam campaigns that mimic official courier company communications. These alerts often claim: **Missed deliveries, Customs issues, or Package returns.**

These fake messages are through SMS, email, phone calls, and other channels to impersonate major postal and courier services. These messages often mimic the branding and language of trusted delivery companies to appear legitimate with the goal is to trick recipients into clicking malicious links or providing personal information.

Distribution Technique 1: Email Impersonations

The screenshot below shows an example of a phishing email impersonating well-known postal & courier companies. Scammers design these emails to closely replicate the branding, layout, and tone of legitimate delivery services, making them appear authentic. The message within the email usually claims that a package is delayed, pending, or requires further action, urging the recipient to click a link or open an attachment. These links often lead to malicious websites intended to steal personal or financial information or to install malware on the recipient's device. Such scams are especially effective because they exploit the sense of urgency and trust commonly associated with package deliveries.



Hi [redacted]

Your packages has been returned to our warehouse as we were unable to locate your address and house number. Please provide us with a valid data and address so that we can send it again.

UPS Next Day Air Saver®

You will be prompted to accept Terms and Conditions to change delivery.

Do you like this email? Give feedback

USPS <support@xmtservices.com>
Important: Verification Required
To: [redacted]

Yesterday at 3:31 PM

This email is from an external source. Only open links and attachments from a Trusted Sender.

Your package is waiting for delivery.

Important message!

In order to complete the delivery of your package , please confirm the payment . Online confirmation must be made within the next 3 business days, before it expires.

Confirm My Package >>

Kind regards,
Tracking services.

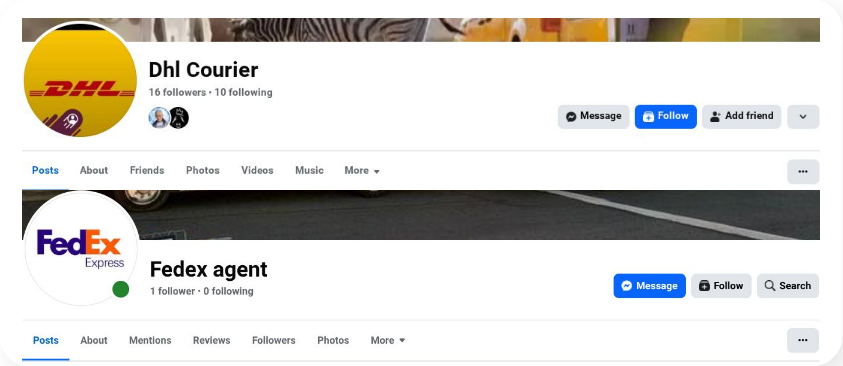
2020 © All rights reserved.

Email received by victims urging them to take action by clicking on a link.

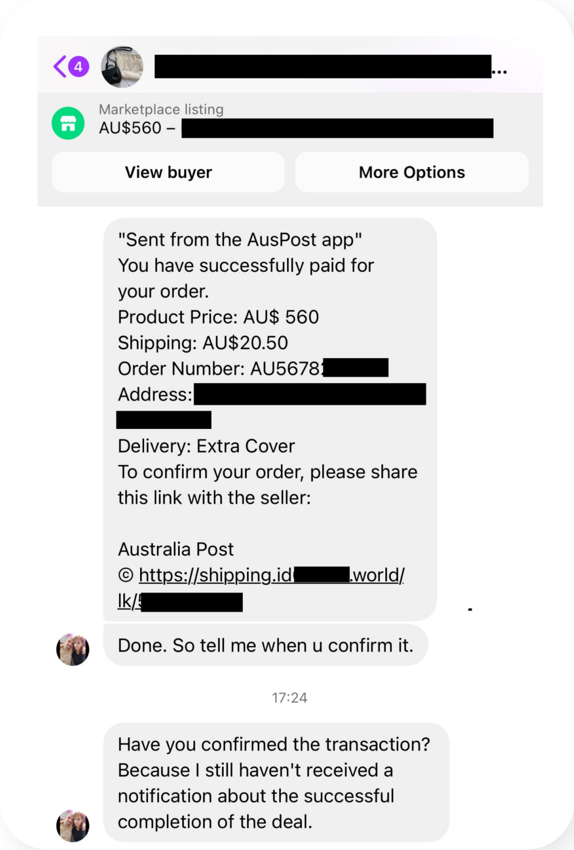
CTM360 Observations

Distribution Technique 2: Social Media Impersonations & Instant Messaging Platforms

The screenshots below showcases how social media impersonation and instant messaging platforms are increasingly being used to facilitate courier-related scams. In these cases, the scammers create fake accounts posing as representatives of well-known courier companies or customer support agents.



They reach out to users via platforms like Facebook Messenger, Instagram, or WhatsApp, often claiming there is an issue with a delivery or that a package is awaiting payment or verification. Victims are then prompted to share personal details, click on malicious links, or make payments to resolve the supposed issue. These scams are highly effective as they exploit both the perceived credibility of courier brands and the immediacy and informality of social media communication.



Marketplace listing
AU$560 – [redacted]

"Sent from the AusPost app"
You have successfully paid for your order.
Product Price: AU$ 560
Shipping: AU$20.50
Order Number: AU5678[redacted]
Address: [redacted]
Delivery: Extra Cover
To confirm your order, please share this link with the seller:

Australia Post
© https://shipping.id[redacted].world/lk/[redacted]

Done. So tell me when u confirm it.

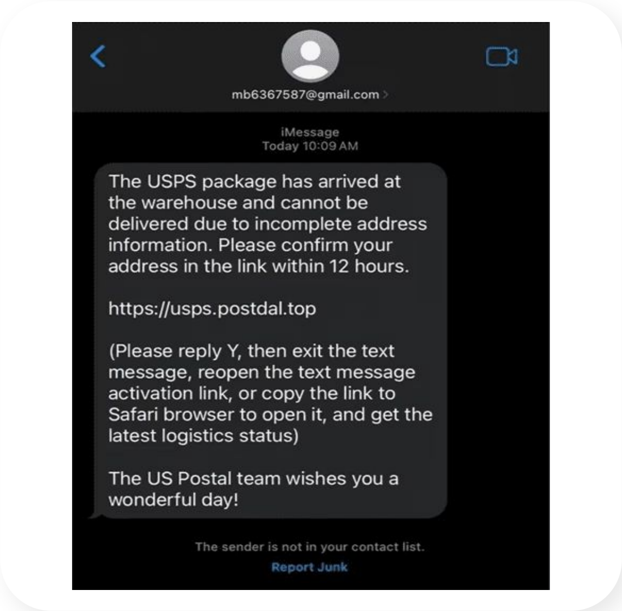
17:24

Have you confirmed the transaction? Because I still haven't received a notification about the successful completion of the deal.

CTM360 Observations

Distribution Technique 3: SMS, iMessage & RCS

The Darcula platform uses alternative distribution methods to spread phishing links, primarily through iMessage and RCS (Rich Communication Services), allowing it to bypass standard SMS firewall protections. These links are often disguised using URL shorteners such as Bit.ly and TinyURL to further evade detection and enhance click-through rates.



mb6367587@gmail.com

iMessage
Today 10:09 AM

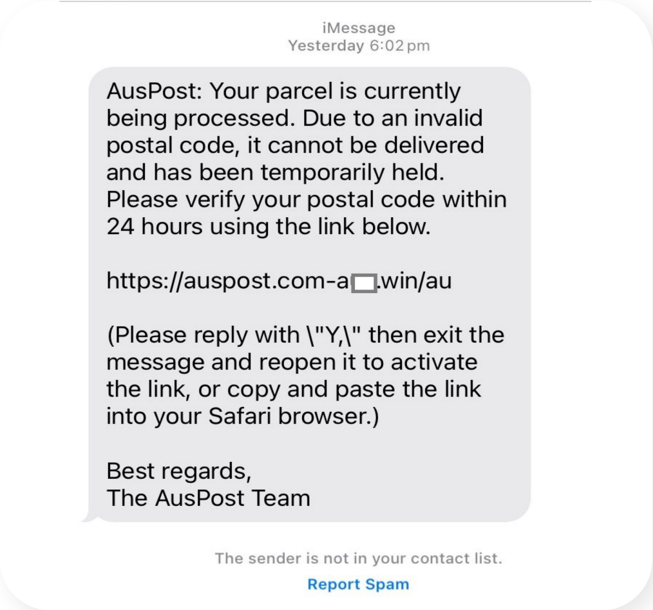
The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

https://usps.postdal.top

(Please reply Y, then exit the text message, reopen the text message activation link, or copy the link to Safari browser to open it, and get the latest logistics status)

The US Postal team wishes you a wonderful day!

The sender is not in your contact list.



iMessage
Yesterday 6:02 pm

AusPost: Your parcel is currently being processed. Due to an invalid postal code, it cannot be delivered and has been temporarily held. Please verify your postal code within 24 hours using the link below.

https://auspost.com-a□.win/au

(Please reply with \"Y,\" then exit the message and reopen it to activate the link, or copy and paste the link into your Safari browser.)

Best regards,
The AusPost Team

The sender is not in your contact list.

iMessage used to distribute postal phishing links

The choice to use iMessages and Google Messages (based on the RCS standard) to lead users to the phishing sites is clever:

- They are free to send
- They are more trusted by consumers than regular text messages
- They are end-to-end encrypted, preventing network operators from analyzing their content, thus allowing the messages to evade filters put in place by to block unsolicited and fraudulent SMS messages.
- It creates a false sense of urgency through well-crafted messages

iMessages can be sent in bulk via “mass sender” scripts, the researchers also pointed out, as can Google Messages, via Android device farms.

CTM360 Observations

Motive

The operators behind the global postal & courier scam is primarily motivated by financial gain and data exploitation. Their operations are characterized by:

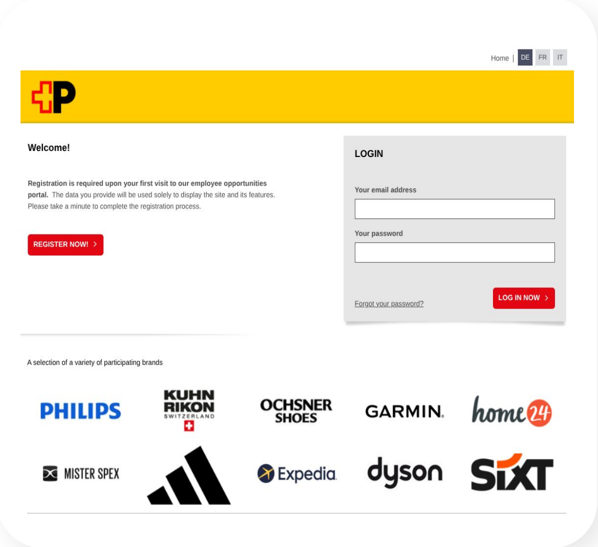
Credential Harvesting

Threat actors collect login credentials to online banking, email, e-commerce, and government service portals. These credentials are either:
- Used directly to gain access to financial or valuable digital assets.
- Sold to other cybercriminals on underground forums.

Personally Identifiable Information (PII) Harvesting

Victims are tricked into entering sensitive details such as:
- Full names, addresses, dates of birth
- National ID numbers, Social Security Numbers (SSNs)
- Contact information, including phone numbers and email addresses

This data is highly valuable for **identity theft**, **account takeovers**, and further social engineering campaigns.



Welcome!

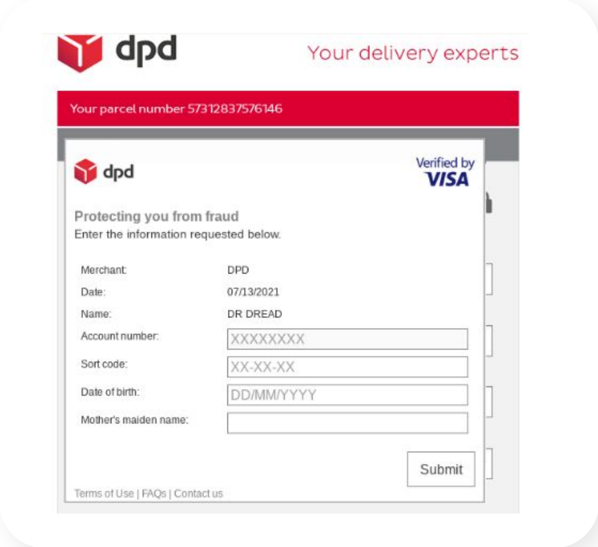
Registration is required upon your first visit to our employee opportunities portal. The data you provide will be used solely to display the site and its features. Please take a minute to complete the registration process.

LOGIN

Your email address

Your password

A selection of a variety of participating brands



Your parcel number 57312837576146

Protecting you from fraud
Enter the information requested below.

Merchant:	DPD
Date:	07/13/2021
Name:	DR DREAD
Account number:	XXXXXXXX
Sort code:	XX-XX-XX
Date of birth:	DD/MM/YYYY
Mother's maiden name:	

Requesting OTP (One-Time Password) and MFA Information

To bypass modern multi-factor authentication (MFA) systems, many Darcula phishing kits ask for:
- SMS-based OTPs
- App-based codes (e.g., Google Authenticator)
- Biometric confirmations (simulated via UI deception)

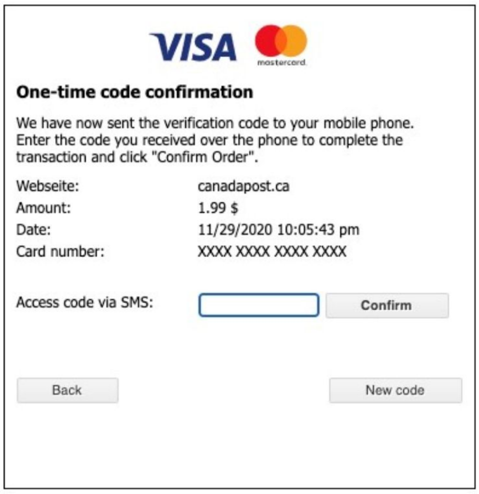
This allows actors to perform real-time **session hijacking**.

CTM360 Observations

Monetization

Fraudulent Transactions Using Credit/Debit Card Data

After victims are tricked into submitting their payment card information through phishing sites, attackers often prompt them to enter a one-time passcode (OTP), claiming it's for verification. In reality, this OTP is sent by the victim's bank to authorize adding the card to a digital wallet such as Apple Pay or Google Wallet. Once the victim provides this code, fraudsters can successfully link the stolen card to a mobile wallet on a device they control, usually a burner phone. These wallets are then used to make unauthorized transactions, including online purchases or in-store payments.



One-time code confirmation

We have now sent the verification code to your mobile phone. Enter the code you received over the phone to complete the transaction and click "Confirm Order".

Webseite:	canadapost.ca
Amount:	1.99 $
Date:	11/29/2020 10:05:43 pm
Card number:	XXXX XXXX XXXX XXXX

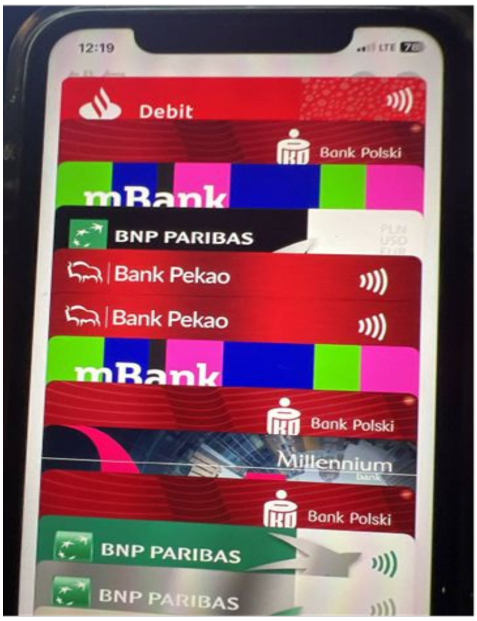
Access code via SMS:

The fake OTP page

Exploitation of Stolen Card Data

Stolen card data harvested through phishing kits like the Dracula-suite can be weaponized further by generating realistic images of the victim's card, making it easier to bypass certain verification checks. Fraudsters commonly load up to 20 stolen cards onto a single burner phone. These phones, preloaded with active digital wallets, are then sold or used directly for fraud. The practice has been openly showcased in Telegram channels linked to Darcula, confirming a broader ecosystem where digital wallets serve as a monetization method for compromised card data.

The exploitation of stolen card data is not limited to postal & courier scams and is increasingly observed across other phishing campaigns that use phishing kits.



Posted on a Telegram channel, this image shows a burner phone loaded with multiple stolen cards.

ABOUT US

CTM360 is a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

☎ +973 77 360 360

✉ info@ctm360.com

🌐 www.ctm360.com

📍 21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents, or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential, or other damages or claims whatsoever including, but not limited to loss of data, loss in profits/business, network disruption...etc., arising out of or in connection with this advisory.

CTM360®