Timos & Cia.:

Desvelando los entresijos de Telekopye

Josep Albors

Responsable de investigación y concienciación ESET España

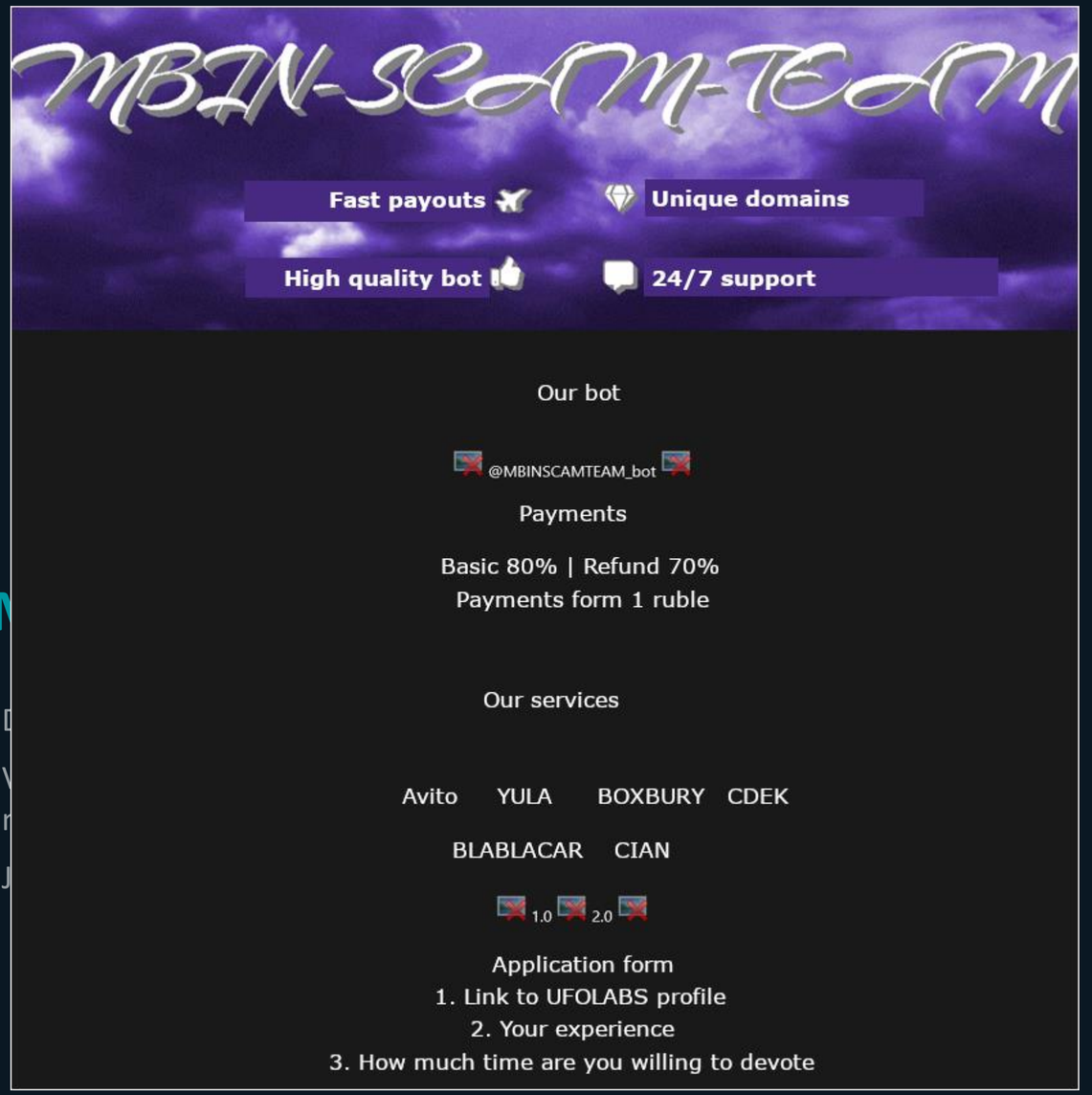
Digital Security
Progress. Protected.

Terminología

- Mamuts
  - Alguien a quien quieres fastidiar (jerga rusa)
- Neandertal
  - El scammer
- Telekopye
  - Telegram + копье (lanza en ruso)

Introducción a Telekopye

nociendo a Telekopye



antes

Total

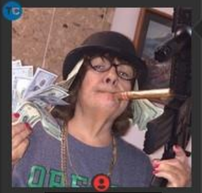
go

del código

Uniéndose a un grupo

Набор в команду GIPSY TEAM [avito-scam] [Recruitment for the GIPSY TEAM]

[redacted] scam scam avito work work 2.0



[redacted]

Незнакомец

ЧИТАТЕЛЬ

11

Регистрация: 11.03.23
Сообщения: 17
Онлайн: 22ч 32м
Сделки: 0
Нарушения: 0 / 0

#1

⚜ GIPSY - RU WORK ⚜

♻ Платим честные 75% без скрытых комиссий ♻
[We pay stable 75% without hidden fees]

⌛ Стабильная работа на протяжении 3-х лет ⌛
[Stable work for 3 years]

⚙ Дизайн сайтов полностью повторяет оригинальный Авито/Юла/CDEK ⚙
[The website completely replicates the original Avito/Yula/CDEK]

➡ Ждем ваших заявок - [redacted]bot ⬅
[We are waiting for your application at **REDACTED**]

⚠ Твоя заявка отправлена на рассмотрение, ожидай сообщение от бота ⚠ [Your application has been sent for consideration, please wait] 14:47

🥳 Поздравляем, ты стал членом нашей команды! Наши ссылки: [Congratulations, you have become a member of our team! Our links:]

💬 ЧАТ
💰 ЗАЛЕТЫ

Telegram
💬 GIPSY | Chat 🍾
[redacted] invites you to join this group on Telegram.

VIEW GROUP

14:48

Roles dentro de Telekopye

Administradores

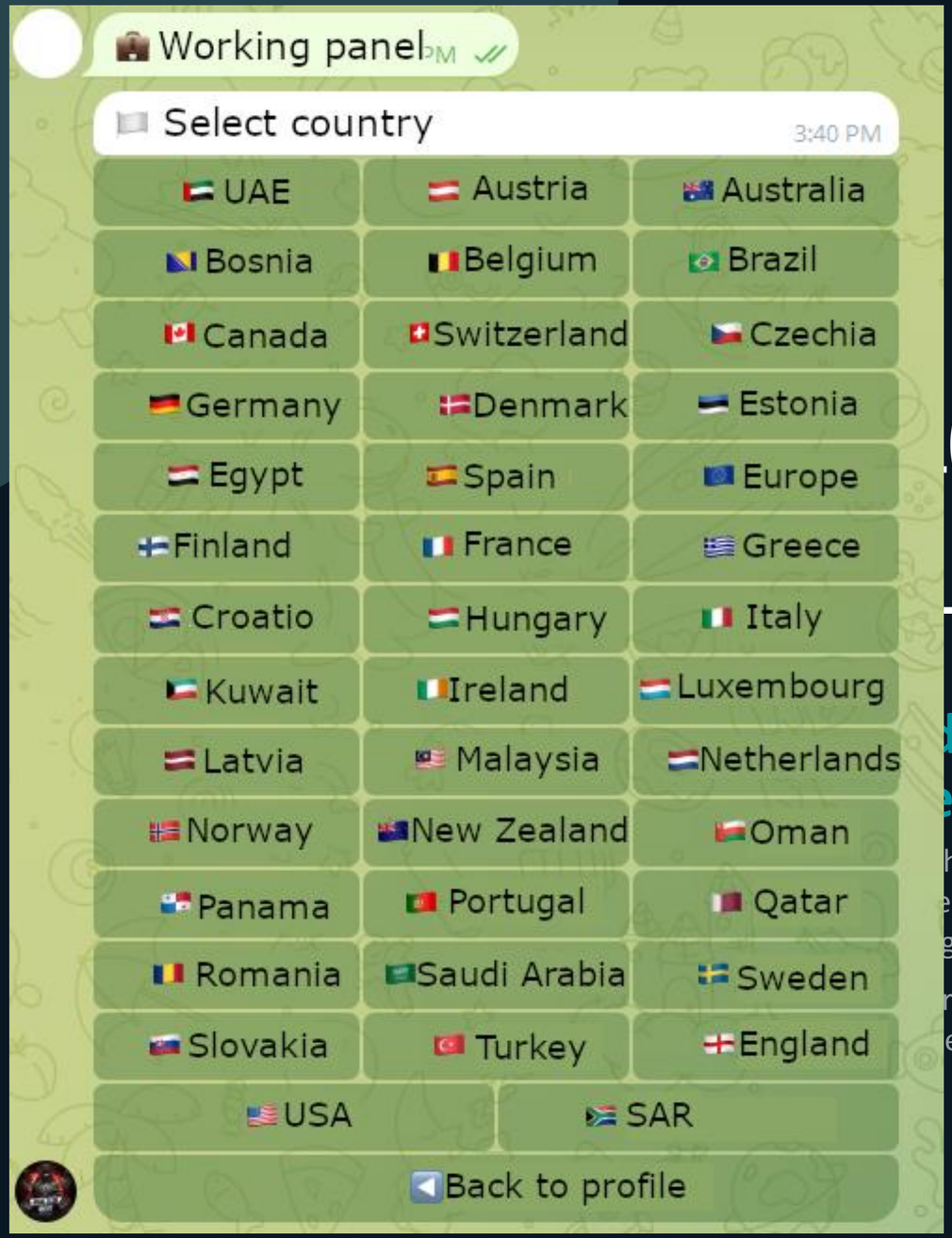
Moderadores

Buenos trabajadores (75%)

Bots de Soporte

Trabajadores (65%)

Bloqueados



Telekopye - objetivos

de pago
entas

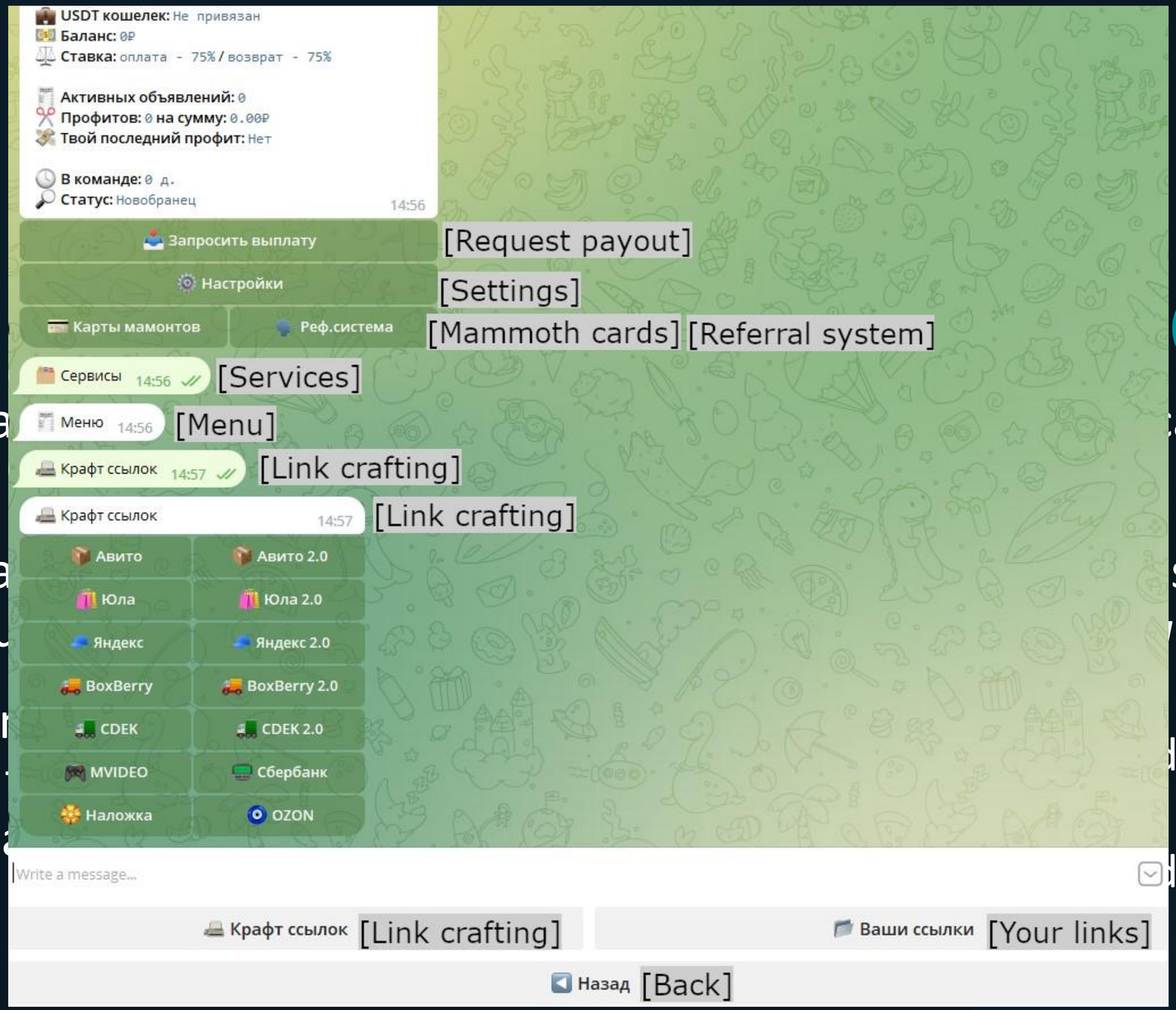
has de
eedores de
go

roblemas de
enes

M

-
-

- El Nea
- El Nea
- El Mar



(2.0)

a un Mamut

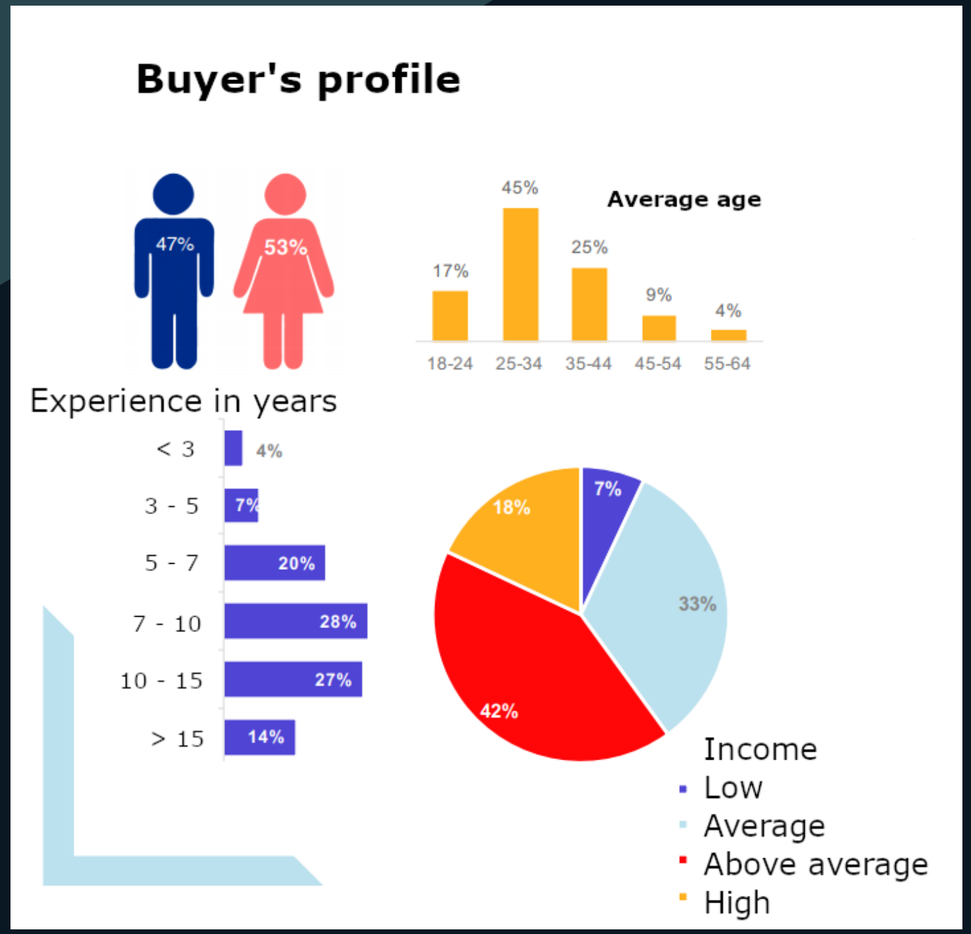
stra interes y

t para que

de la

del

Búsqueda de víctimas



	A	D	E	F	G	N	T	AH	AL	AP	AQ	AS
1	**Seller**	**Gender**	**Product**	**Description**	**Price**	**Address**	**Creation date**	**Delivery**	**Link to profile**	**Active Ads**	**Finished Ads**	**Rating**
2	User	Not specified	iPhone 5S, 32 ГБ	Продаю iphone	1000	**REDACT	2023-10-24 16:21:50	0	**REDACTED**	4	20	5
3	User	Not specified	Nokia 1200	Продаются на	2000	**REDACT	2023-10-24 16:21:49	1	**REDACTED**	22	83	4,4
4	**REDAC	Not specified	OPPO Reno9, 8/256 ГБ	id: 774930Мы х	2500	**REDACT	2023-10-24 16:21:49	0	**REDACTED**	нет	нет	3,8
5	**REDAC	Male	iPhone 11, 128 ГБ	Айфон 11 на 1	24500	**REDACT	2023-10-24 16:21:47	1	**REDACTED**	0	0	4,5
6	User	Not specified	iPhone 15, 128 ГБ	Оригинальный	89999	**REDACT	2023-10-24 16:21:46	1	**REDACTED**	2	0	0
7	**REDAC	Not specified	Samsung Galaxy A04s, 4/64 ГБ	№ товара: 969	10752	**REDACT	2023-10-24 16:21:44	0	**REDACTED**	нет	нет	4,1
8	User	Not specified	Sony Ericsson K770i	K770I работает	400	**REDACT	2023-10-24 16:21:41	1	**REDACTED**	36	3	4,8
9	**REDAC	Not specified	iPhone Xr, 64 ГБ	— Экран 6.1" (	17990	**REDACT	2023-10-24 16:21:40	0	**REDACTED**	нет	нет	4,6
10	**REDAC	Мужской	Samsung Galaxy S22, 8/256 ГБ	Магазин SotBe	50000	**REDACT	2023-10-24 16:21:40	0	**REDACTED**	нет	нет	4,9
11	**REDAC	Male	Samsung Galaxy A32, 6/128 ГБ	Samsung a32 1	11500	**REDACT	2023-10-24 16:21:38	1	**REDACTED**	0	0	5
12	User	Not specified	Телефон i14pro max	Полный компл	7500	**REDACT	2023-10-24 16:21:36	1	**REDACTED**	1	0	0
13	**REDAC	Not specified	INOI 99	INOI 99 (24.10)	999	**REDACT	2023-10-24 16:21:34	1	**REDACTED**	нет	нет	4,2
14	User	Not specified	iPhone 6, 64 ГБ	Продам iPhone	2000	**REDACT	2023-10-24 16:21:34	0	**REDACTED**	6	34	4,7
15	**REDAC	Not specified	iPhone 8 Plus, 64 ГБ	Полный компл	14500	**REDACT	2023-10-24 16:21:34	1	**REDACTED**	0	0	5
16	User	Not specified	Xiaomi Redmi Go, 16 ГБ	Все детали в р	2000	**REDACT	2023-10-24 16:21:30	0	**REDACTED**	3	1	3
17	**REDAC	Not specified	iPhone 11, 128 ГБ	В продаже:iPh	28400	**REDACT	2023-10-24 16:21:30	1	**REDACTED**	0	0	5
18	User	Not specified	TECNO Spark Go 2022, 2/32 ГБ	Полностью раб	3490	**REDACT	2023-10-24 16:21:30	1	**REDACTED**	228	685	4,5
19	User	Not specified	iPhone 11, 128 ГБ	В наличии iphc	51000	**REDACT	2023-10-24 16:21:29	1	**REDACTED**	4	2	0
20	**REDAC	Male	Xiaomi 12X, 8/256 ГБ	Гарантия само	37990	**REDACT	2023-10-24 16:21:29	0	**REDACTED**	0	0	5
21	User	Not specified	iPhone 14, 128 ГБ	Iphone 14 128 I	78990	**REDACT	2023-10-24 16:21:24	1	**REDACTED**	24	267	4,8

Escenario del vendedor

amazon

Making an order

Payment method

By Card Online

Jura S8 Automatic Coffee and Espresso Machine (Piano Black)

Warehouse Amazon • 1 product

Delivery Amazon

Delivery from Amazon

Method of obtaining

Delivery by courier ✓

amazon

Payment by bank card

Total including delivery and VAT

1359.99$

VISA

Card number

1234 4567 7890 0000

Card owner

Valid until

MM / ГГ

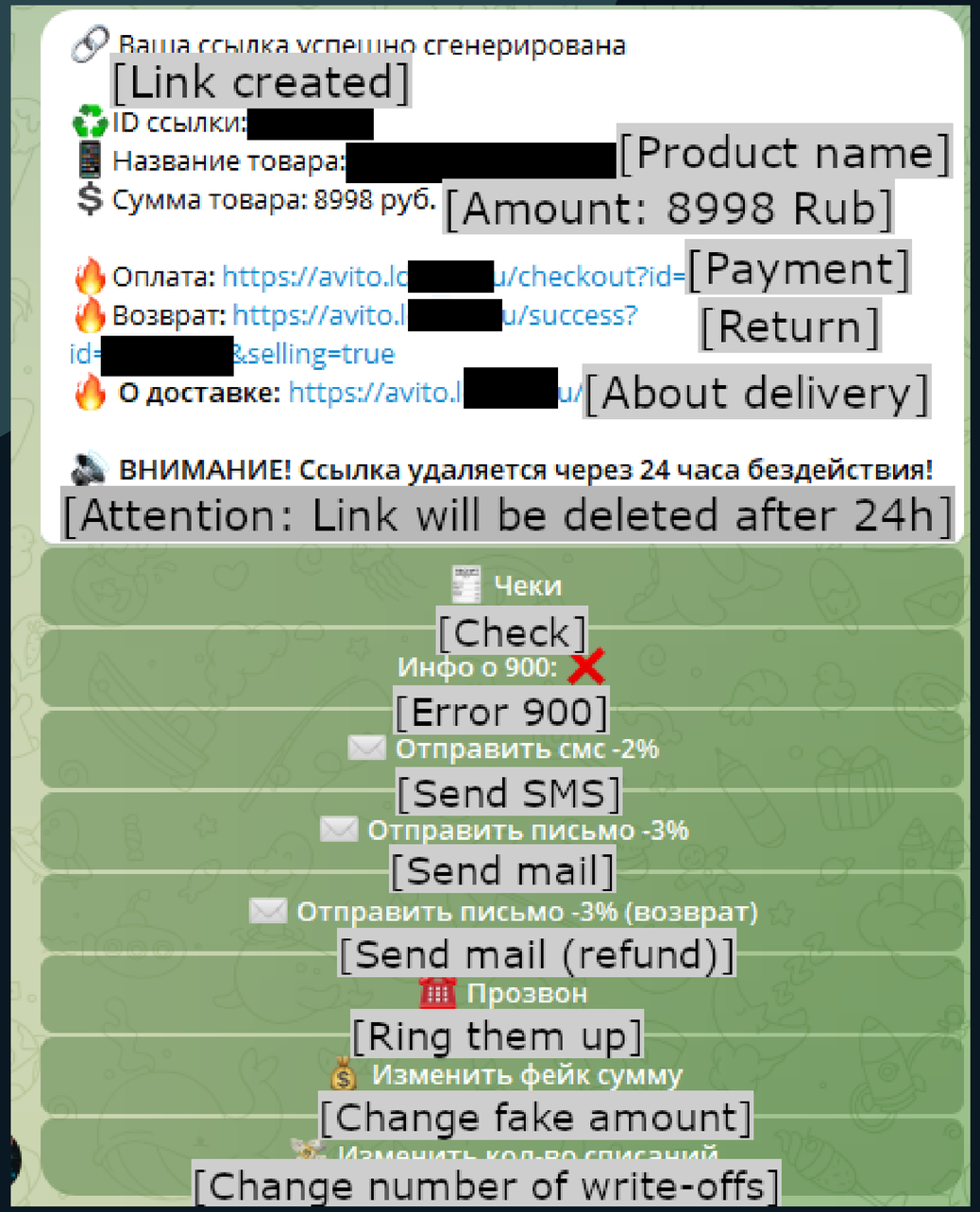
CVV/CVC

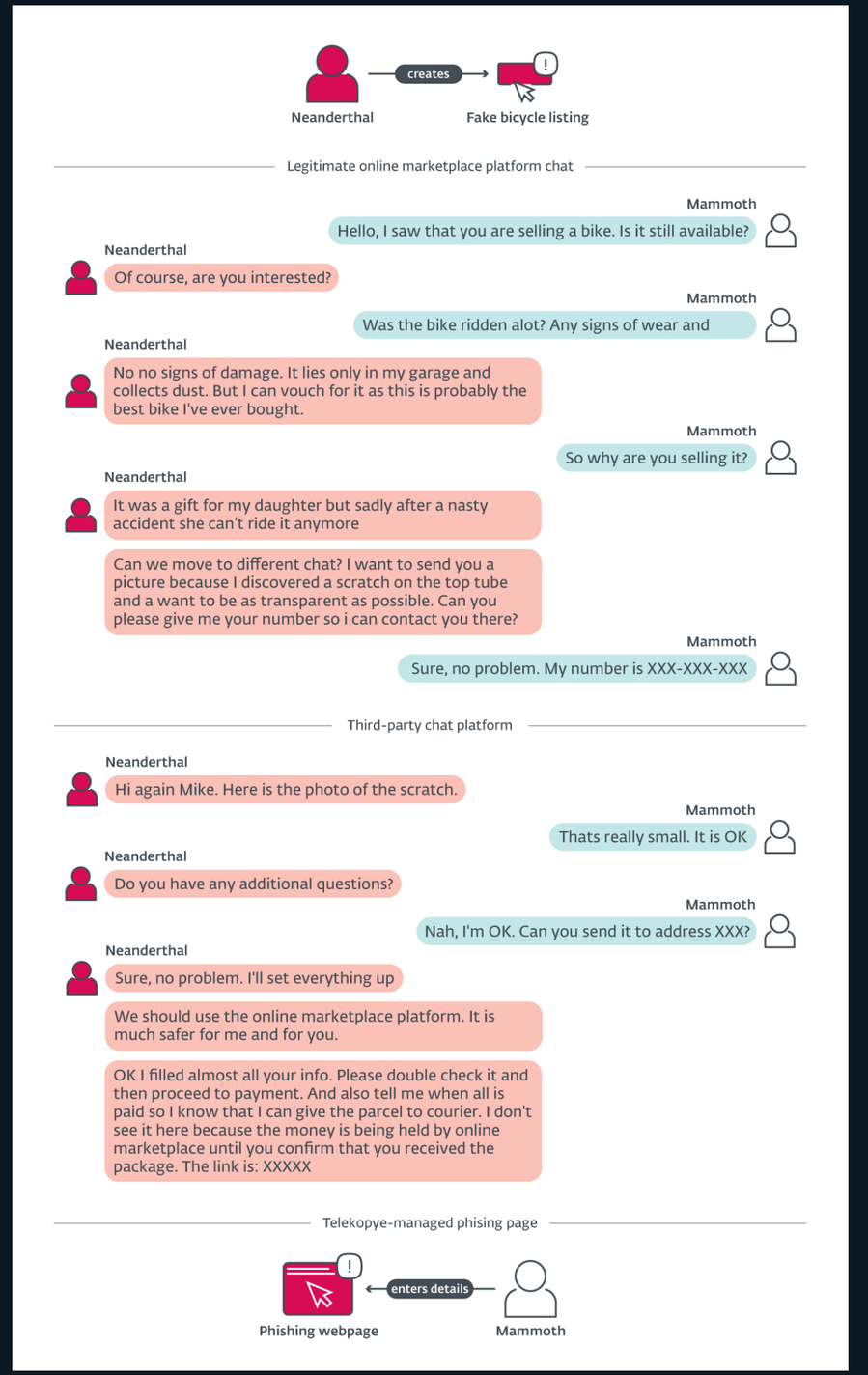
123

three numbers from the back of the card

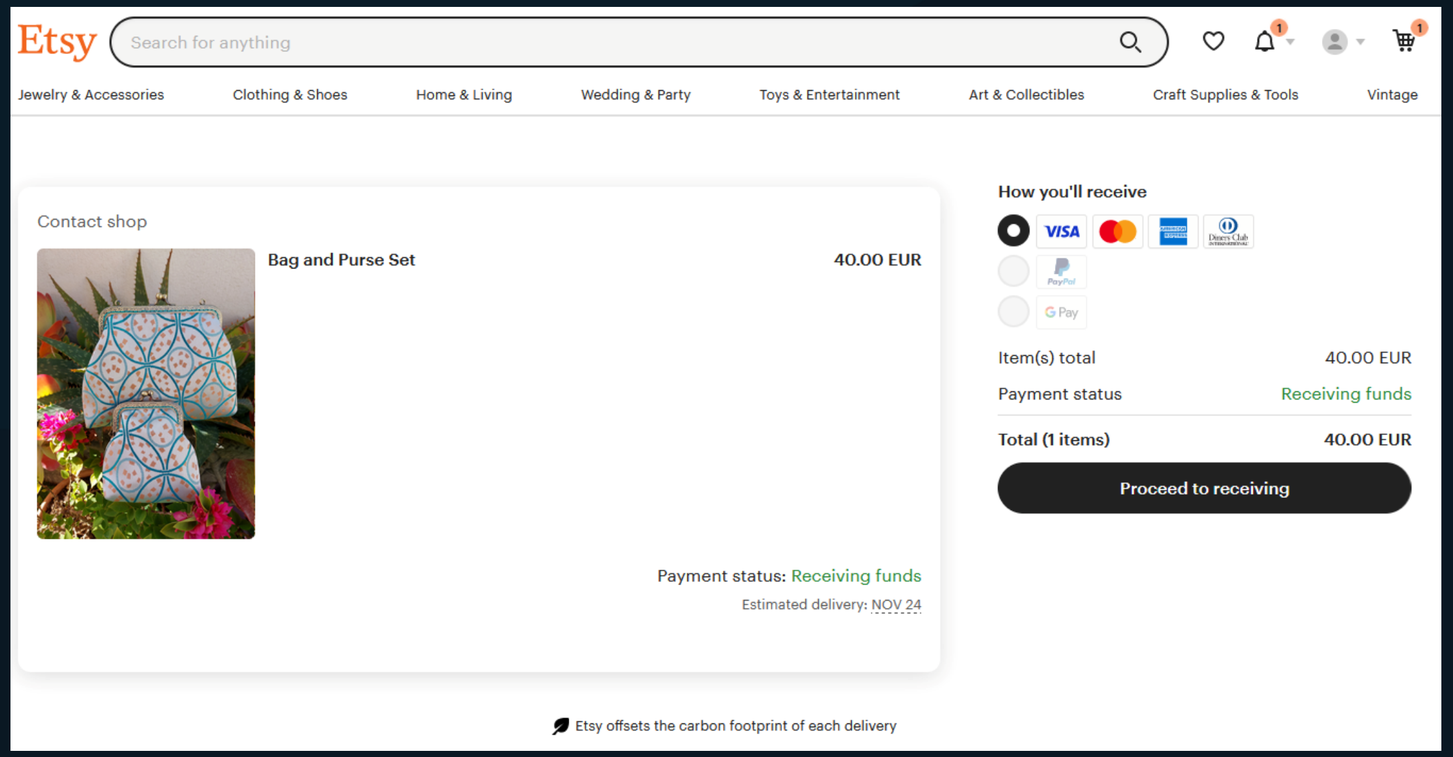
To pay 1359.99$

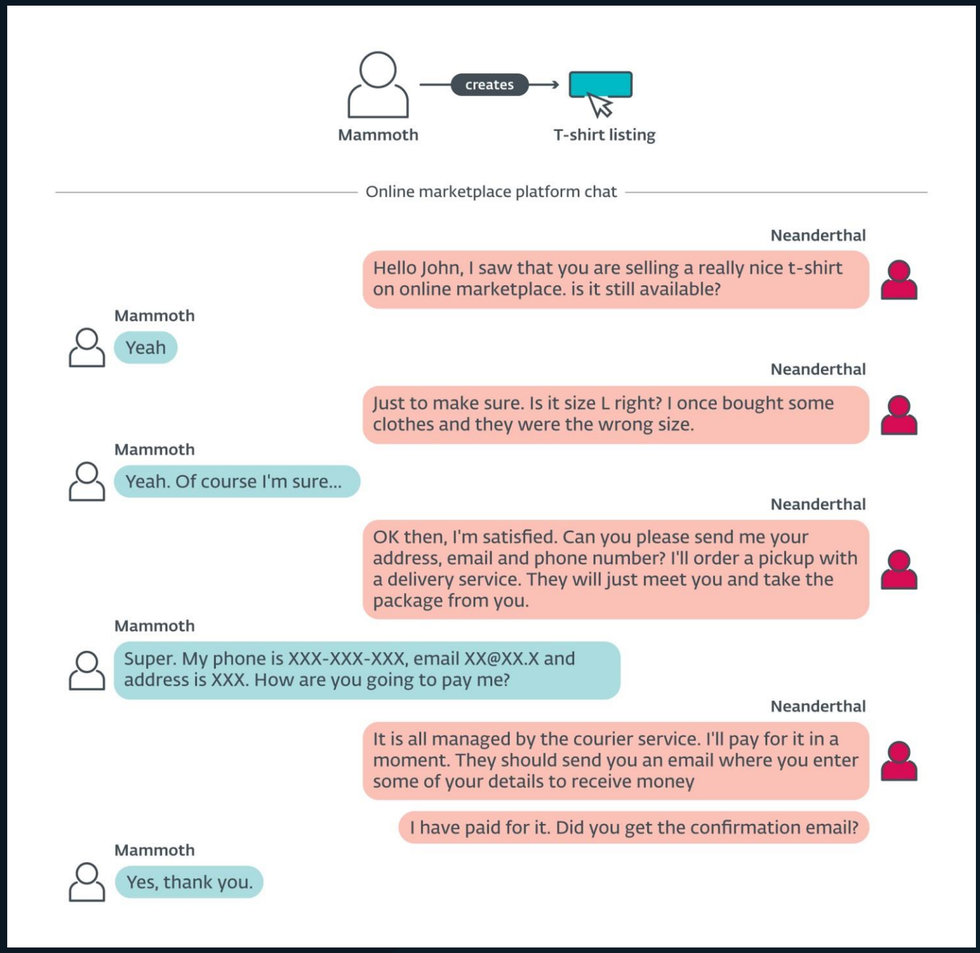
Escenario del vendedor



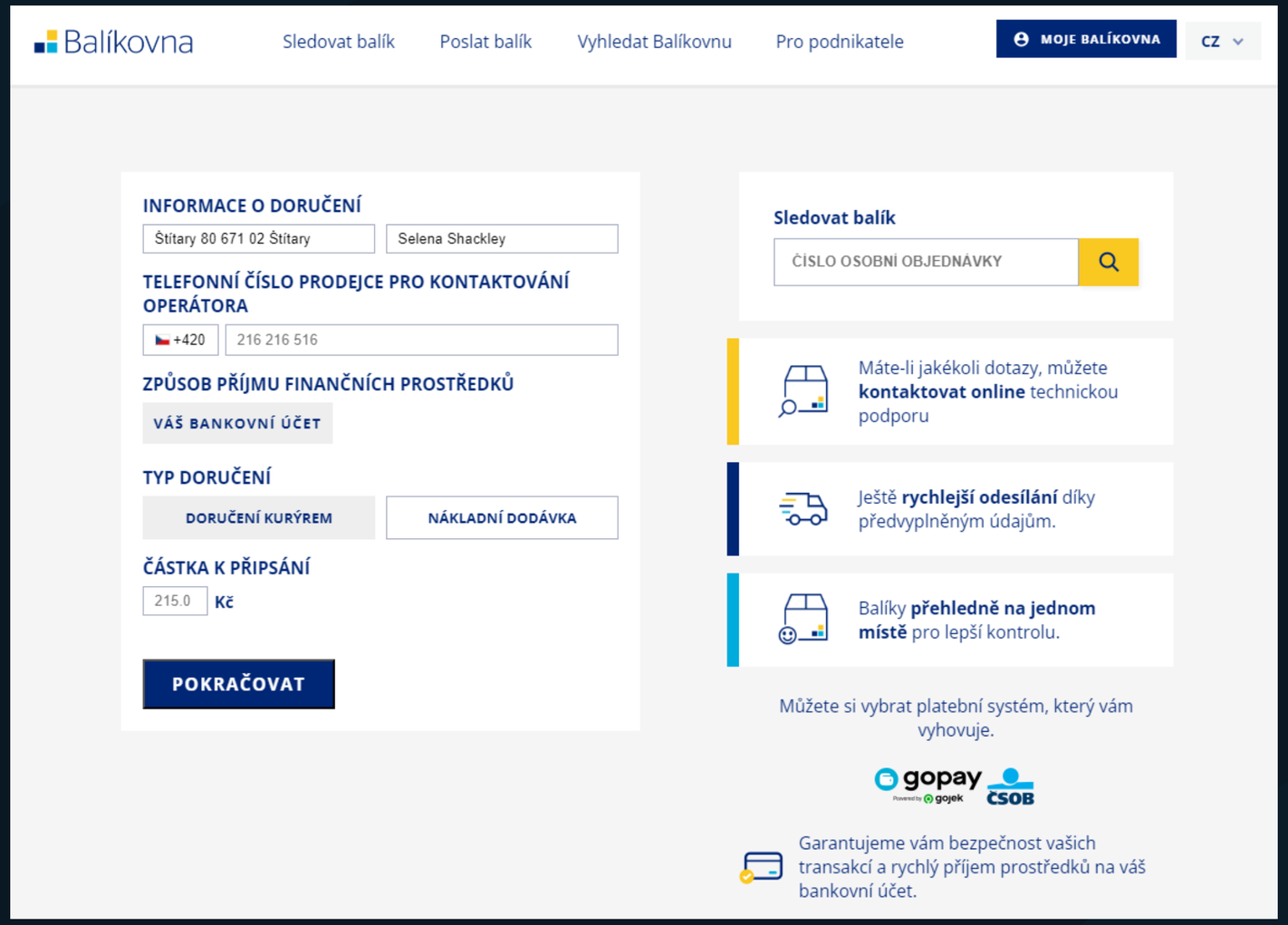


Escenario del comprador + abuso de la marca de la plataforma





Escenario del comprador + abuso de la marca del transportista



Credenciales / tarjetas / MFA

Revolut

Log in using your phone

To keep your account secure, we'll send you a code to log in. New to Cash App?
Create account

Mobile number

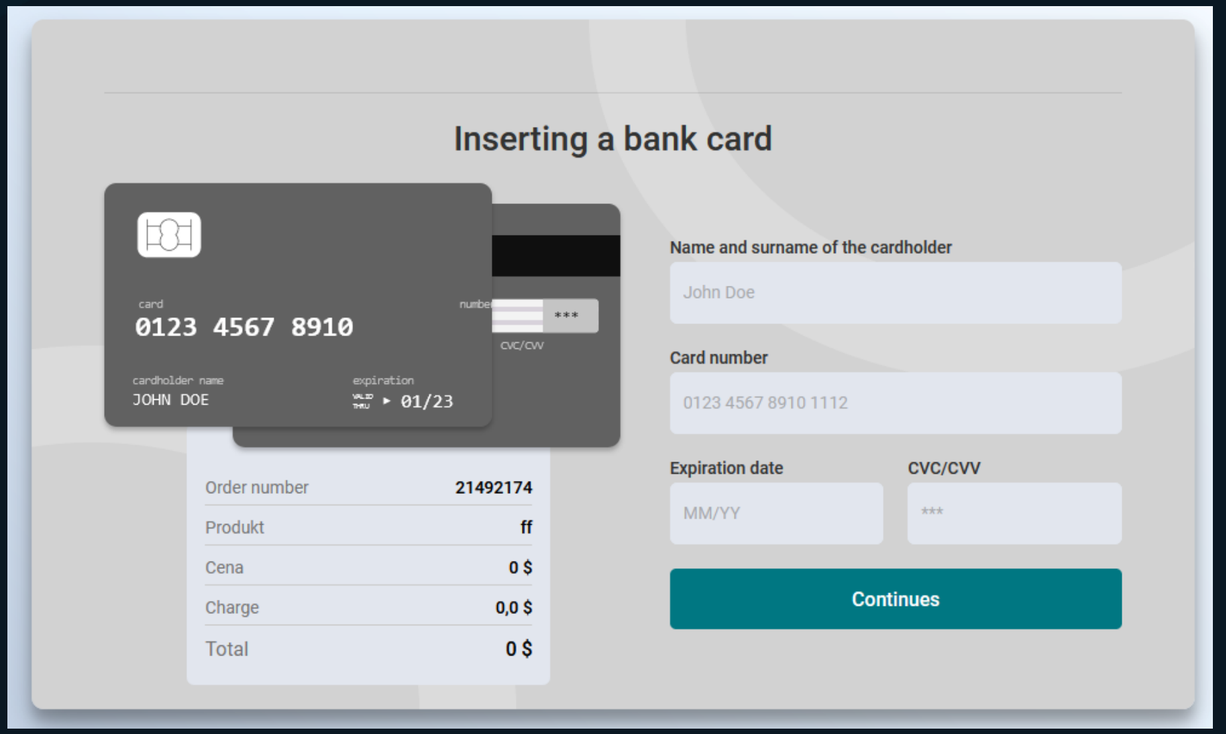
+1 (123) 456-7890

Password

Your password

Log in

By entering and clicking Next, you agree to the Terms, E-Sign Consent, & Privacy Policy



Подтверждение операции

Магазин	**OZON**
Сумма	**3708 ₽**
Номер карты	****** **** **** 9184**
Комментарий	**-**

Для подтверждения операции на Ваш номер телефона было отправлено смс сообщение с кодом подтверждения. Введите его в поле ниже.

Код из смс:

Введите код из смс...

Запросить повторно через 0149

Отправить код

Uso de plantillas

ebay

The receipt of funds

Buyer

FCS	%namef%
Product	%title%
Address	%address%

Receive %amount2% EUR

The buyer has already paid for the order, it remains only to receive the money and transfer the goods.

The order is paid

%title%

Product	%amount2% EUR
Total	**%amount2% EUR**

Conferma di pagamento

Avito

Per confermare il pagamento, è stato inviato un messaggio SMS al tuo numero di telefono con un codice di verifica. Digitalo nella casella sottostante.

Attenzione! a causa del carico elevato del server, l'invio del codice può essere ritardato di alcuni minuti.

Importante! se l'elaborazione del pagamento è lunga, riprova.

Negozio:	**%shop%**
Importo:	**%summ% €.**
Numero della carta:	****** **** **** %card%**

%msg%

Codice di conferma:

Inserisci il codice...

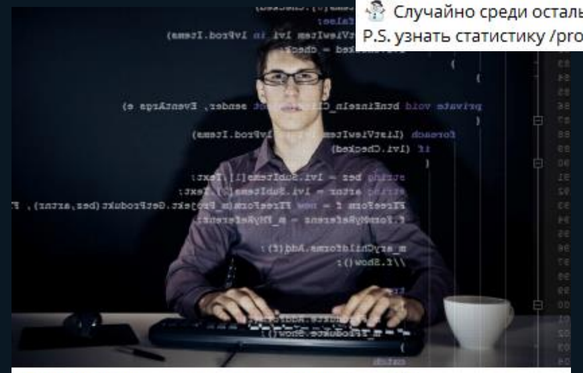
Confermare

Cultura interna

GIPSY | Money
Forwarded from GIPSY | Money

🎅 НОВОГОДНИЙ КОНКУРС 🎁 на 3.5% от общего банка на период с 1.12 до 30.12

🏆 Победители получат:
🥇 1. - место — 2% от 🏦
🥈 2. - место — 1% от 🏦
🥉 3. - место — 0.5% от 🏦
🌟 4-6. - место — 1.000₽
🎰 Случайно среди остальных — 1.000₽ (x3)
P.S. узнать статистику /promo в чат



🤖 *КОДЕРЫ кто занимается созданием фишей ?*

🔥 *Есть свежие интересные офера, есть работа* 🔥

✏️ *Подробности*: @specagentmoney 5:13 PM

✅FULL WORK!✅

🇵🇱 Польша 🇫🇮 Финляндия 🇳🇱 Нидерланды 🇵🇹 Португалия
🇪🇸 Испания 🇬🇷 Греция 🇨🇿 Чехия 🇸🇰 Словакия 🇫🇷 Франция,
🇱🇺 Люксембург 🇨🇭 Швейцария
🇩🇪 Германия

✅Перед началом ворка просьба убедиться что ваш ТПшер онлайн! По возможности прыгайте на других! 9:20 AM

February 6

🟢 FULL WORK 😛 11:07 AM

🔴 STOP WORK ❗ 10:08 PM

February 7

🟢 FULL WORK 😛 11:04 AM

🔴 STOP WORK ❗ 10:22 PM

February 8

🟢 FULL WORK 😛 11:08 AM

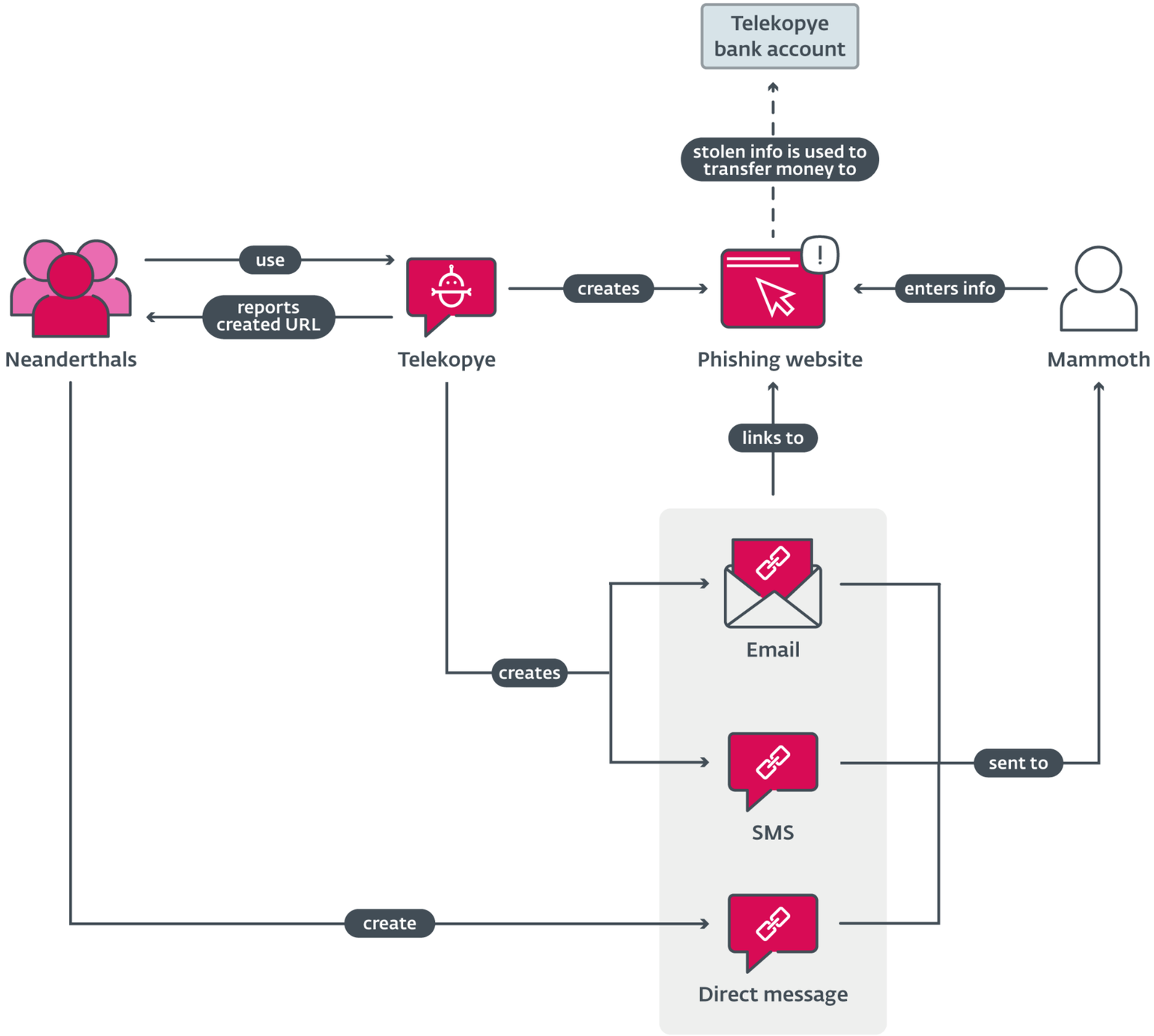
🔴 STOP WORK ❗ 9:55 PM

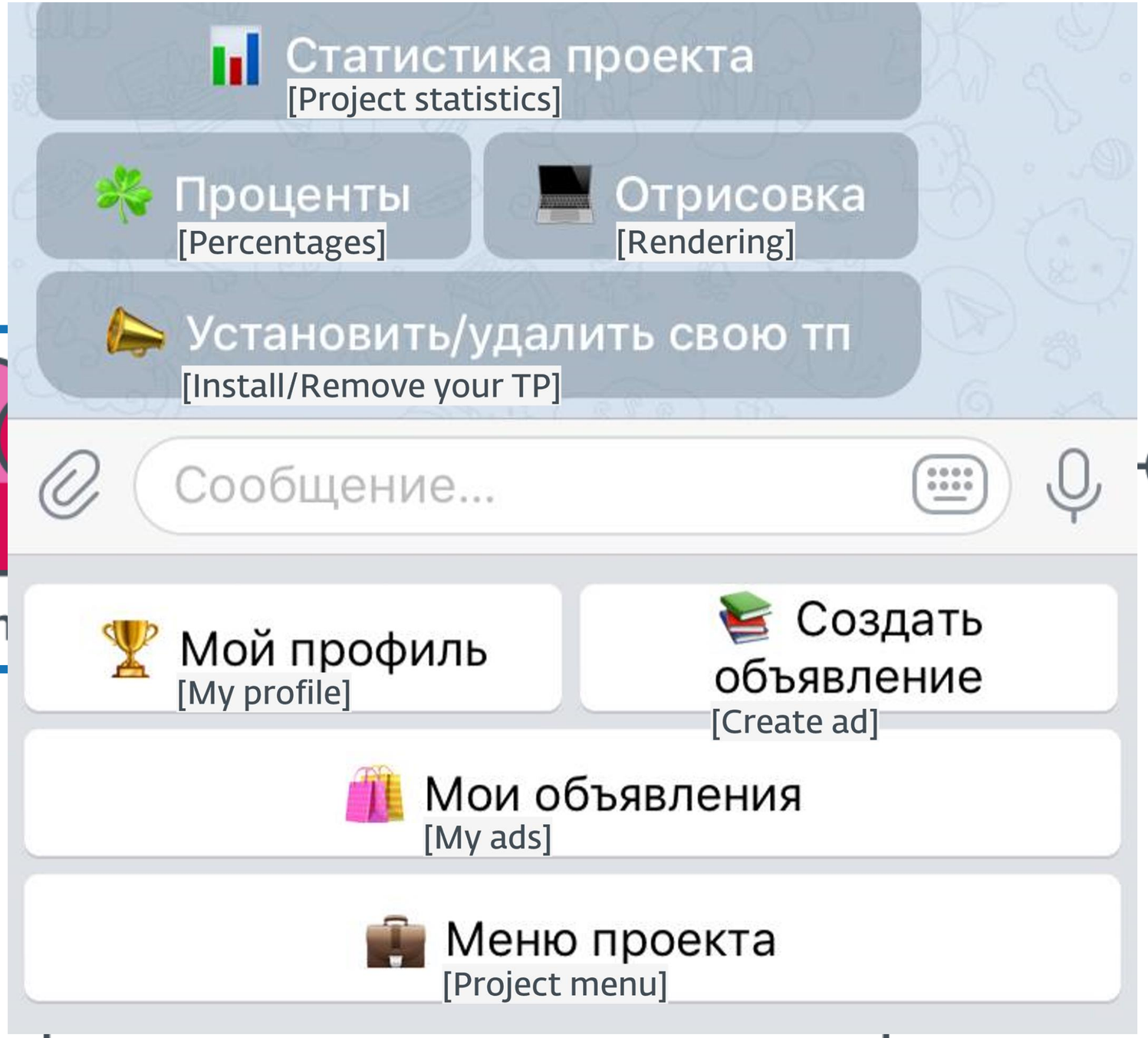
February 9

🟢 FULL WORK 😛 11:15 AM

🔴 STOP WORK ❗ 10:10 PM

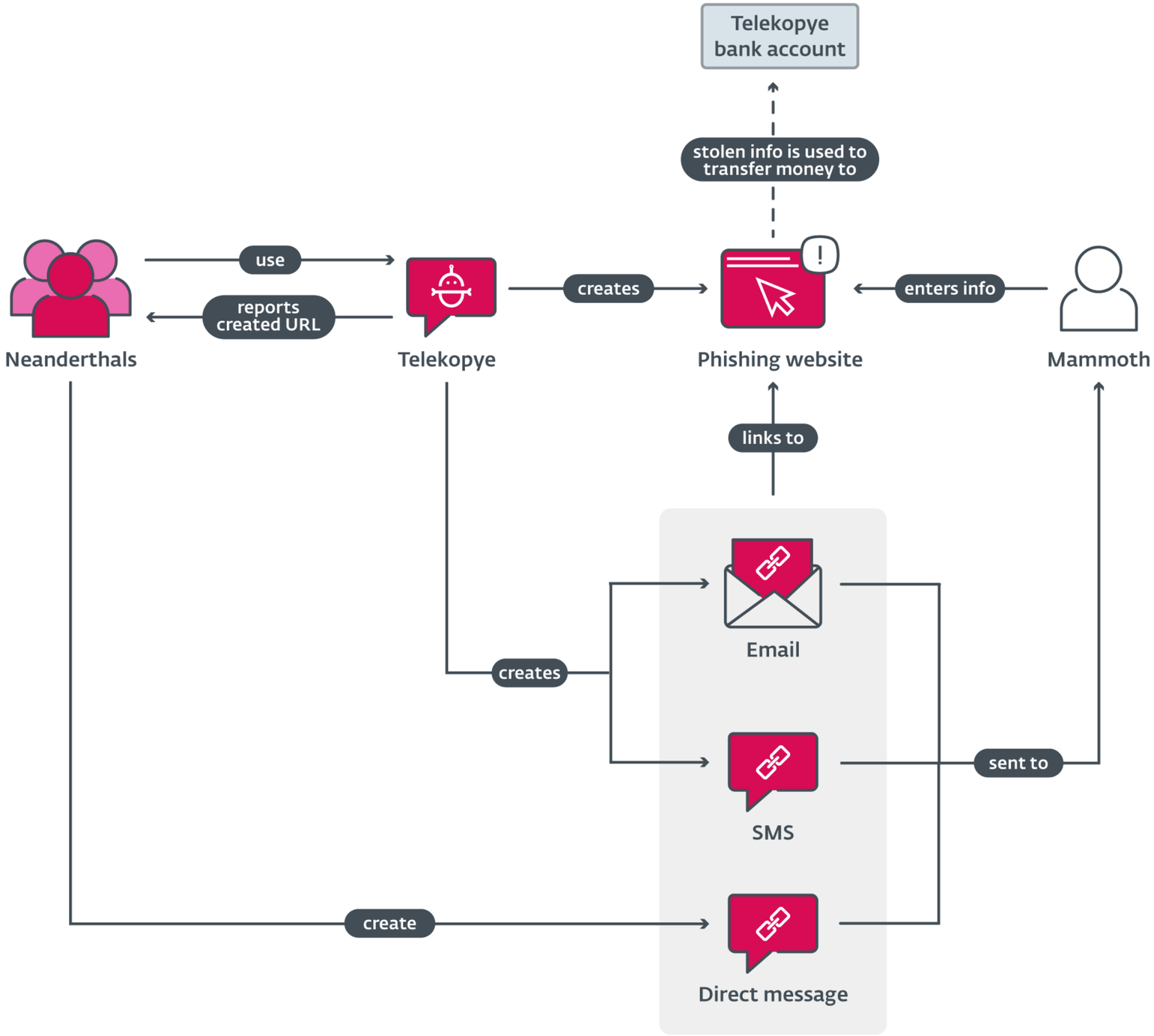
Funcionamiento de Telekopye


Telekopye bank account
stolen info is used to transfer money to
use
reports created URL
creates
enters info
Neanderthals
Telekopye
Phishing website
Mammoth
links to
Email
creates
SMS
sent to
create
Direct message



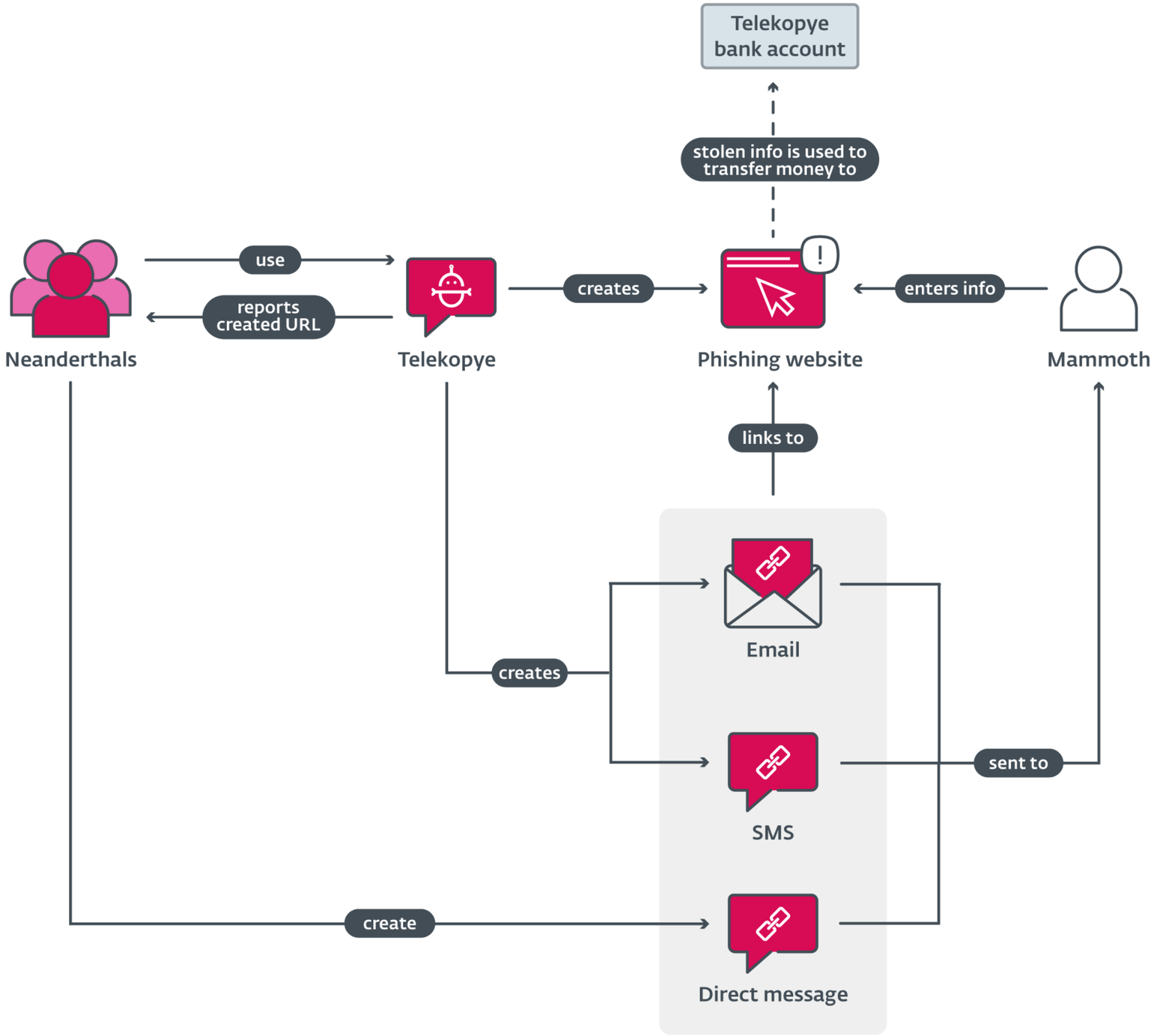
Nean

creates

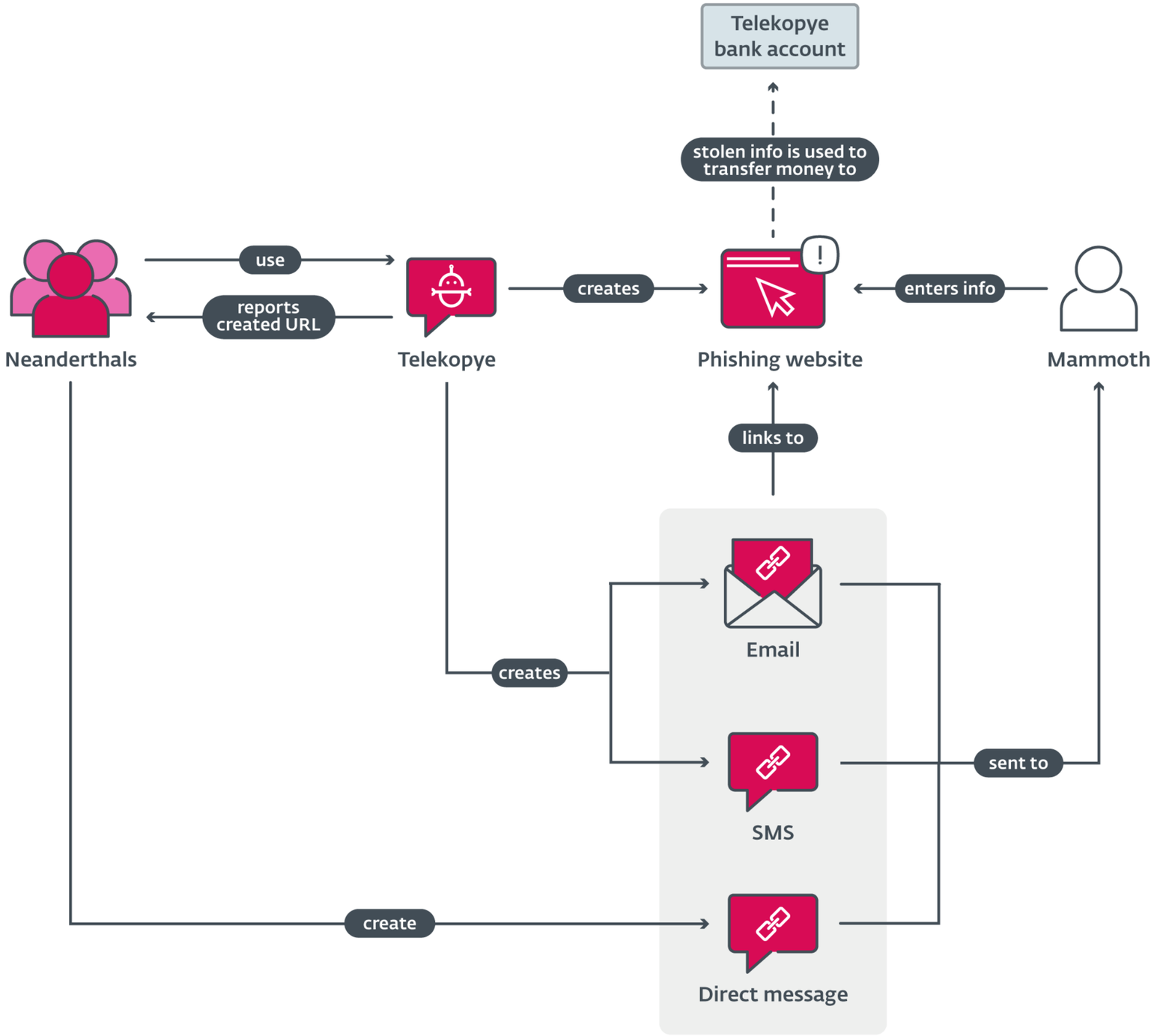

Telekopye bank account
stolen info is used to transfer money to
use
reports created URL
creates
enters info
Neanderthals
Telekopye
Phishing website
Mammoth
links to
Email
creates
SMS
sent to
create
Direct message

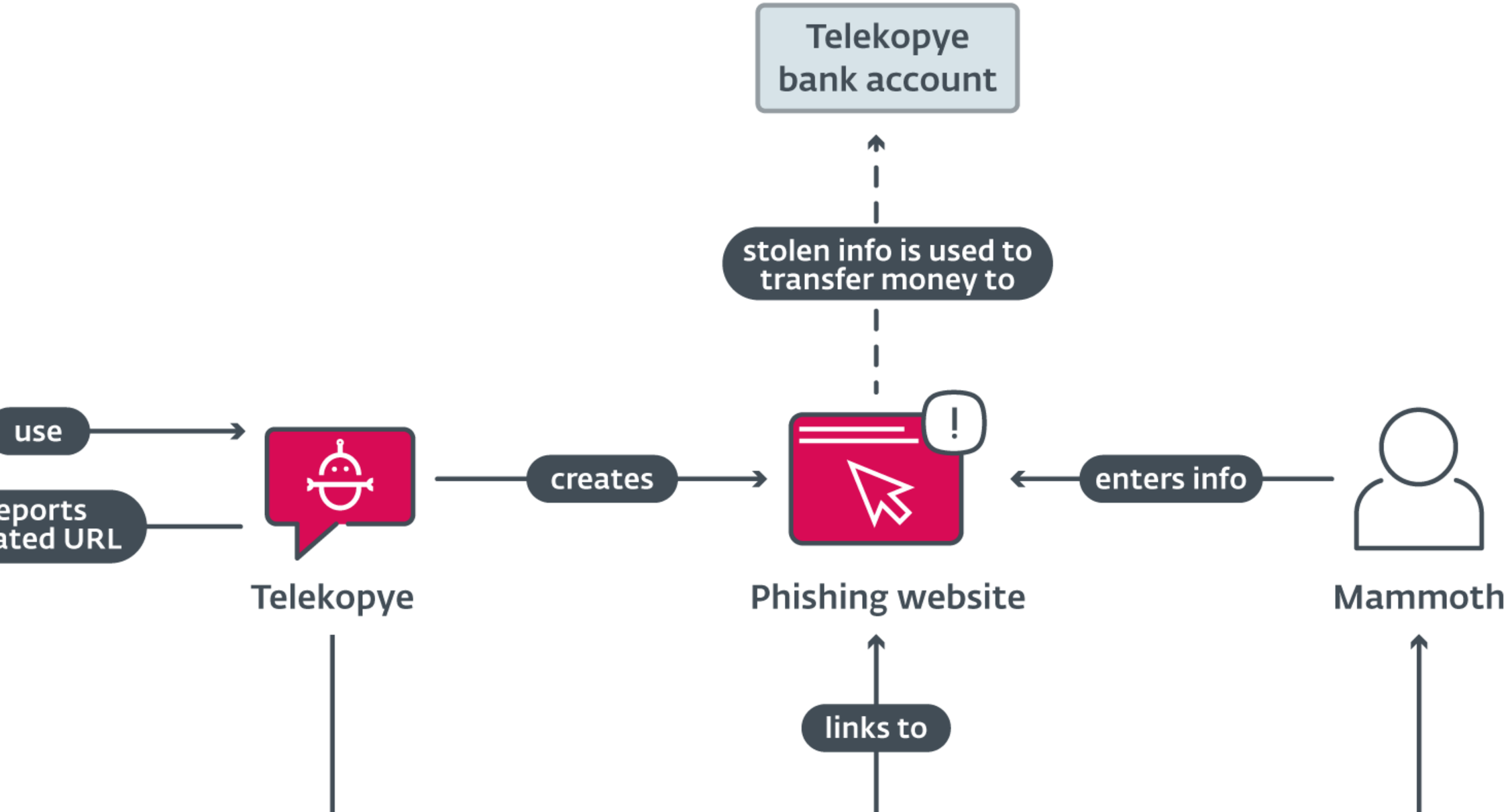

Меню создания ссылок:
22:11
[Link creation menu]
Словакия
[Slovakia]
Испания
[Spain]
Швецария
[Switzerland]
Чехия
[Czech Republic]
Румыния
[Romania]
Болгария
[Bulgaria]
Польша
[Poland]
Германия
[Germany]
Австралия
[Australia]
Англия
[England]
Италия
[Italy]
BlaBlaCar
Назад
[Back]
Выберите сервис:
22:11
[Selected service]
Ebay
Назад
[Back]

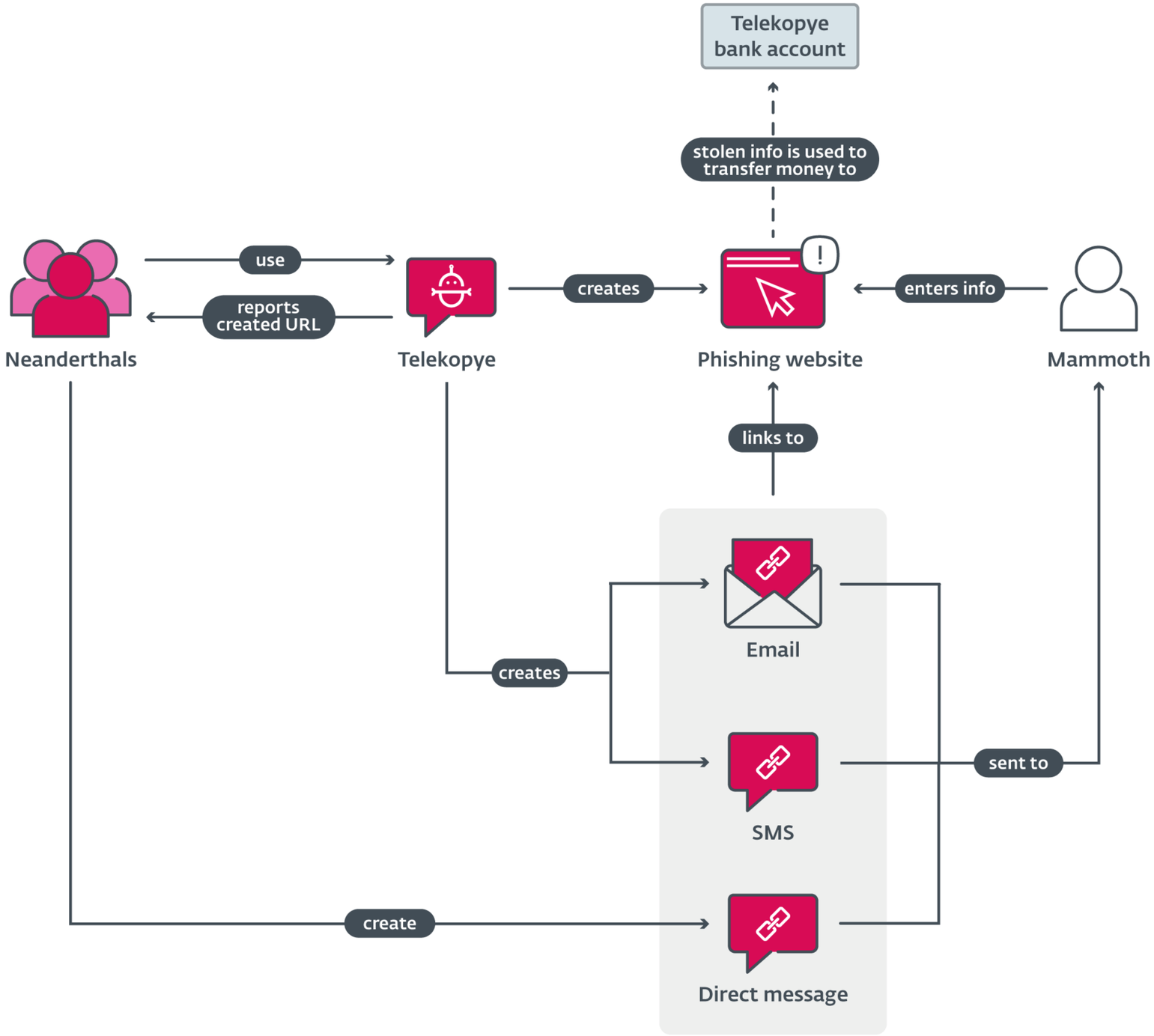
sent to


Telekopye bank account
stolen info is used to transfer money to
use
reports created URL
creates
enters info
Neanderthals
Telekopye
Phishing website
Mammoth
links to
Email
creates
SMS
sent to
create
Direct message

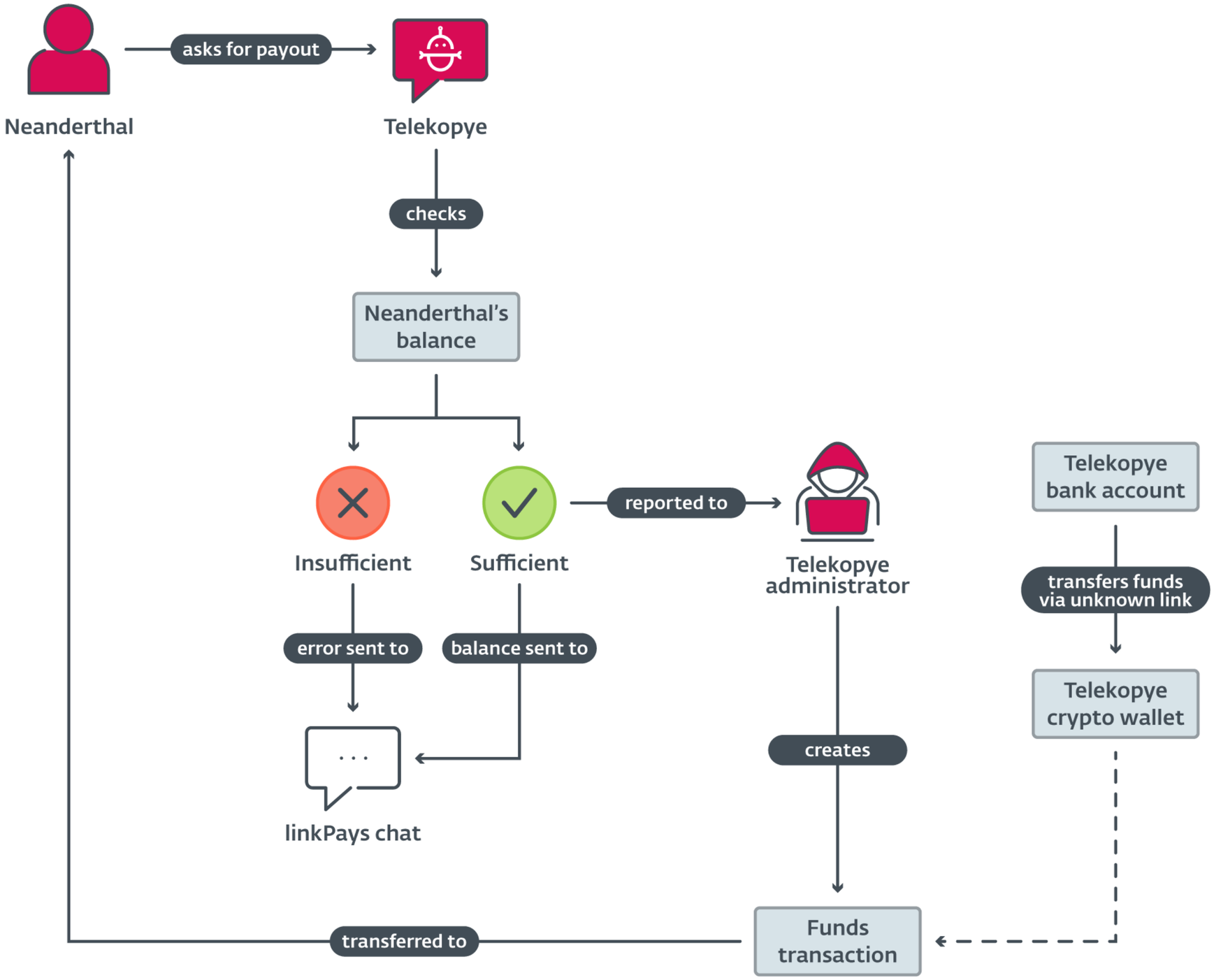

use
reports created URL
creates
Payment by bank card
Total including delivery and VAT
1359.99$
Card number
1234 4567 7890 0000
Card owner
Valid until
MM / ГГ
CVV/CVC
123
three numbers from the back of the card
To pay 1359.99$
creates
ANZ
ANZ Internet Banking
Customer number
Password
Log on
Email
payer24
SecureCode
Подтверждение операции
Магазин YOULA
Сумма 3000 ₽
Номер карты **** **** **** 4979
Комментарий -
Для получения средств на Ваш номер телефона было отправлено SMS сообщение с кодом подтверждения. Введите его в поле ниже.
Введите код из SMS
Запросить повторно через 01:37
Подтвердить
Secure Connection
Verified by VISA
Mastercard SecureCode

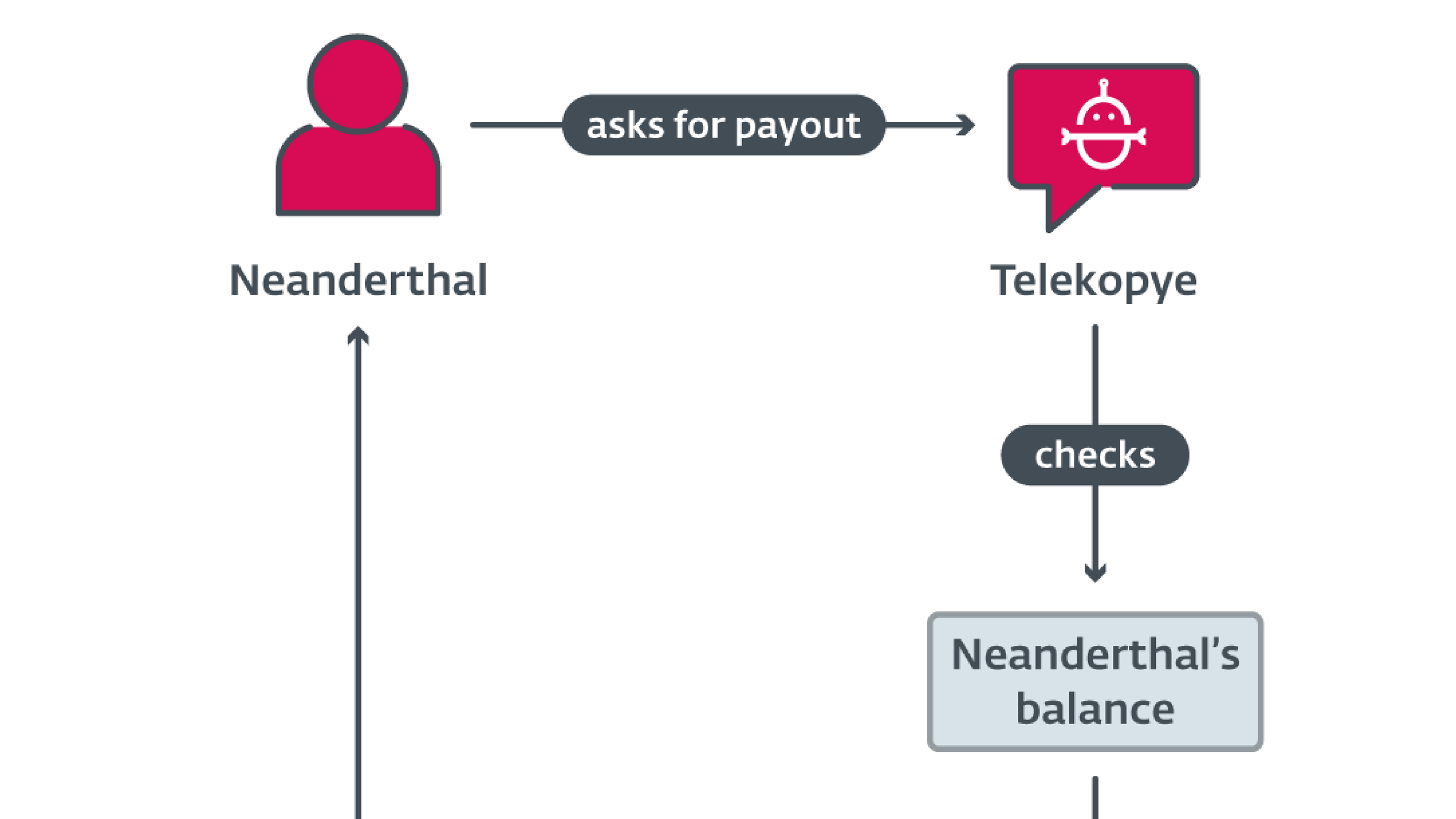

Telekopye bank account
stolen info is used to transfer money to
use
reports created URL
creates
enters info
Neanderthals
Telekopye
Phishing website
Mammoth
links to
Email
creates
SMS
sent to
create
Direct message

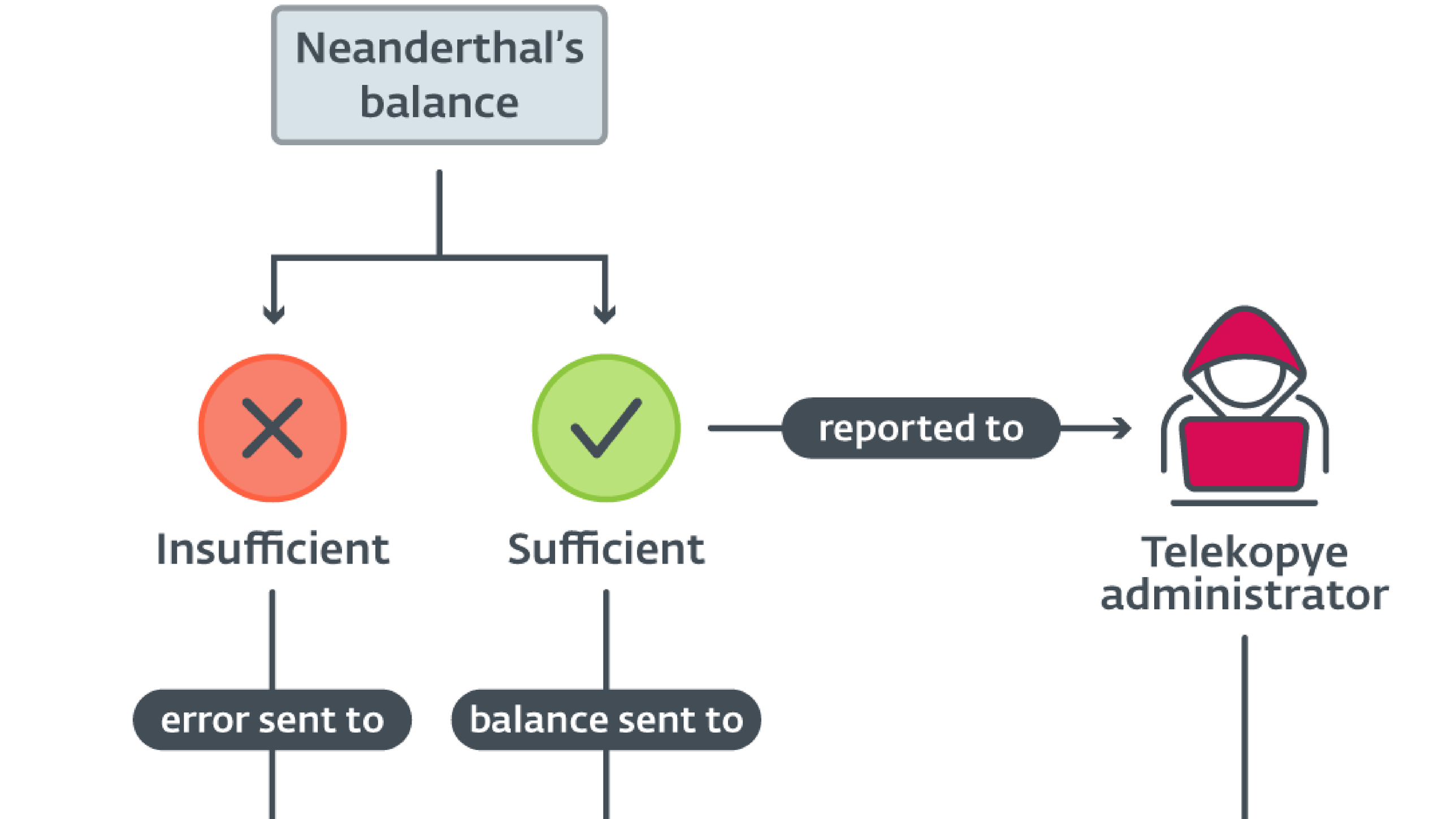

Telekopye
bank account
stolen info is used to
transfer money to
use
eports
ated URL
creates
enters info
Telekopye
Phishing website
Mammoth
links to

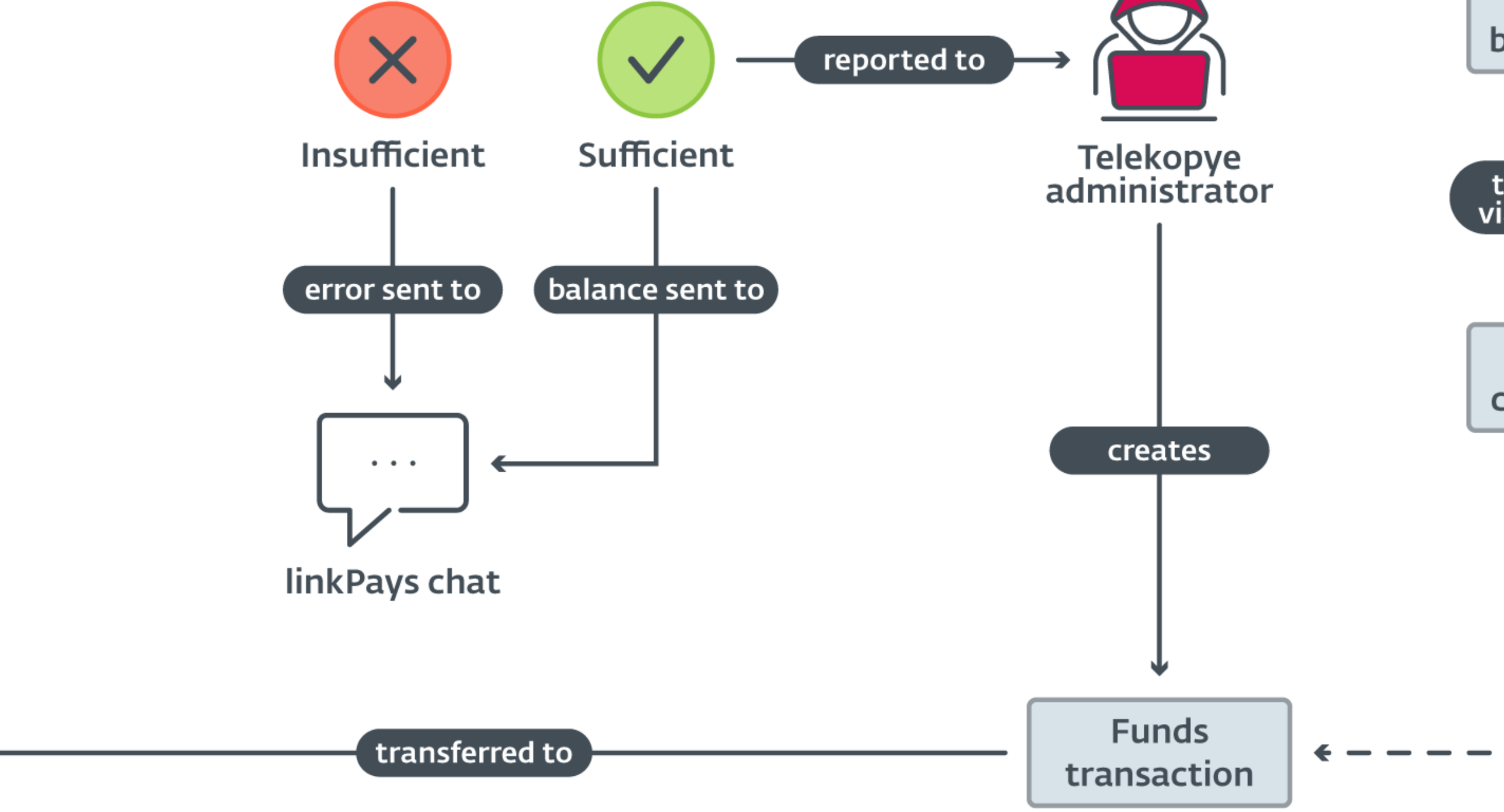

Telekopye bank account
stolen info is used to transfer money to
use
reports created URL
creates
enters info
Neanderthals
Telekopye
Phishing website
Mammoth
links to
Email
creates
SMS
sent to
create
Direct message

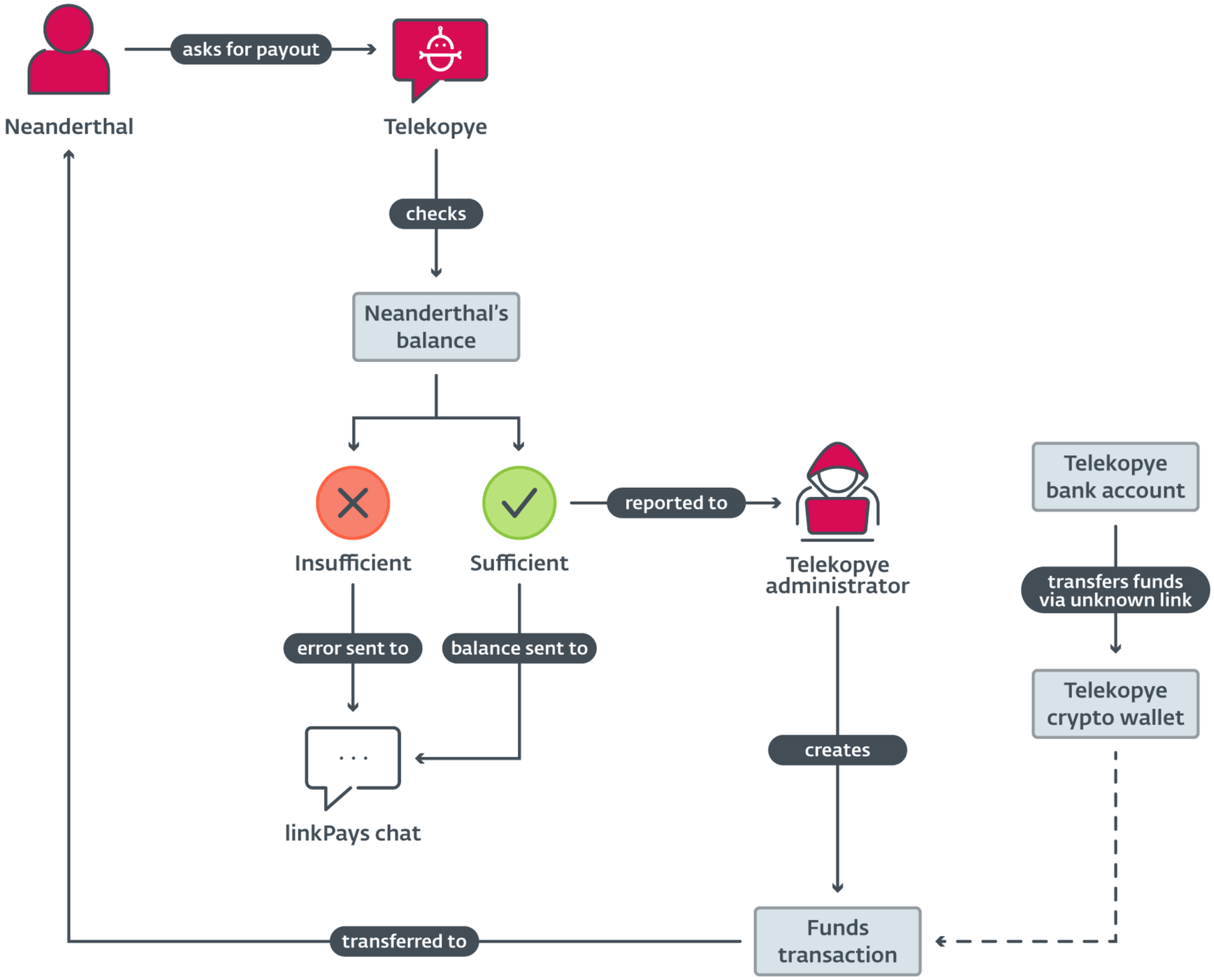
Cómo reciben el pago los neandertales

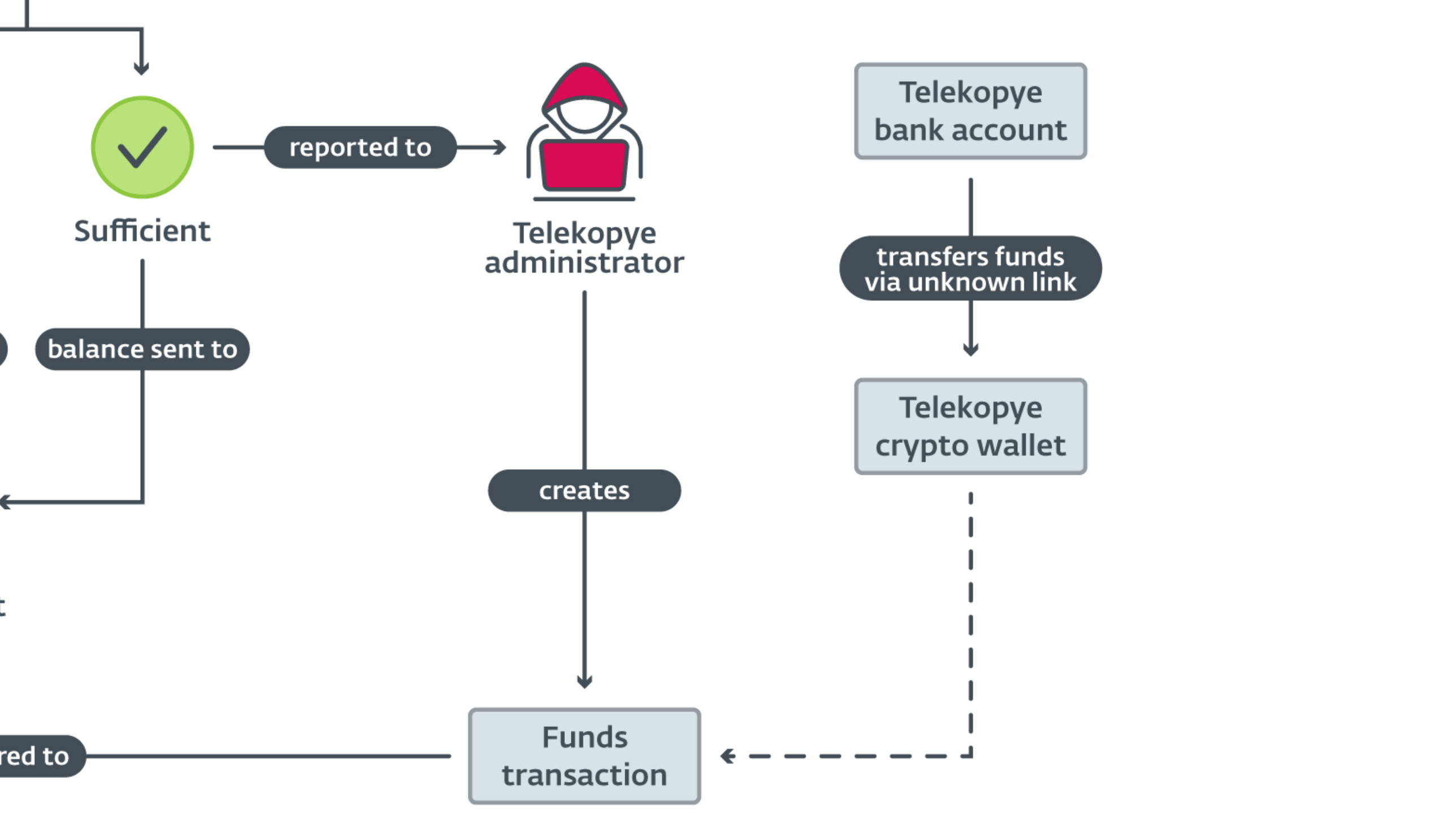

asks for payout
Neanderthal
Telekopye
checks
Neanderthal's balance
Insufficient
Sufficient
reported to
Telekopye administrator
Telekopye bank account
transfers funds via unknown link
Telekopye crypto wallet
error sent to
balance sent to
linkPays chat
creates
Funds transaction
transferred to


asks for payout
Neanderthal
Telekopye
checks
Neanderthal's balance


Neanderthal's balance
Insufficient
Sufficient
reported to
Telekopye administrator
error sent to
balance sent to


Insufficient
Sufficient
reported to
Telekopye administrator
error sent to
balance sent to
linkPays chat
creates
transferred to
Funds transaction


asks for payout
Neanderthal
Telekopye
checks
Neanderthal's balance
Insufficient
Sufficient
reported to
Telekopye administrator
Telekopye bank account
transfers funds via unknown link
Telekopye crypto wallet
error sent to
balance sent to
linkPays chat
creates
Funds transaction
transferred to


Sufficient
reported to
Telekopye administrator
Telekopye bank account
transfers funds via unknown link
Telekopye crypto wallet
balance sent to
creates
Funds transaction

Cómo reciben el pago los neandertales

```
case '/dobalout': {
    $balout = getUserBalanceOut($id);
    if ($balout != 0) {
        $result = [
            //Translation: You have already applied for the payout '.beaCash($balout).', please wait for the check to arrive',
            '❗ Вы уже подавали заявку на выплату '.beaCash($balout).', дождитесь прихода чека',];
        break;
    }
    $balance = getUserBalance($id);
    // Note: Has Neanderthal scammed enough money to be eligitimate to payout?
    if ($balance < baloutMin()) {
        $result = [
            // Translation: Minimum withdrawal amount: beaCash(baloutMin())
            '❗ Минимальная сумма для вывода: '.beaCash(baloutMin()),];
        break;
    }
    setInput($id, 'dobalout1');
    $keybd = [true,[[
            ['text' => $btns['outyes'], 'callback_data' => '/dooutyes'],
            ['text' => $btns['outno'], 'callback_data' => '/dooutno'],],]];
    $result = [
        // Translation: Are you sure you want to apply for a payout?
        '⚠ <b>Вы действительно хотите подать заявку на выплату?</b>', '',
        // Translation: Summa: beaCash($balance)
        '💳 Сумма: <b>'.beaCash($balance).'</b>', '',
        // Translation: The bot will send you a BTC banker check for the specified amount
        '❗ <i>Бот отправит вам чек BTC banker на указанную сумму</i>',];
    break;
}
case '/dooutyes': {
    if (getInput($id) != 'dobalout1')
        break;
    setInput($id, '');
    $balout = getUserBalanceOut($id);
    if ($balout != 0)
        break;
    // Note: Sets scammers balance to 0
    $balance = createBalout($id);
    $dt = date('d.m.Y</b> в <b>H:i:s');
    $result = [
        // Translation: You have applied for a payment
        '✅ <b>Вы подали заявку на выплату</b>', '',
        // Translation: Summa: beaCash($balance)
        '💳 Сумма: <b>'.beaCash($balance).'</b>',
        // Translation: Date: $dt
        '📅 Дата: <b>'.$dt.'</b>',];
    $edit = true;
    // Note: Send to admin that can accept the payout
    botSend([
        // Translation: Application for payment
        '💠 <b>Заявка на выплату</b>', '',
        // Translation: Summa: beaCash($balance)
        '💳 Сумма: <b>'.beaCash($balance).'</b>',
        // Translation: To: userLogin()
        '👤 Кому: <b>'.userLogin($id, true, true).'</b>',
        // Translation: Date: $dt
        '📅 Дата: <b>'.$dt.'</b>',
    ], chatAdmin(), [true, [[
        ['text' => $btns['outaccpt'], 'callback_data' => '/outaccpt '.$id],],]]);
    break;
}
```

16 March 2022

10:31

✅ **Успешная оплата** [Successful payment]

💳 **Сумма платежа:** `18700 RUB` [Payment amount]
🔧 **Сервис:** `wallapop` [Platform]
🥷 **Воркер:** [Worker]

11:35

✅ Бесплатный парсер на Румынию, Болгарию, Словакию, Испанию – [Free parser for Romania, Bulgaria, Slovakia, Spain]

18 March 2022

21:49

✅ **Успешная оплата**

💳 **Сумма платежа:** `18500 RUB`
🔧 **Сервис:** `Ebay`
🥷 **Воркер:**

23 March 2022

20:48

✅ **Успешная оплата**

💳 **Сумма платежа:** `18900 RUB`
🔧 **Сервис:** `ebey`
🥷 **Воркер:**

24 March 2022

20:23

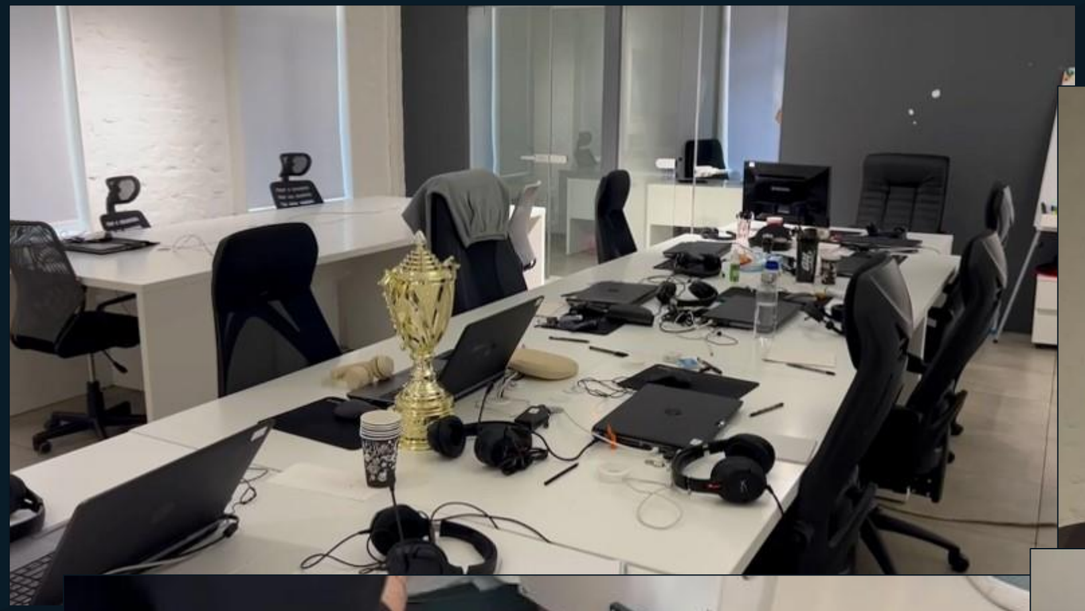
✅ **Успешная оплата**

💳 **Сумма платежа:** `12750 RUB`
🔧 **Сервис:** `Gumtree`
🥷 **Воркер:**

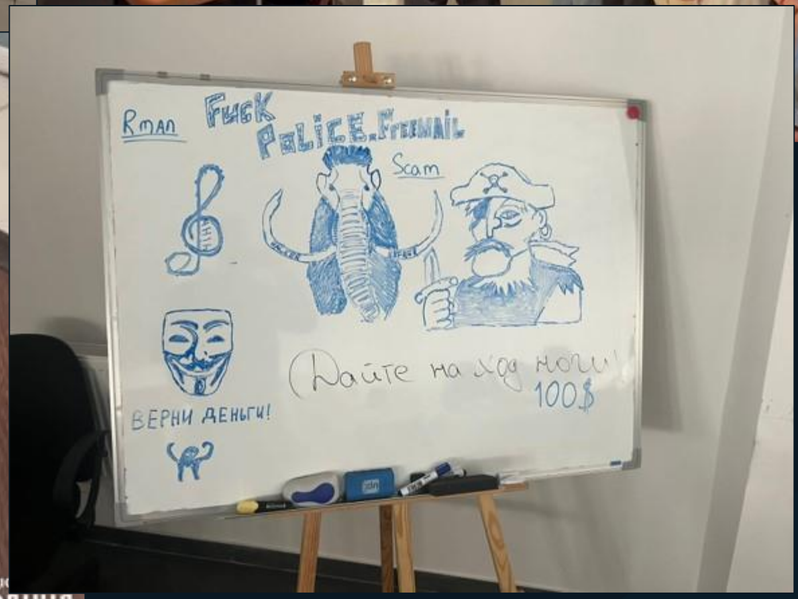
Contraatacando

Operaciones RIP & VICTORY

- Policias de CZ y UA arrestaron a decenas de Neandertales
- Ganancias estimadas de, al menos, €5 mill. desde 2021
- Grupos organizados por hombres de mediana edad de Europa del este y Asia central y occidental.
- Reclutaban a personas en situaciones difíciles.
- Reclutaban en portales de trabajo e incluso en universidades
- Relacionados con la operación “call center” – confiscaban pasaportes, amenazaban a miembros de su familia

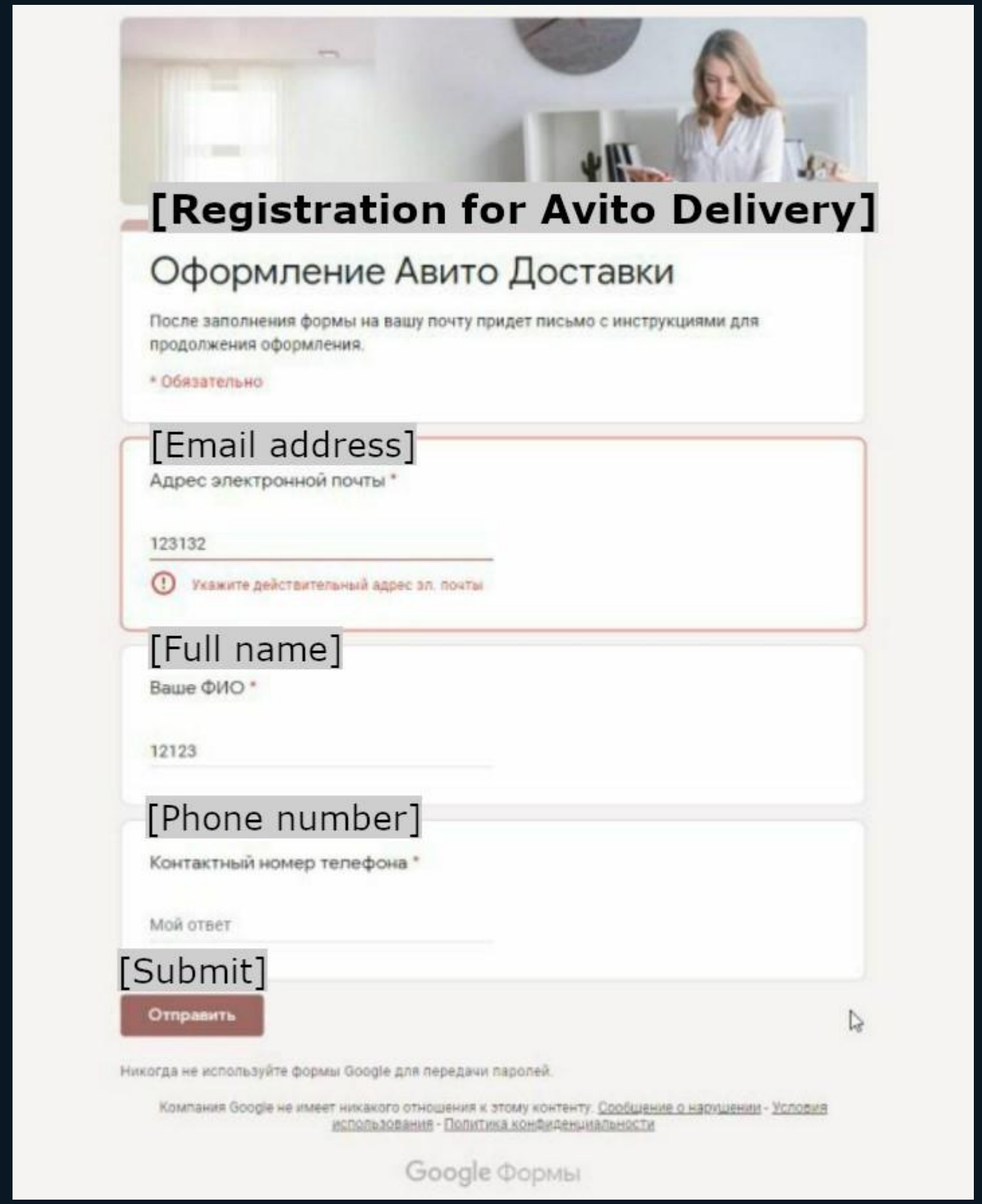



100
100
НАЦІ
ПОЛІЦІЯ


Rman
FuckPoLiCE.Freemail
Scam
ВЕРНИ ДЕНЬГИ!
(Дайте на ход ноги!
100$

Mecanismos de defensa de las plataformas suplantadas

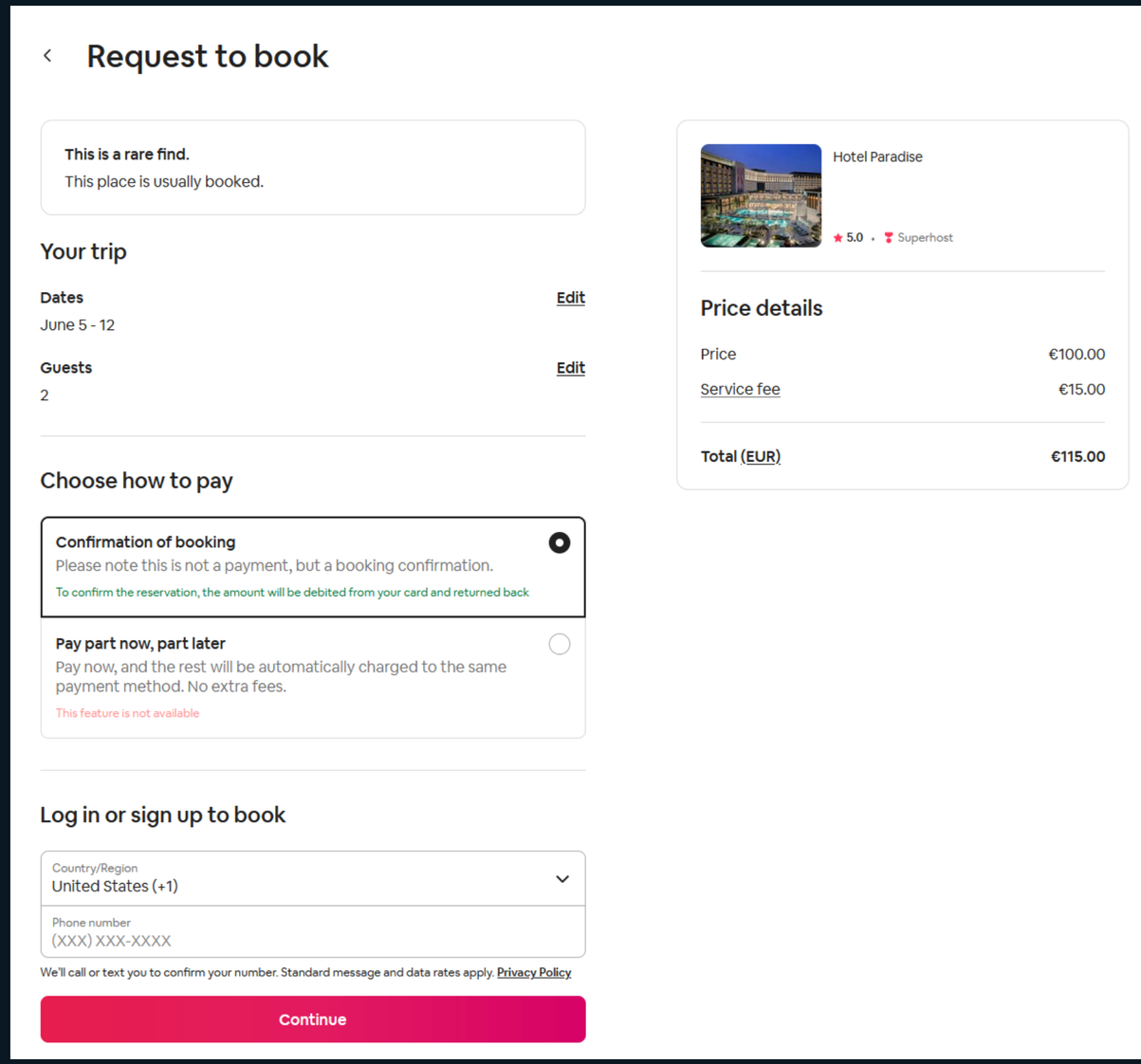
- ESET estuvo en contacto con varias de las plataformas afectadas. Estas eran plenamente conscientes de la situación y no se encontraban indefensas.
- Técnicas
  - Verificación de usuarios
  - Visualización de información de los usuarios
  - Chat dentro de la plataforma
- Problema principal: cantidad y velocidad
- Ejemplo:
  - Plataforma con unos pocos millones de usuarios
  - Hasta 1.000 usuarios selecionados como objetivos cada día, centrándose en los nuevos
  - En ocasiones, más de la mitad de esos usuarios son atacados al día
  - Al menos 14 grupos tienen a esta plataforma como objetivo
  - Mas de 100 nuevos dominios al día



Expansion – servicios de alojamiento

Escenario de los servicios de alojamiento

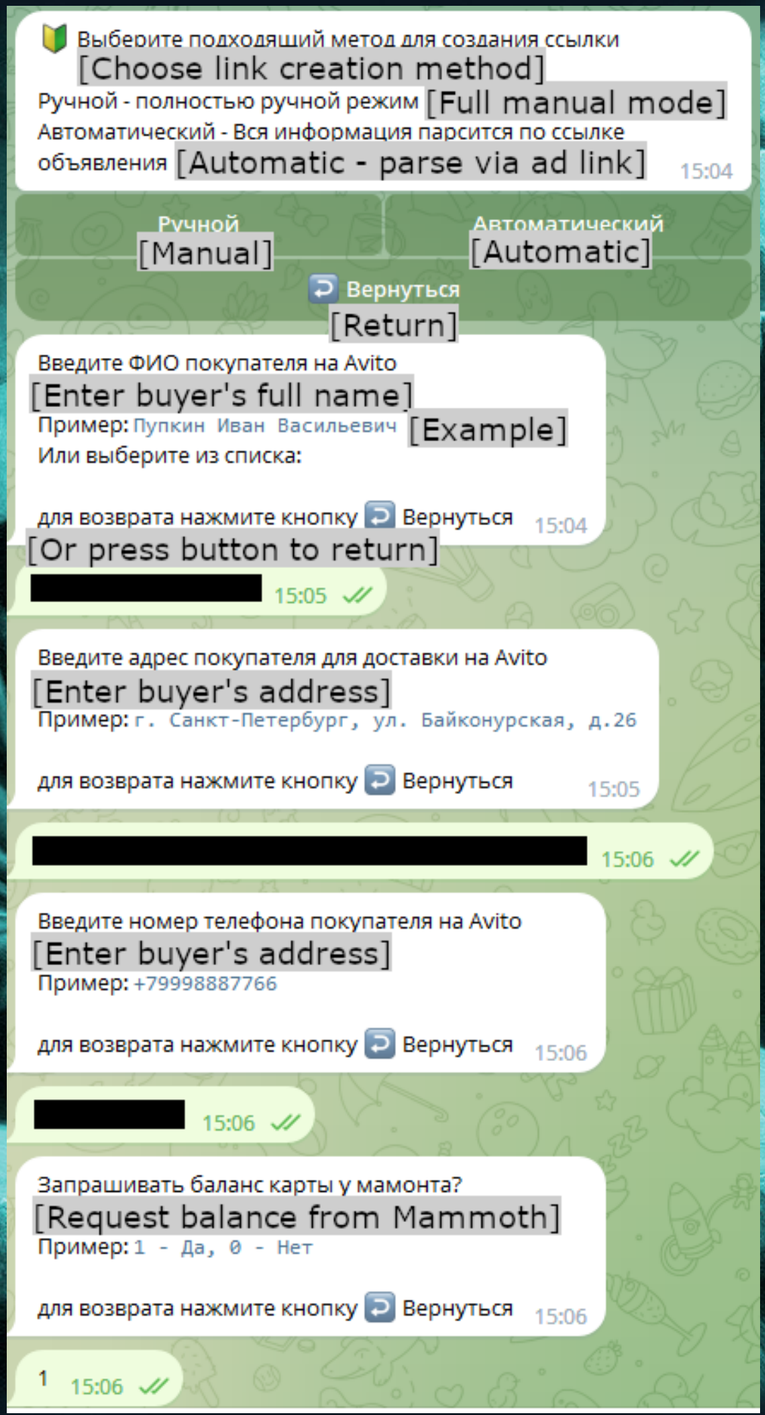
- Adquisición de credenciales de anunciantes en webs de alojamientos
- Dirigido a usuarios que:
  - Reservaron su alojamiento recientemente y lo pagaron
  - Reservaron su alojamiento recientemente y no lo pagaron todavía
- Creación de webs de phishing muy dirigidas
  - Datos ya proporcionados como fechas, Información de los huéspedes, precios, etc…
- Presión para realizar el pago
  - Problemas con el pago
  - Pocas habitaciones disponibles



Características personalizadas

Rapidez en la generación

- Aproximación tradicional = rellenar un cuestionario
  - Nombre del mamut
  - Nombre del artículo
  - Imagen del artículo
  - Precio del artículo
- Los neandertales desarrollaron analizadores para los mercados online más populares
- Con la URL es suficiente
- Aumento significativo de la velocidad de generación de webs de phishing



Archived chats

GIPSY | Mo... 1:14 PM
GIPSY оплата ... 1571

SIZO TEAM | BOT 1:11 PM
Переход на ввод карты...

Diverolli Family... 1:07 PM
Diverolli Family | Bo... 14107

MONCLER TEA... 1:06 PM
MONCLER TEAM: ... 7733

Marvel Team • ... 1:06 PM
Marvel Team • Бот ... 21166

ЧАТ | HAU... 12:30 PM
HF MODER: Sticker 2034

GRAND PROJE... 11:57 AM
ОТДАДИМ 10 К... 50

SIZO TEA... 11:36 AM
SZT | Smotryaga: У Г... 41412

Diverolli Fami... 10:13 AM
Добрый день D... 83

DarkSpire • Pay... 9:56 AM
Успешный залет! ... 104

LIMUR SHOP 9:51 AM
04.08 | Анаста... 176

MONCLER TEAM 9:39 AM
FULL WORK 113

DarkSpire_BOT 9:10 AM
FULL WORK ... 112

CHAT WITCHER... 9:00 AM
Group Help: НОЧН... 11

Fairy tales of th... 9:06 PM
Венгрию позаводил ... 566

PAYS / HUSTLE... 6:27 PM
Успешная опл... 191

SIZO TEAM | BOT
bot

Что бы приступить к работе воспользуйтесь кнопками ниже. 12:36 PM

Рабочая панель 12:46 PM

❌ Действие отменено. 12:46 PM

/start 1:10 PM

С возвращением, @Sinolly:

Что бы приступить к работе воспользуйтесь кнопками ниже. 1:10 PM

Рабочая панель 1:10 PM

Сбор данных... 1:11 PM

⚠️ Внимание!

Подтвердите удаление всех ссылок 1:11 PM

❌ Подтвердить удаление всех объявлений

Переход по ссылке

Vinted 2.0: 253394906
Название: adidas Gazelle Indoor Orange/Mint
Стоимость: £60.00

IP: 185.209.199.83 (Sweden)
Устройство: PC, Firefox, Windows 10.0 1:11 PM

Проверить

Написать в ТП

Переход на ввод карты

Платформа: Vinted
Объявление: adidas Gazelle Indoor Orange/Mint
ID Объявления: 253394906
Цена: £60.00

IP: 185.209.199.83 (Sweden)
Устройство: PC, Firefox, Windows 10.0 1:11 PM

Проверить

Написать в ТП

Menu

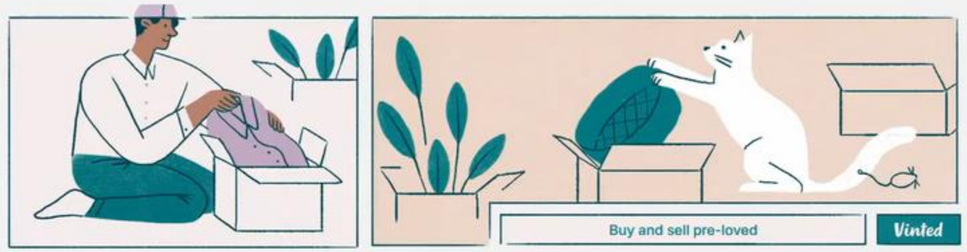
Write a message...

Dr martens ASHA sandals | Vint

https://www.vinted.co.uk/items/4853809669-dr-martens-asha-sandals?homepage_session_id=9058ceb4-2b5f-49ff-84fd

Vinted Catalogue Search for items Sign up | Log in Sell now

Women Men Designer Kids Home Entertainment Pet care About Our Platform



£40.00
£42.70
Includes Buyer Protection

BRAND	DR. MARTENS
SIZE	6
CONDITION	GOOD
MATERIAL	LEATHER
COLOUR	BLACK
LOCATION	PONTEFRACT, UNITED KINGDOM
PAYMENT OPTIONS	CREDIT CARD
VIEWS	26
INTERESTED	2 MEMBERS
UPLOADED	43 MINUTES AGO

Dr martens ASHA sandals

Well worn in but with lots of life left, super comfy

Postage from £2.49

Buy now

Make an offer

Ask seller

Buyer Protection fee
Our Buyer Protection is added for a fee to every purchase made with the "Buy now" button. Buyer Protection includes our Refund Policy.

Home / Women / Shoes / Sandals / Dr. Martens Sandals

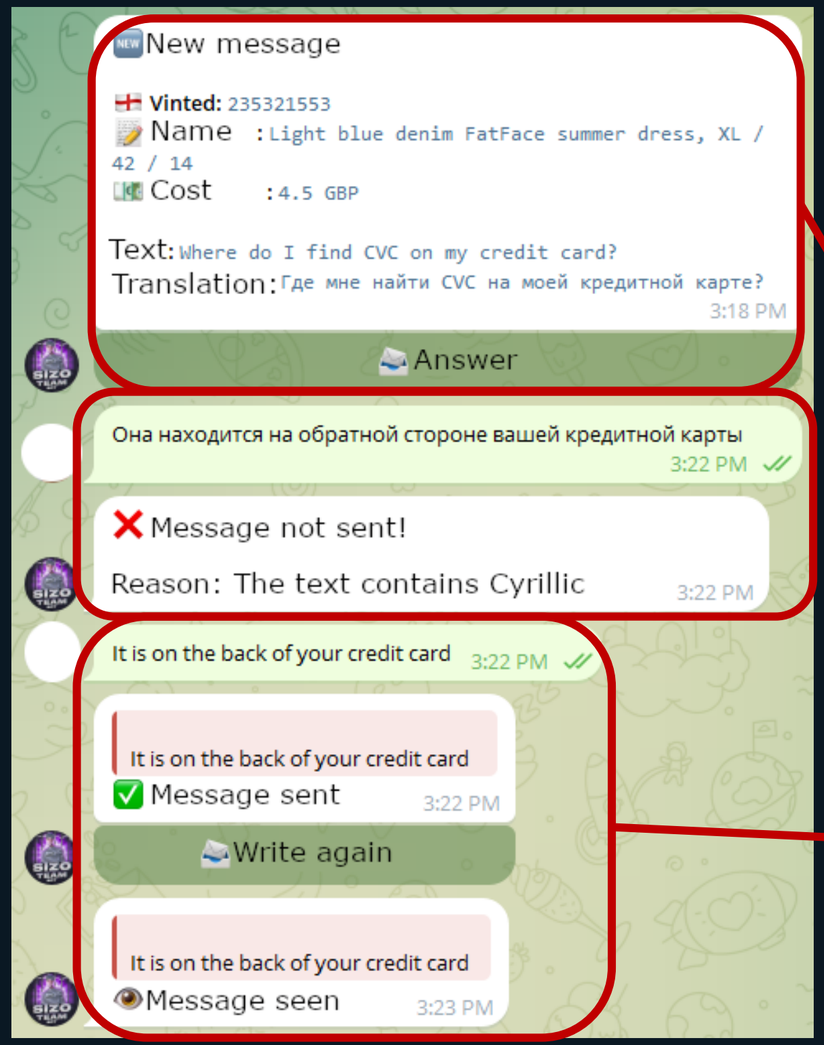
Member's Items (39)

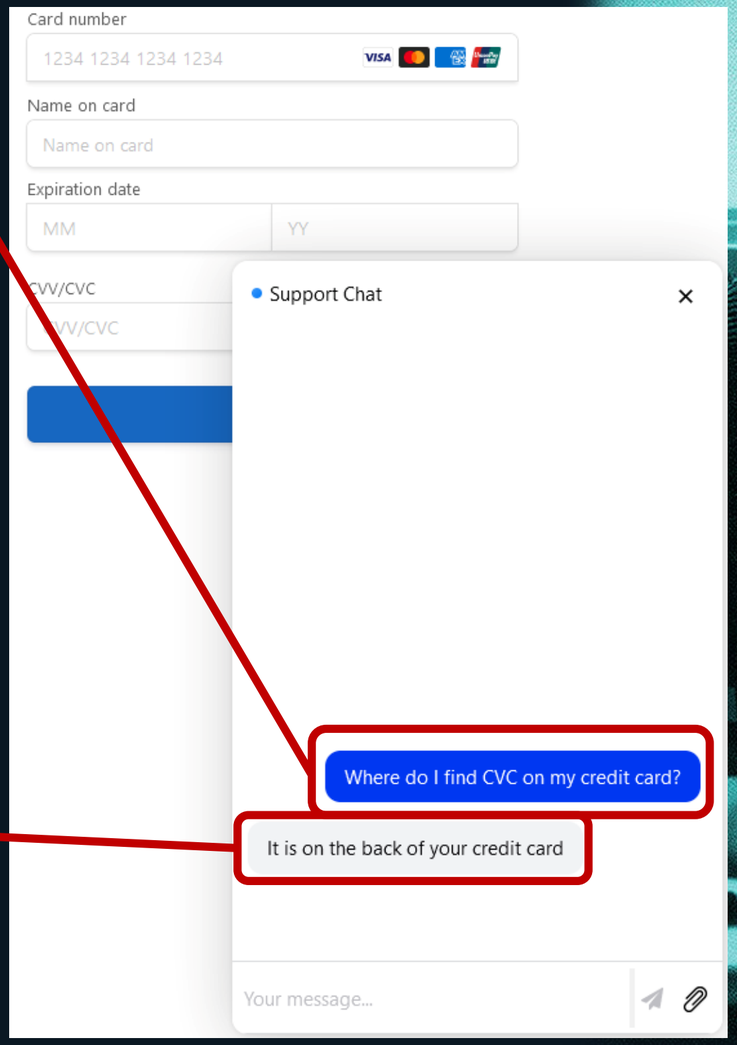
cowgirlrae cowgirlrae cowgirlrae cowgirlrae

Type here to search

1:15 PM 8/6/2024

Chatbot con traducción automática





Archived chats

SIZO TEAM | BOT 1:58 PM
Переход по ссылке ...

LIMUR SHOP 1:51 PM
ОТДАДИМ 10 К... 177

Diverolli Family... 1:38 PM
Diverolli Family | Bo... 14116

Fairy tales of th... 1:30 PM
Как легко заставить л... 567

MONCLER TEA... 1:22 PM
MONCLER TEAM: ... 7734

GIPSY | Mo... 1:14 PM
GIPSY оплата ... 1571

Marvel Team • ... 1:06 PM
Marvel Team • Бот ... 21166

ЧАТ | HAU... 12:30 PM
HF MODER: Sticker 2034

GRAND PROJE... 11:57 AM
ОТДАДИМ 10 К... 50

SIZO TEA... 11:36 AM
SZT| Smotryaga: У Г... 41412

Diverolli Fami... 10:13 AM
Добрый день D... 83

DarkSpire • Pay... 9:56 AM
Успешный залет! ... 104

MONCLER TEAM 9:39 AM
FULL WORK 113

DarkSpire_BOT 9:10 AM
FULL WORK ... 112

CHAT WITCHER... 9:00 AM
Group Help: НОЧН... 11

PAYS / HUSTLE... 6:27 PM
Успешная опл... 191

SIZO TEAM | BOT
bot

Сбор данных... 1:58 PM

Vinted 2.0

Название: Dr martens ASHA sandals
Стоимость: £40.00

Ссылки: Фейк ссылка / / Возврат
UNI-Ссылка: https://vinted-uk.i9d48120.info/218862098
OFFI-Link: https://vinted.co.uk@i9d48120.info/218862098

Сокращенные ссылки:

https://offers-8731.info/m1M5w (Обычное)
https://offers-8731.info/m1M5w (UNI)
https://vinted.co.uk@offers-8731.info/m1M5w (OFFI) 1:58 PM

Повторить создание ссылки
YOUR MAILER
APEX MAILER | Anafema Mailer
Meow SMS
DEPA SMS | MOONHEIM SMS
Проверить ссылку на КТ | Сгенерировать QR-код
Выключить чекер баланса
Изменить цену
Удалить объявление
Вернуться в список

Переход по ссылке

Vinted 2.0: 218862098
Название: Dr martens ASHA sandals
Стоимость: £40.00

IP: 185.209.199.83 (Sweden)
Устройство: PC, Firefox, Windows 10.0 1:58 PM

Проверить
Написать в ТП

Menu | Write a message...

Dr martens ASHA sandals | Vint | Vinted | Dr martens ASHA sand

https://vinted-uk.i9d48120.info/order/218862098

Vinted | Catalogue | Search in "Men" | Sell now | EN

Women Men Kids Home Entertainment Pet care About Our Platform

Your product has been purchased

Dr martens ASHA sandals
Total funds receivable:
£40.00

The buyer has already paid for your product, the money is safe, get it.

Obtain Money

Secure purchase system

The purchase was paid through our secure purchase system. Is it the first time you use it? Read the brief introduction to stay informed.

Vinted
About us
Jobs
Sustainability
Press
Advertising

Discover
How it works
Mobile apps
Help Centre
Infoboard
Vinted Pro
Vinted Pro guide

Help
Help Centre
Selling
Buying
Trust and Safety

Community
Forum
My topics

Download on the App Store | GET IT ON Google Play

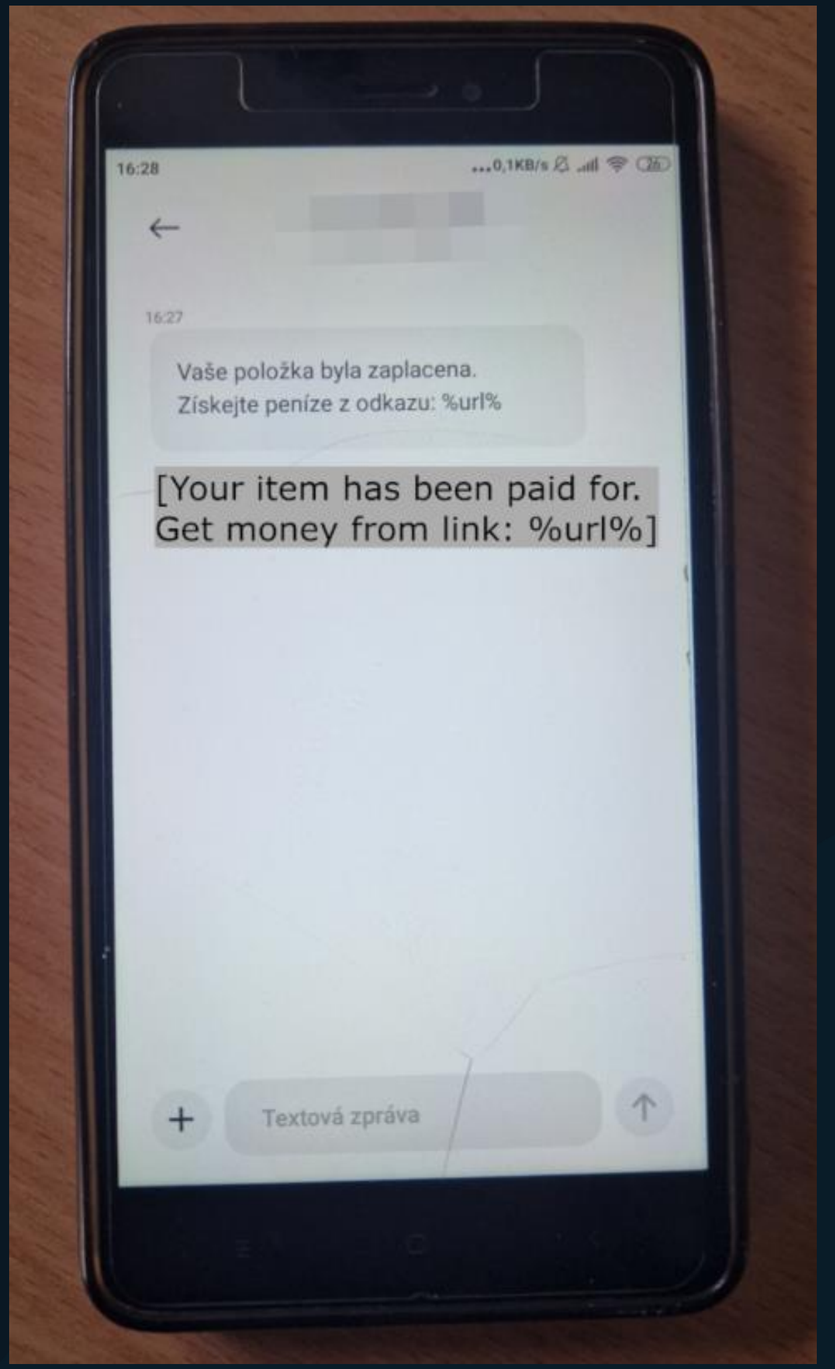
Privacy Policy Cookie Policy Cookie Settings Terms & Conditions Our Platform Pro terms of sale Pro terms of use

Type here to search

1:59 PM 8/6/2024

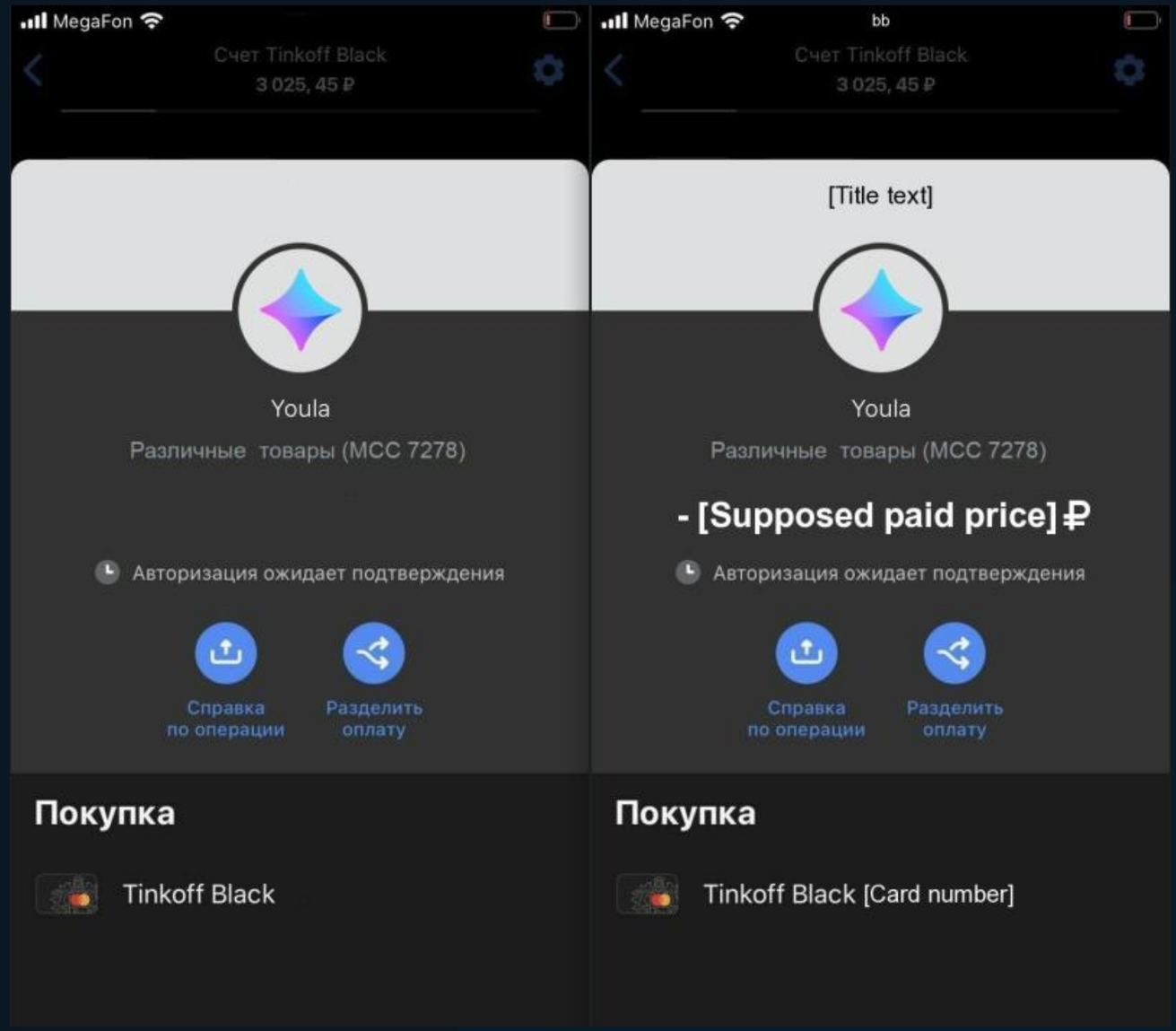
Envío de SMS

```
function smsTexts() {
    return [
        // Translation: Product payment form:
        'Форма для оплаты товара: %url%',
        // Translation: Refund form:
        'Форма для возврата средств: %url%',
        // Translation: Your item has been paid for. To receive funds, fill out the form:
        'Ваш товар оплачен. Для получения средств заполните форму: %url%',
        // Translation: For a refund fill out the form:
        'Для возврата средств заполните форму: %url%',
        // Translation: Form to conclude a secure transaction:
        'Форма для заключения безопасной сделки: %url%',
    ];
}
```



Manipulación de imágenes

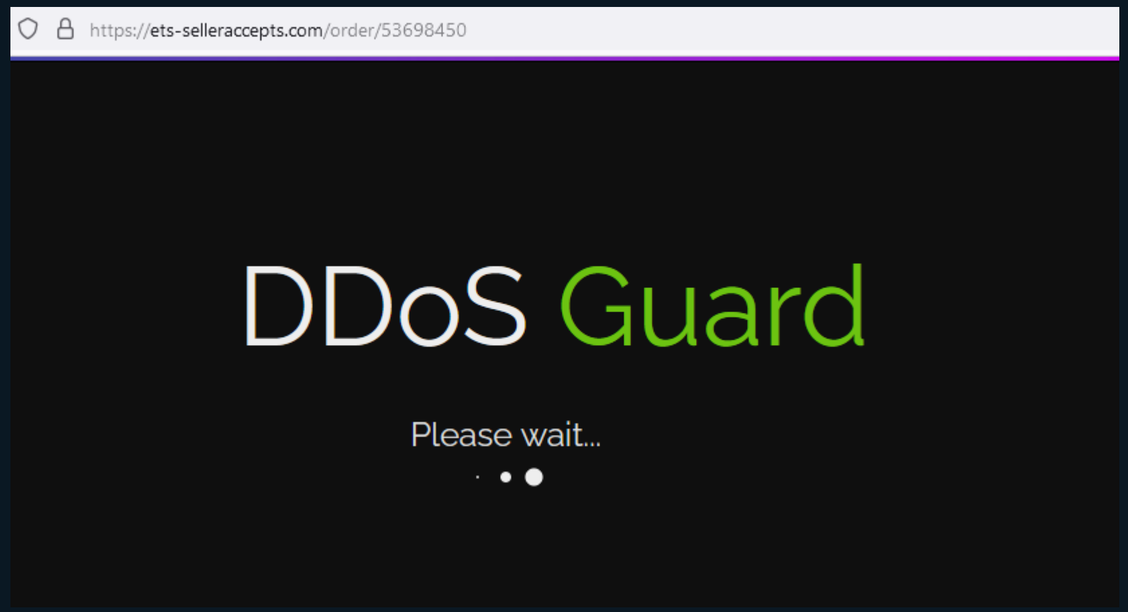
```
$startmsg = [
    // Translation: Render Bot
    '🎨 <b>Бот отрисовок</b>',
    // Translation: In this section you can:
    '<b>📂 В данном разделе вы можете:',
    // Translation: Create fake checks of Sberbank, QIWI and other banks
    '🔸 Создавать фейковые чеки Сбербанка, QIWI и других банков',
    // Translation: Create fake receipts for Avito and Yula with Tinkoff
    '🔸 Создавать фейковые чеки Авито и Юлы с Тинькофф',
    // Translation: Create fake OLX.UA checks with PrivatBank and Monobank
    '🔸 Создавать фейковые чеки OLX.UA с ПриватБанк и Монобанк',
    // Translation: Edit photos to bypass moderation
    '🔸 Редактировать фотографии для обхода модерации',
    // Translation: Make fake emails from Yula and Avito
    '🔸 Сделать фейковые письма Юлы и Авито</b>'
];
```



Manipulación de imágenes

Protección DDoS

- Demasiados mamuts al mismo tiempo no son un problema
- El verdadero problema es la competencia
- Los grupos competidores realizan ataques DDoS ocasinalmente a las webs de phishing



Generación desde web

GREEDY RENT

Auth key: bae***fe116

Manual mode | Parser

Service name
DPD

Country
Хорватия

Version
2.0

Product name
Nintendo Switch Lite

Creation date
04.08.2024

Transaction date
06.08.2024

Delivery address
Hickory Street 3, Philadelphia

Price
20 €

Create Ad

Request status Completed

UNI-link https://dpd.onlyoffer-check.com/22290733

link https://dpd.onlyoffer-check.com/order/22290733

Generate QR cod

Copy link | Download

Cómo protegernos

En las plataformas de compras online

- Ser extramadamente cuidadosos si es la primera vez que compramos
- Buscar errores gramaticales
- Cuidado con los compradores / vendedores excesivamente ansiosos
- Verificar el historial de la persona con la que estamos tratando
  - Historial en la plataforma
  - Antigüedad de su cuenta
  - Puntuación
  - Ubicación
- Tener en cuenta que los neandertales también usan cuentas robadas
- Insistir en las compras/ventas en persona siempre que sea posible
- En caso contrario
  - Vendedor → gestionar las opciones de envío personalmente
  - Comprador → pago a la recepción del artículo o contratar seguro
- No abandonar la plataforma

Fuera de las plataformas

- Algunas plataformas, principalmente por cuestiones de legado, redirigen a la comunicación via email tras cerrarse un trato
- Apps de mensajería populares como WhatsApp deberían ser consideradas como banderas rojas
  - “Estoy de viaje de negocios”
  - “Tengo que dejar de trabajar desde mi ordenador”
- Comprobar muy bien cada enlace

En la web de phishing

- Poner atención adicional a:
  - La URL
  - Contenido
  - Certificado
  - Fecha de creación
- Se puede probar a introducir datos inválidos y observar a ver que sucede
- Contar con una solución de seguridad
- Revisar opiniones de terceros y servicios especializados
- Si no se está seguro, contactar con nuestro banco / proveedor de medios de pago

Cuando hemos sido estafados

- Presentar denuncia en la Policía
- Informar del caso a nuestro banco, adjuntando la denuncia
- Hacerlo lo antes posible, para ver si aun se puede recuperar el dinero
- Los bancos valoran estas denuncias, ya que pueden informar a otros usuarios de la estafa
- No eliminar ninguna prueba de nuestro dispositivo y proporcionar toda la Información posible a la Policía si:
  - Se ha compartido Información confidencial
  - Se ha producido un daño económico
  - Se dispone de Información valiosa para iniciar una posible investigación

Conclusión

Conclusion

- Telekopye es responsable de una porción importante de los fraudes en mercados online
- La preparación de la estafa es rápida y sencilla
- Los grupos de estafadores están bien organizados
- Los neandertales se están adaptando y expandiendo
- La major defensa es estar informado de estas estafas y prepararse en consecuencia

Jakub Souček

Senior Malware Researcher & Manager

Martin Knotek

Malware Analyst (APT)

Radek Jizba

Malware Researcher

Q & A

Telekopye: Hunting Mammoths using Telegram bot

[2023-08-24]

Telekopye: Chamber of Neanderthals’ secrets

[2023-11-23]

Josep Albors

Responsable de investigación y concienciación
ESET España

@josepalbors

mypublicinbox.com/JosepAlbors

Digital Security
Progress. Protected.