ШКОЛА КІБЕРБЕЗПЕКИ

EMA

ПРОЕКТЫ

ПО ОБУЧЕНИЮ НАСЕЛЕНИЯ БЕЗОПАСНЫМ БЕЗНАЛИЧНЫМ РАСЧЕТАМ

Автор: Раиса Федоровская

EMA

Плати безопасно!

Наша миссия:

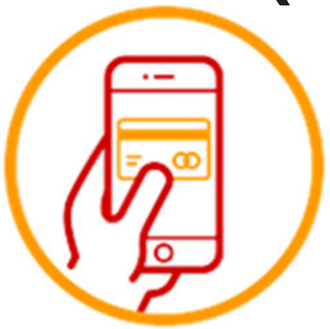
всестороннее содействие развитию
безналичных платежных инструментов и сервисов в Украине

ЧЛЕНЫ «ЕМА»

Банки (40+)

Платежные системы

Платежные сервисы и компании (20+)



Основные партнеры Ассоциации «ЕМА»

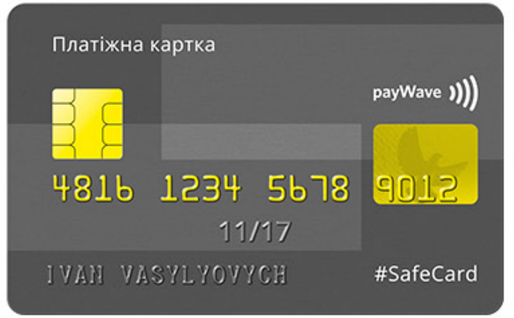
НАШИ ПРОЕКТЫ

По обучению населения безопасным безналичным расчётам

ШКОЛА КІБЕРБЕЗПЕКИ

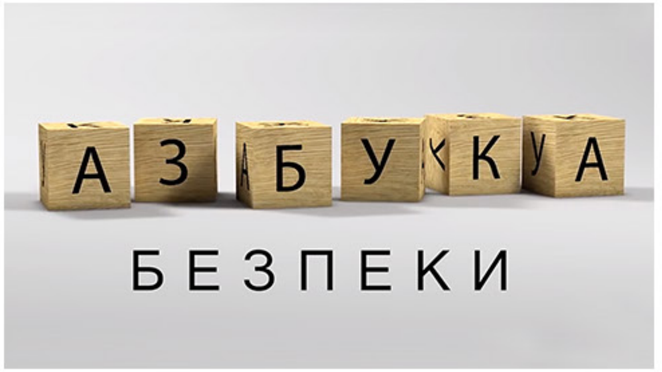
BLACK SQUIRREL

ПЕРШИЙ АНТИШАХРАЙСЬКИЙ ТЕЛЕСЕРІАЛ



EMA Academy

ГУМАННИЙ ЛІНІФ



СОЦИНЖЕНЕРИЯ — КИБЕРОРУЖИЕ #1 XXI в.

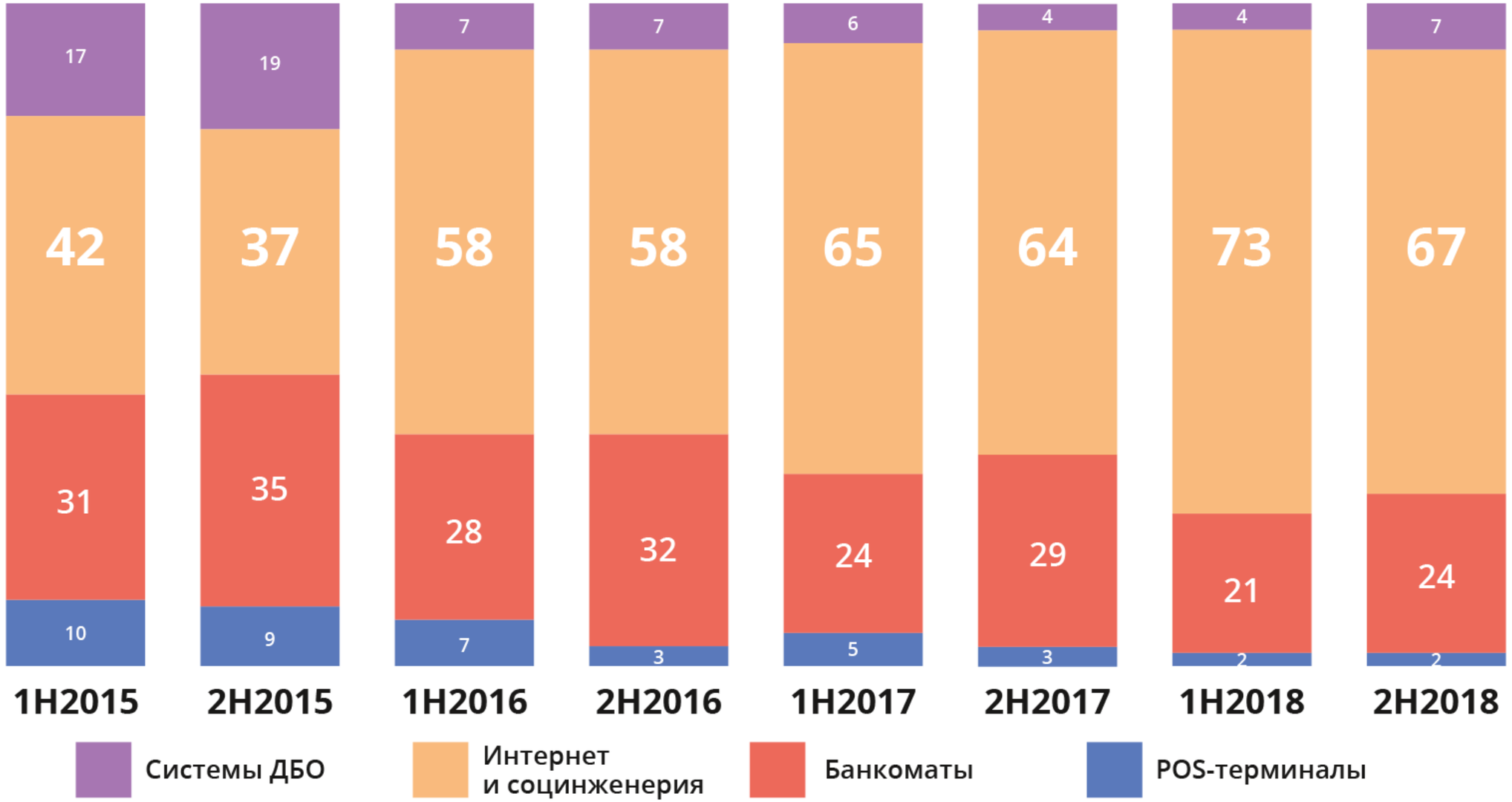
ВЗЛОМ МОЗГОВ

ШКОЛА КІБЕРБЕЗПЕКИ

EMA

КИБЕРМОШЕННИЧЕСТВО В УКРАИНЕ

Красноречивая статистика (данные Exchange-Online)



КИБЕРМОШЕННИЧЕСТВО В МИРЕ

2018 Social Engineering Report, FBI

60% считают
социнженерию
одной из наибольших
сегодняшних угроз

60% были или знают,
где могли стать жертвой
социнженерии
за последний год

65% — результат атак —
потеря конфиденциальной
информации
работниками компаний

Online crimes responsible for the greatest financial loss totals, FBI's

Crime Type	Loss
BEC/EAC	$676,151,185
Confidence Fraud/Romance	$211,382,989
Non-Payment/Non-Delivery	$141,110,441
Investment	$96,844,144
Personal Data Breach	$77,134,865
Identity Theft	$66,815,298
Corporate Data Breach	$60,942,306

Crime Type	Loss
Advanced Fee	$57,861,324
Credit Card Fraud	$57,207,248
Real Estate/Rental	$56,231,333
Overpayment	$53,450,830
Employment	$38,883,616
Phishing/Vishing/Smishing/ Pharming	$29,703,421
Other	$23,853,704
Lottery/Sweepstakes	$16,835,001
Extortion	$15,302,792
Tech Support	$14,810,080

Crime Type	Loss
Misrepresentation	$14,580,907
Harassment/Threats of Violence	$12,569,185
Government Impersonation	$12,467,380
Civil Matter	$5,766,550
IPR/Copyright and Counterfeit	$5,536,912
Malware/Scareware/ Virus	$5,003,434
Ransomware	$2,344,365

Crime Type	Loss
Denial of Service/TDoS	$1,466,195
Charity	$1,405,460
Health Care Related	$925,849
Re-Shipping	$809,746
Gambling	$598,853
Crimes Against Children	$46,411
Hacktivist	$20,147
Terrorism	$18,926
No Lead Value	$0

Descriptors*	
Social Media	$56,478,483
Virtual Currency	$58,391,810

*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.

«Невежество должно доставлять человеку неудобство»

Александр Невзоров

«При всем богатстве выбора другой альтернативы нет»

Легендарний рекламний слоган

Cameralabs В ФОКУСЕ ВДОХНОВЕНИЕ ФОТОГРАФИЯ ОНЛАЙН СЕРВИСЫ ФОТО ДНЯ

Реклама Яндекс

Яндекс.Директ

Оператор Лайф, Киевстар, МТС.
Золотые номера операторов. МТС, **Киевстар**, Life. Быстрая доставка.
zmobi.in.ua

Пополнение мобильного телефона
Пополнение мобильного телефона банковской картой. Без комиссии.
bosteri.ml

Мобильные операторы.
Способы пополнения Life, MTS, Kyivstar
popolni.cf

Пополнение счета
0% Пополнение **счета** быстро и без комиссии!!!
popolnyashka.info

ОРУЖИЕ

ПРОТИВ СОЦИНЖЕНЕРИИ

КІБЕР-ПРОСВІТОЮ

БИЙ ШАХРАЯ!

EMA Academy

ОБУЧЕНИЕ НАСЕЛЕНИЯ

#SAFECARD

ОБРАЗОВАТЕЛЬНАЯ КАМПАНИЯ

EMBASSY OF THE UNITED STATES
KYIV, UKRAINE

ЄМА

MBASSY OF THE UNITED STATI
KYIV, UKRAINE
EMA

ЗАЧЕМ?

#SAFECARD

CARD FRAUD RATE В УКРАИНЕ

лично столкнулись с карточным мошенничеством

ЭТАПЫ КАМПАНИИ

PRE-TEST СОЦОПРОС

октябрь – ноябрь, 2016

ИНФОРМАЦИОННАЯ КАМПАНИЯ

декабрь 2016 – сентябрь 2017

MIDDLE & POST-TEST СОЦОПРОС

март – апрель, 2017 и сентябрь – ноябрь, 2017

#SAFECARD | ЭТАПЫ КАМПАНИИ

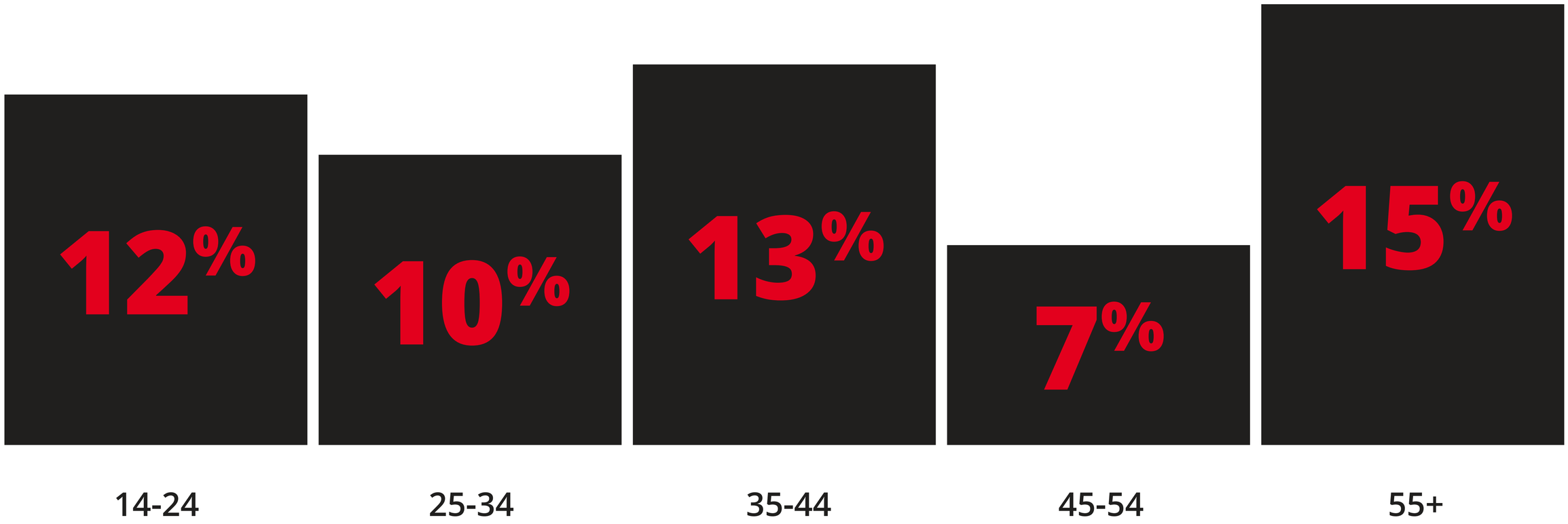
PRE-TEST СОЦОПРОС

ОСВЕДОМЛЕННОСТЬ ГРАЖДАН О ПРИЗНАКАХ И СПОСОБАХ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА В СФЕРЕ БЕЗНАЛИЧНЫХ РАСЧЕТОВ

октябрь – ноябрь, 2016

СТОЛКНОВЕНИЕ С МОШЕННИЧЕСТВОМ

Дифференциация по возрастным категориям



СТОЛКНОВЕНИЕ С МОШЕННИЧЕСТВОМ

Дифференциация по полу

РИСКОВАННОЕ ПОВЕДЕНИЕ

по телефону

77%

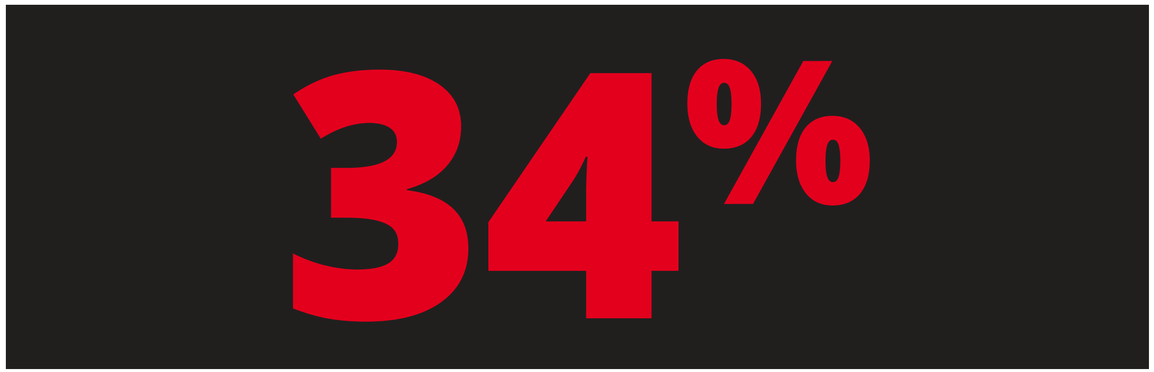
Знают, что никому нельзя сообщать реквизиты карты и коды из банковских sms

76%

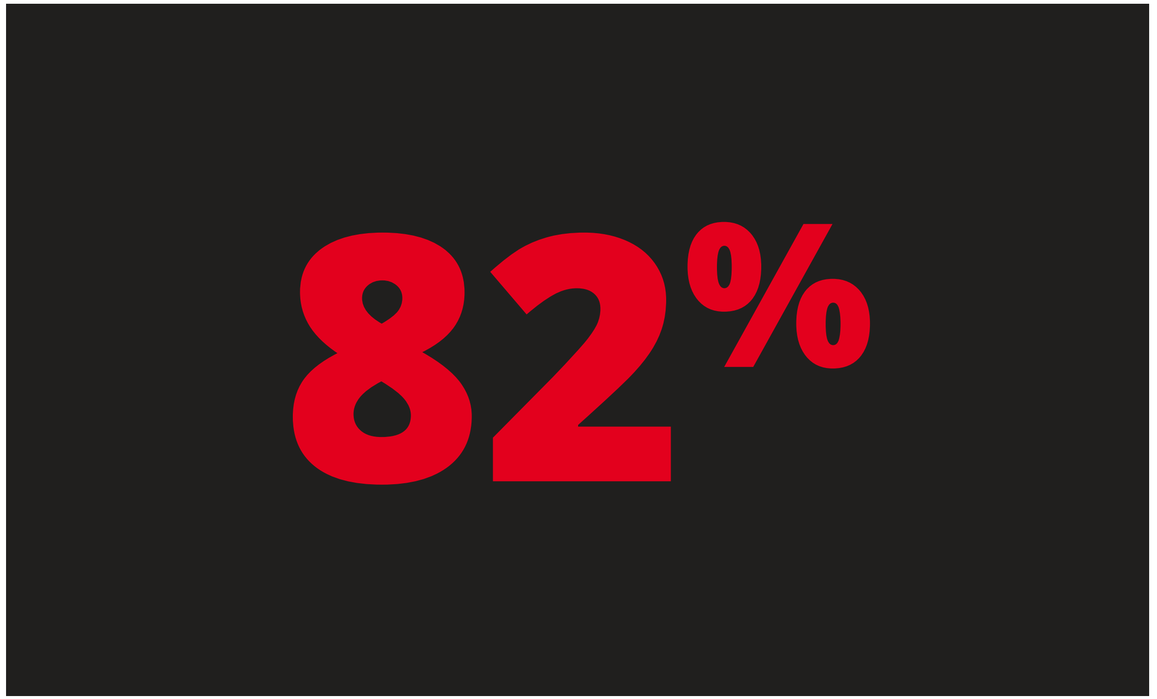
Столкнувшись с мошенничеством, разглашают реквизиты своей карты

РИСКОВАННОЕ ПОВЕДЕНИЕ

в Интернет



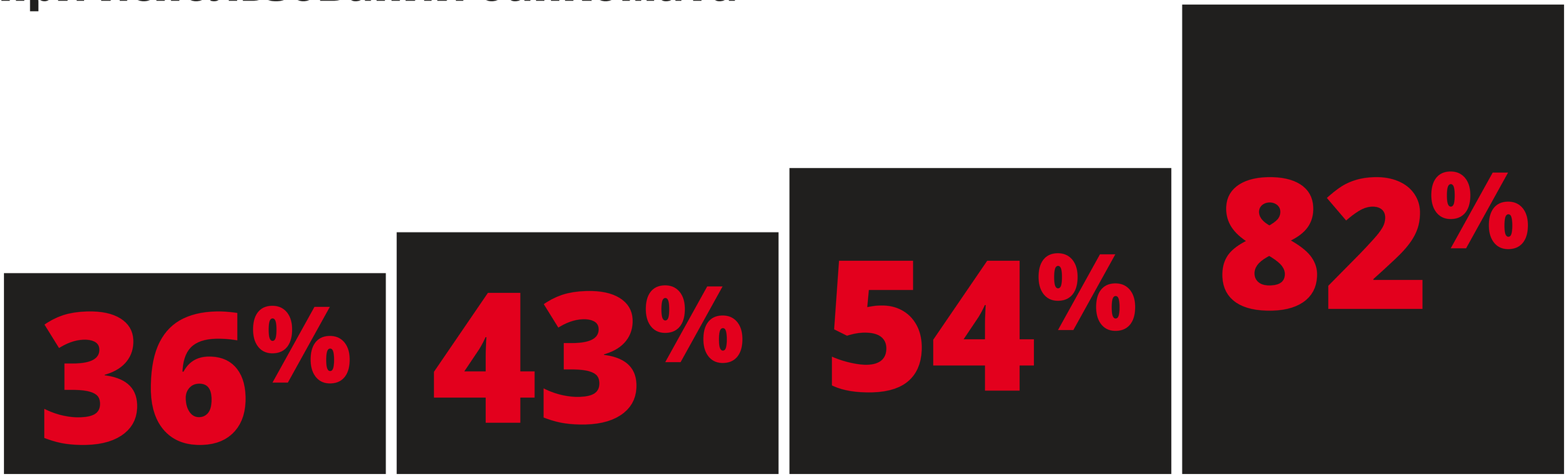
Считают безопасным использовать новый, неизвестный платежный сервис



Считают безопасным использовать платежный сервис, зарегистрированный на домене, без ограничений в регистрации

РИСКОВАННОЕ ПОВЕДЕНИЕ

при использовании банкомата



Считают безопасным не прикрывать ПИН-код

Считают безопасным отойти от банкомата, если он не выдал деньги

Не устанавливают лимиты на платежи по своим картам

Не меняют свой ПИН-код

КАНАЛЫ ОБРАЩЕНИЯ В ПОЛИЦИЮ

Через сайт Киберполиции

Через районное отделение

ВЫВОДЫ

Больше половины украинцев демонстрируют рискованное поведение и нуждаются в КиберЛикБезе

ЧТО ДЕЛАТЬ?

ПРОСВЕЩАТЬ!

Обучая средствам самообороны

Фокусируясь на базовых правилах безопасности

Коммуницируя массово и эффективно

#SAFECARD

ИНФОРМАЦИОННАЯ КАМПАНИЯ

декабрь 2016 – сентябрь 2017

ФОКУС

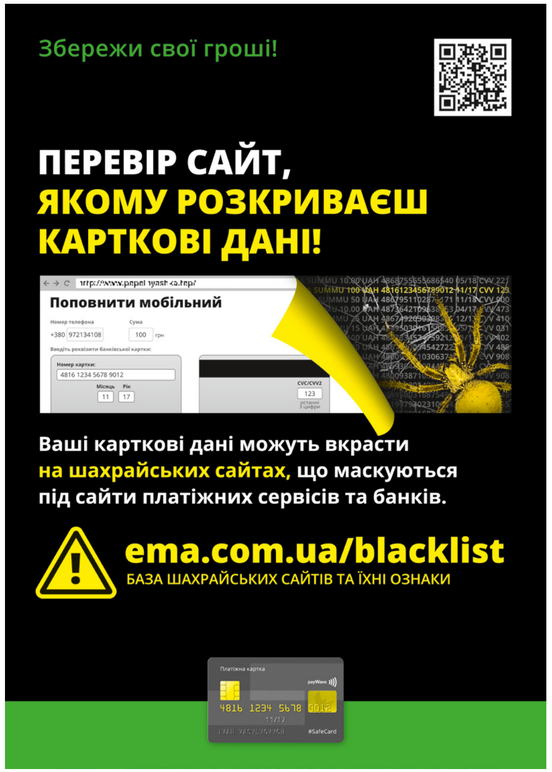
вишинг

фишинг

скимминг

кэш-треппинг

КЛЮЧЕВЫЕ СООБЩЕНИЯ



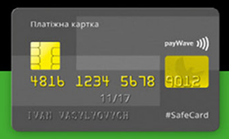
ЗА ЖОДНИХ УМОВ
НЕ РОЗКРИВАЙТЕ ЦІ РЕКВІЗИТИ СВОЇХ КАРТОК!

Збережи свої гроші!

ЗА ЖОДНИХ УМОВ НЕ РОЗКРИВАЙТЕ ЦІ РЕКВІЗИТИ СВОЇХ КАРТОК!

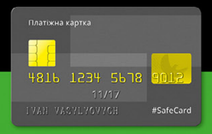
Вам **телефонують** і під різними приводами випитують дані платіжної картки, банківські sms-паролі або змушують зняти ліміти?

Припиніть розмову, бо втратите гроші!



#SafeCard

НОМЕР КАРТКИ — ЄДИНЕ, ЩО МОЖНА ПОВІДОМИТИ ТЕЛЕФОНОМ!



ЄМА ema.com.ua

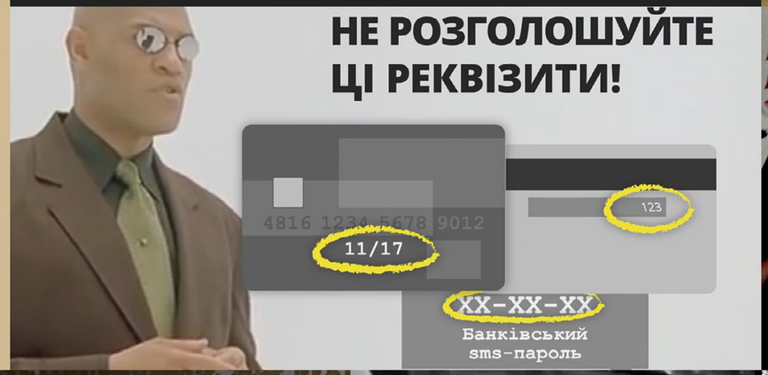
НІКОМУ НЕ КАЖИ

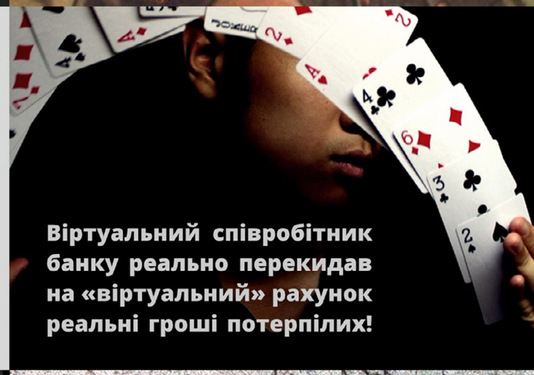
БАНКІВСЬКІ СМС-ПАРОЛІ

ТА ЦИФРИ ЗІ ЗВОРОТУ СВОЄЇ КАРТКИ!

ШАХРАЙ МОЖЕ ПРЕДСТАВИТИСЯ БУДЬ-КИМ:

НЕ РОЗГОЛОШУЙТЕ ЦІ РЕКВІЗИТИ!





Банк ніколи не питає карткові дані телефоном!

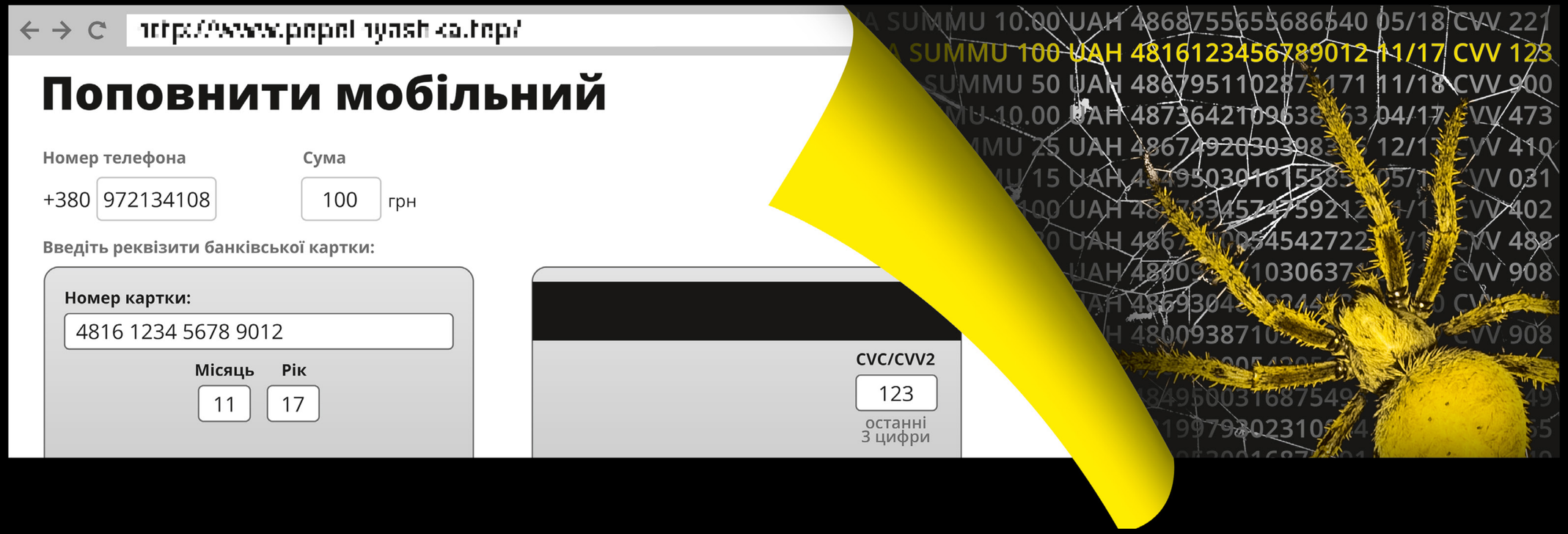
Єдине, що можна повідомити телефоном!

Шахрай може представитися будь-ким!

СБУ ніколи не питає карткові дані телефоном!

Нікому не розкривай свої карткові дані!

ПЕРЕВІР САЙТ, ЯКОМУ РОЗКРИВАЄШ КАРТКОВІ ДАНІ!

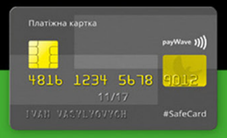


Збережи свої гроші!

ПЕРЕВІР САЙТ, ЯКОМУ РОЗКРИВАЄШ КАРТКОВІ ДАНІ!

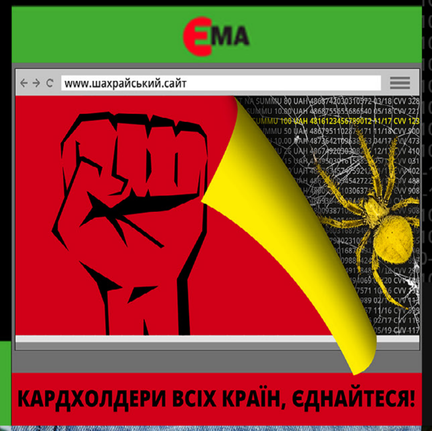
Ваші карткові дані можуть вкрасти **на шахрайських сайтах,** що маскуються під сайти платіжних сервісів та банків.

ema.com.ua/blacklist
БАЗА ШАХРАЙСЬКИХ САЙТІВ ТА ЇХНІ ОЗНАКИ



Дивись, кому розкриваєш свої карткові дані!

ТИСНИ
для переходу в
БАЗУ ШАХРАЙСЬКИХ САЙТІВ

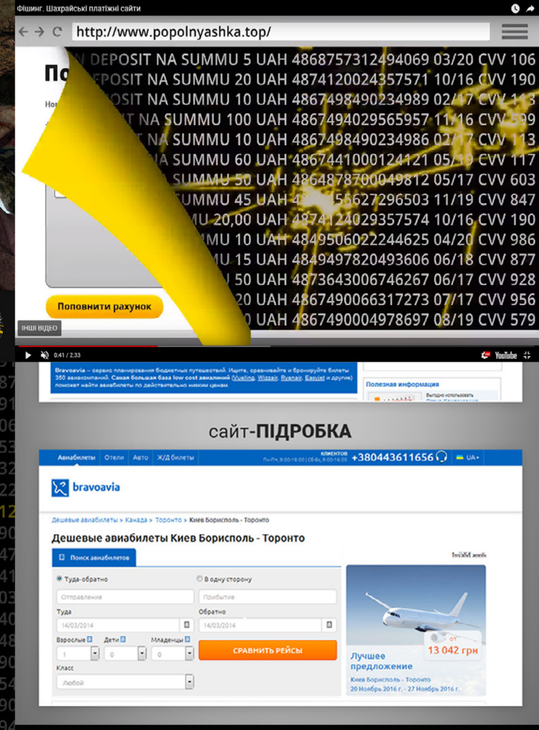


КАРДХОЛДЕРИ ВСІХ КРАЇН, ЄДНАЙТЕСЯ!

Дивись, кому розкриваєш свої карткові дані!

Дивись, кому розкриваєш свої карткові дані!

Фішинговий сайт — це...



сайт-**ПІДРОБКА**

Шахрайські сайти **можуть маскуватися під:**

Сайти з продажу авіа-квитків

Платіжні сайти теж треба перевіряти!

Платіжні сайти теж треба перевіряти!

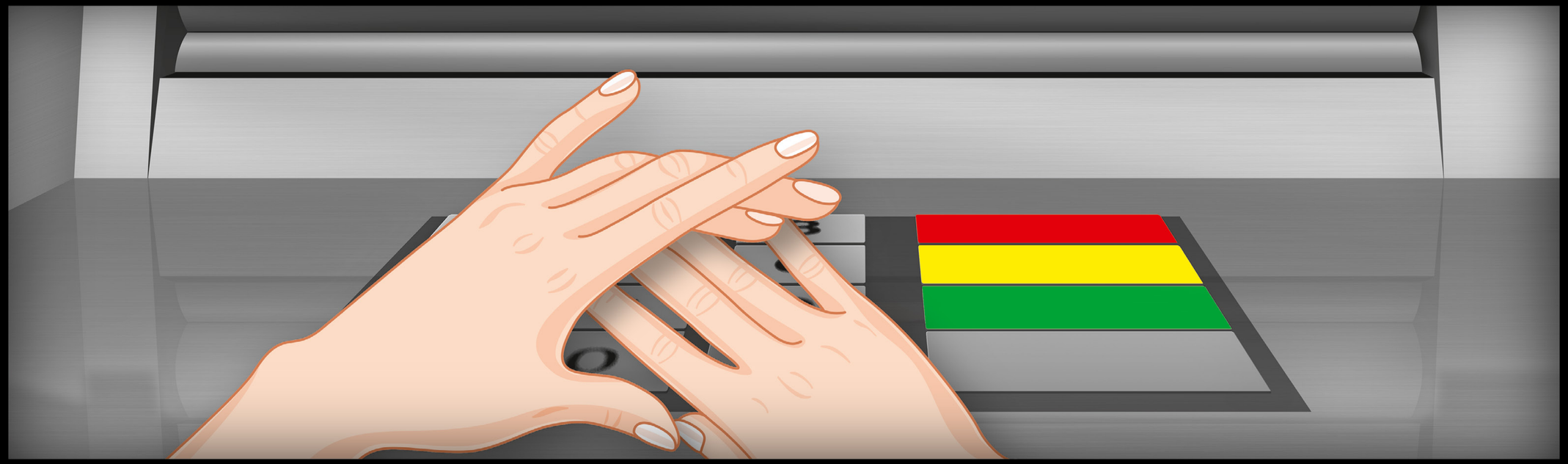
Платіжні сайти теж треба перевіряти!

Це був фішинговий сайт, а не золота рибка!

Такий от, малята, фішинговий сайт

ЗАХИСТИ СВІЙ

ПІН-КОД!

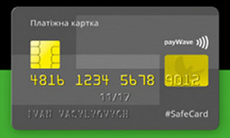


Захисти свої гроші!

ЗАХИСТИ СВІЙ ПІН-КОД!

Ваш ПІН-код можуть вкрасти
під час зняття готівки в банкоматі
через встановлені сторонні пристрої.

Прикривай ПІН-код під час введення!

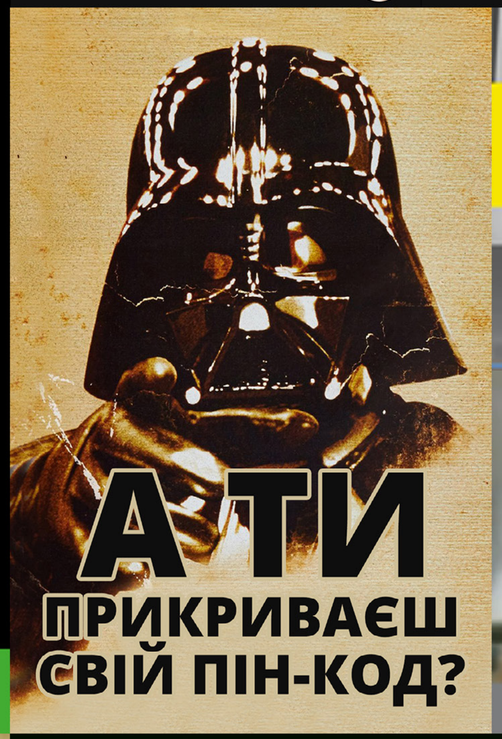


Прикрий свій ПІН!

Прикрий свій ПІН!

Ти не прикриваєш свій ПІН-код?

ТИ ПРИКРИВАЄШ СВІЙ ПІН-КОД?



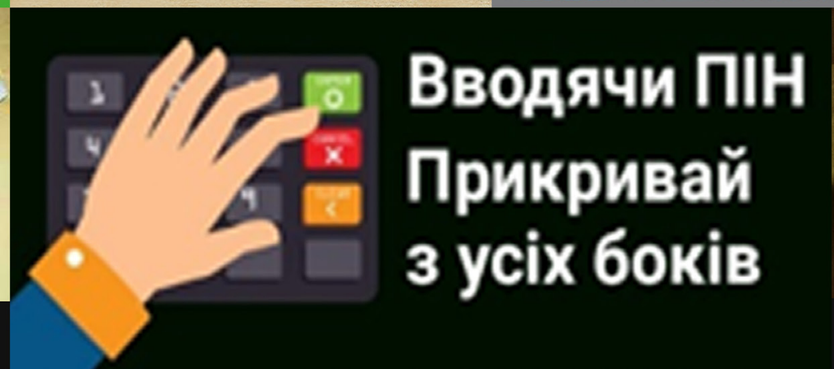
А ТИ ПРИКРИВАЄШ СВІЙ ПІН-КОД?

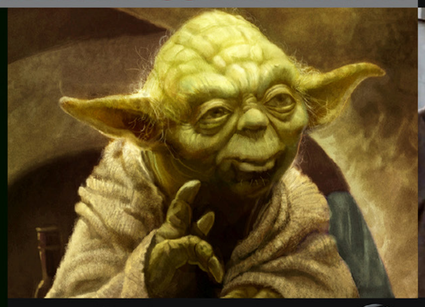
ЗАПИС ШАХРАЙСЬКОЇ ВІДЕОКАМЕРИ

Прикрий свій ПІН!

Я завжди прикриваю свій ПІН в банкоматі! А Ти?

ЦЕ ЙОМУ НЕ ДОПОМОЖЕ! Прикривай ПІН-код правильно!





ПІН свій в банкоматі прикриваю завжди я! А Ти?

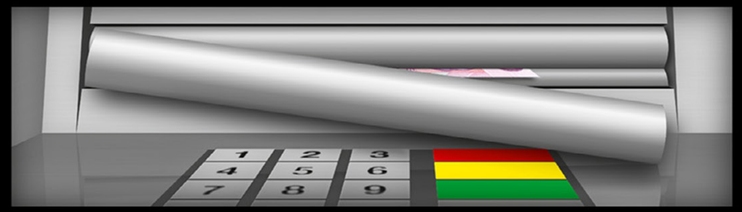
ЗАВЖДИ прикривай свій ПІН-код!

Ваші гроші можуть вкрасти
під час зняття готівки в банкоматі
через встановлені сторонні пристрої.

Не відходьте від банкомату, не перевіривши отвір для отримання готівки!

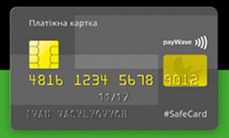
Збережи свої гроші!

ОПЕРАЦІЮ ЗАВЕРШЕНО, А ГРОШІ ДЕ?



Ваші гроші можуть вкрасти
під час зняття готівки в банкоматі
через встановлені сторонні пристрої.

Не відходьте від банкомату, не перевіривши отвір для отримання готівки!



Стій біля банкомату!
Телефонуй в банк!

Стій біля банкомату!
Телефонуй в банк!

Стій біля банкомату!
Телефонуй в банк!

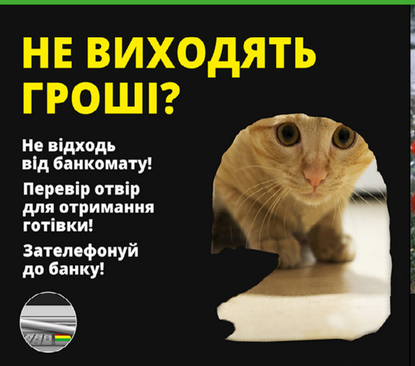
СТІЙ! ПЕРЕВІР ОТВІР!

KEEP CALM AND НЕ ВІДХОДЬ ВІД БАНКОМАТУ!

ПЕРЕВІР ОТВІР ДЛЯ ОТРИМАННЯ ГОТІВКИ!

ЗАТЕЛЕФОНУЙ ДО БАНКУ!

А ОСЬ І ГРОШІ!



Банкомат!
Де мої 200 гривень?

Банкомат!
Я не піду без грошей!

Банкомат!
Ну, і де мої гроші?

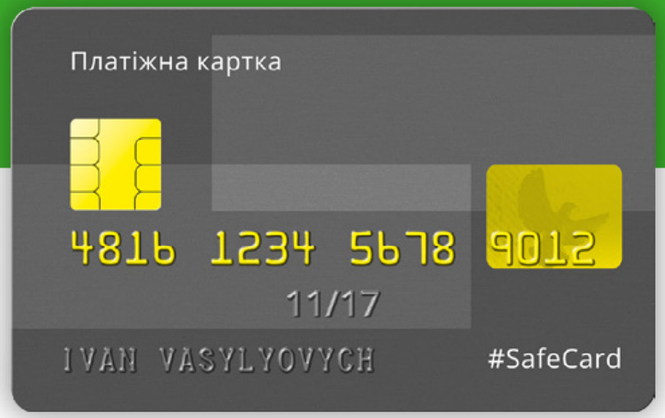
Банкомат!
Ну, і де мої гроші?

ЯК ДІЯТИ?

ЯКЩО ВИ ПІДДАЛИСЯ ШАХРАЙСЬКІЙ ПРОВОКАЦІЇ ТА ПОВІДОМИЛИ ШАХРАЯМ РЕКВІЗИТИ СВОЄЇ КАРТКИ, ПОТРІБНО:

Негайно заблокувати вашу картку

Звернутися із заявою до Кіберполіції онлайн www.cybercrime.gov.ua



#SAFECARD

EMBASSY OF THE UNITED STATES
KYIV, UKRAINE

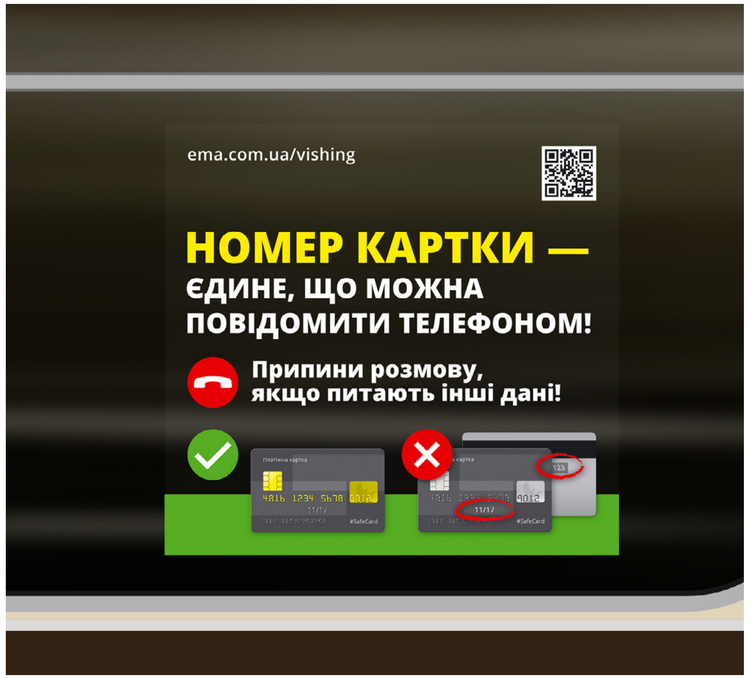
EMA

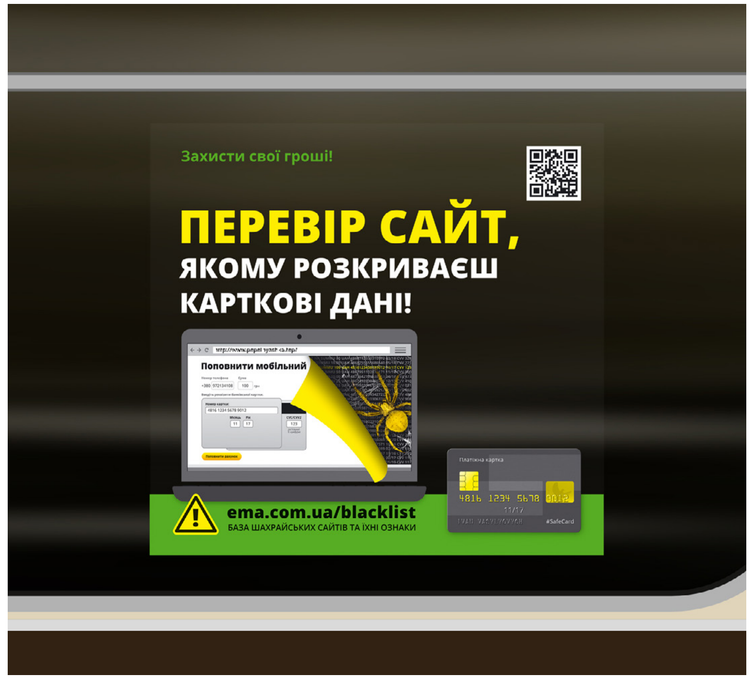
КАНАЛЫ КОММУНИКАЦИИ

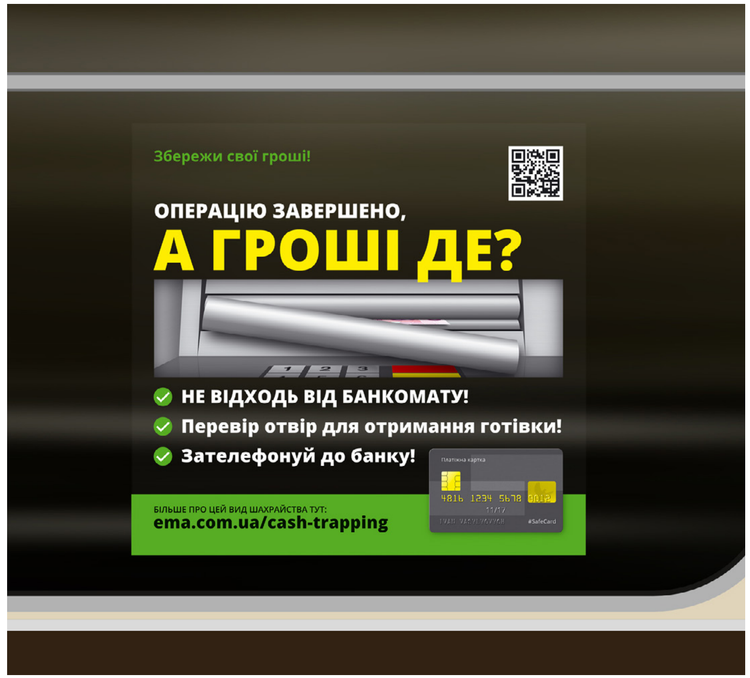
НАРУЖКА

30 биллбордов на улицах Киева.
Охват - 2,1 млн.+ граждан

ТРАНСПОРТ







Информационные плакаты в вагонах киевского метрополитена.
Охват - 1,8 млн.+ граждан в день

Захисти свої гроші!

ПЕРЕВІР САЙТ,
ЯКОМУ РОЗКРИВАЄШ КАРТКОВІ ДАНІ!

ema.com.ua/blacklist

БАЗА ШАХРАЙСЬКИХ САЙТІВ ТА ІХНІ ОЗНАКИ

ema.com.ua/vishing
НОМЕР КАРТКИ –
ЄДИНЕ, ЩО МОЖНА
ПОВІДОМИТИ ТЕЛЕФОНОМ!
Припини розмову,
якщо питають інші дані!
4816 1234 5678
Лісова
Чернігівська
Червоний Хутір
Харківська
SMART
5775

ОПЕРАЦІЮ ЗАВЕРШЕНО,
А ГРОШІ ДЕ?
НЕ ВІДХОДЬ ВІД БАНКОМАТУ!
Перевір отвір для отримання готівки!
Зателефонуй до банку!
ema.com.ua/cash-trapping
SMART
КВАРТИРИ
В КИЄВІ
ТЕЛЕФОНУЙ
5775
www.СМАРТКИЇВ.com

#SAFECARD | КАНАЛЫ КОММУНИКАЦИИ

ПЛАКАТЫ

Информационные плакаты
на Алчевском меткомбинате,
Славянском машиностроительном
заводе и других промышленных
предприятиях

ПЛАКАТЫ

В 500+ Центрах
бесплатной правовой помощи
и отделениях 20+ банков

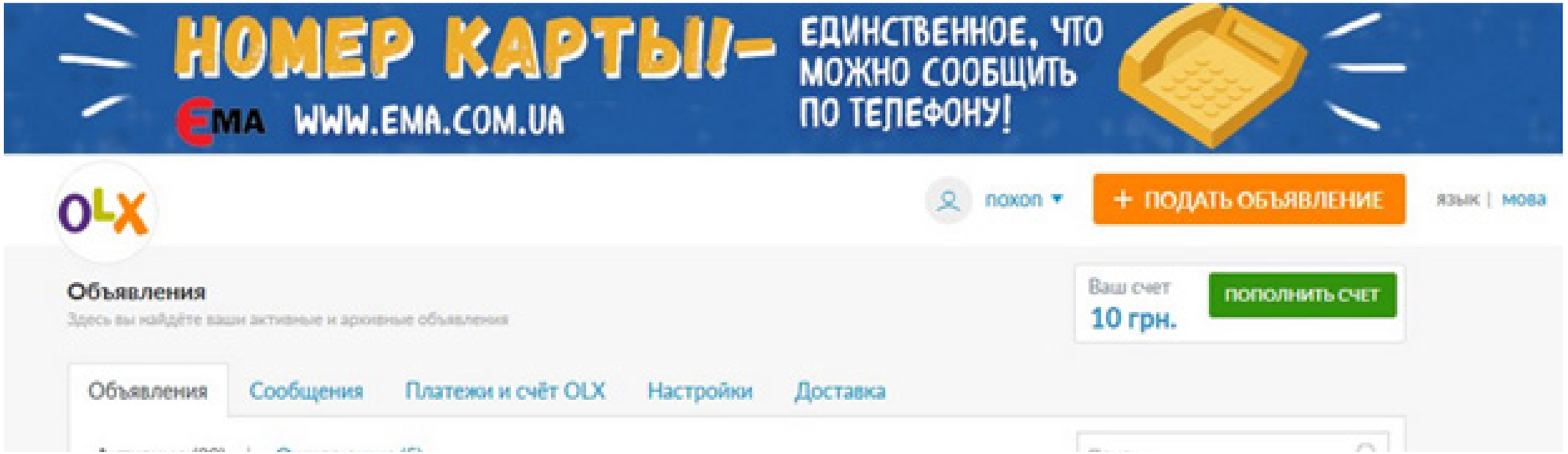
ГАЗЕТЫ

Социальные газеты для пенсионеров распространены через Центры бесплатной правовой помощи, банковские отделения и ... в сумках почтальонов

СМИ

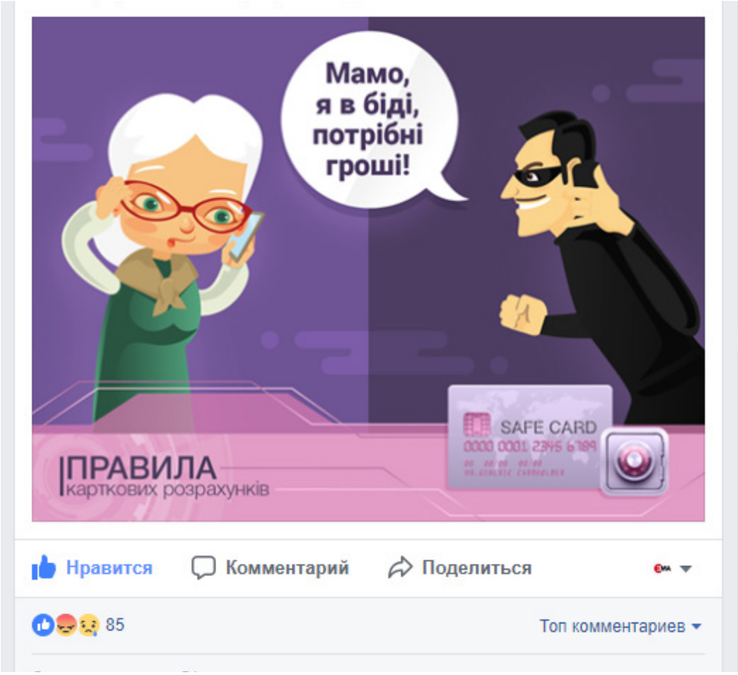
2000+ публикаций
в украинских СМИ

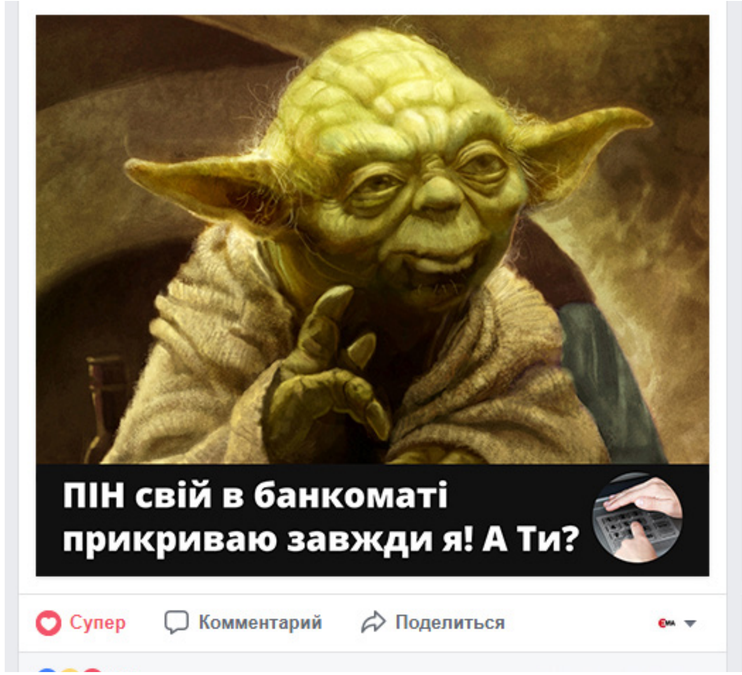
ИНТЕРНЕТ

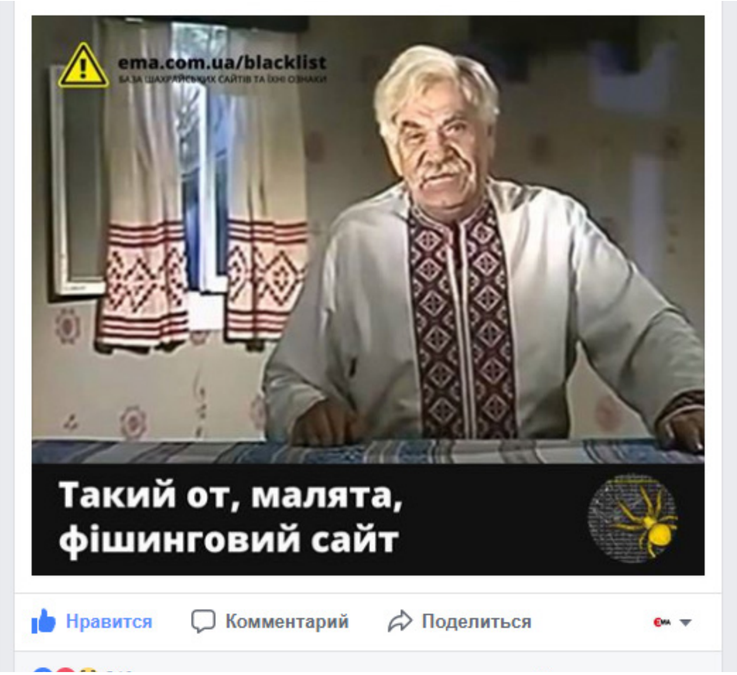


Информационные баннера размещены на 400+ популярных веб-сайтах (YouTube, Skype, OLX)

СОЦСЕТИ

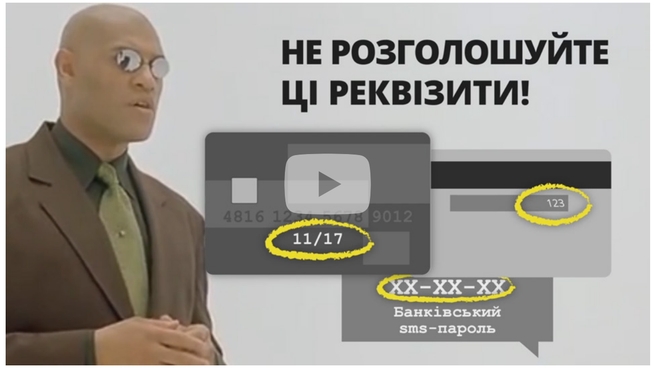


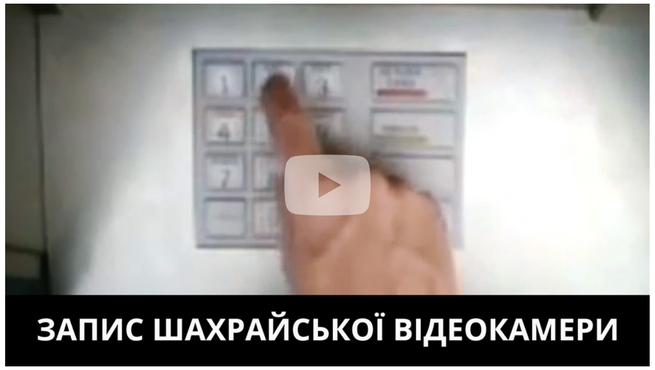




Информационная кампания проведена в Facebook и Vkontakte.
Охват — 4,3+ млн. граждан

YOUTUBE





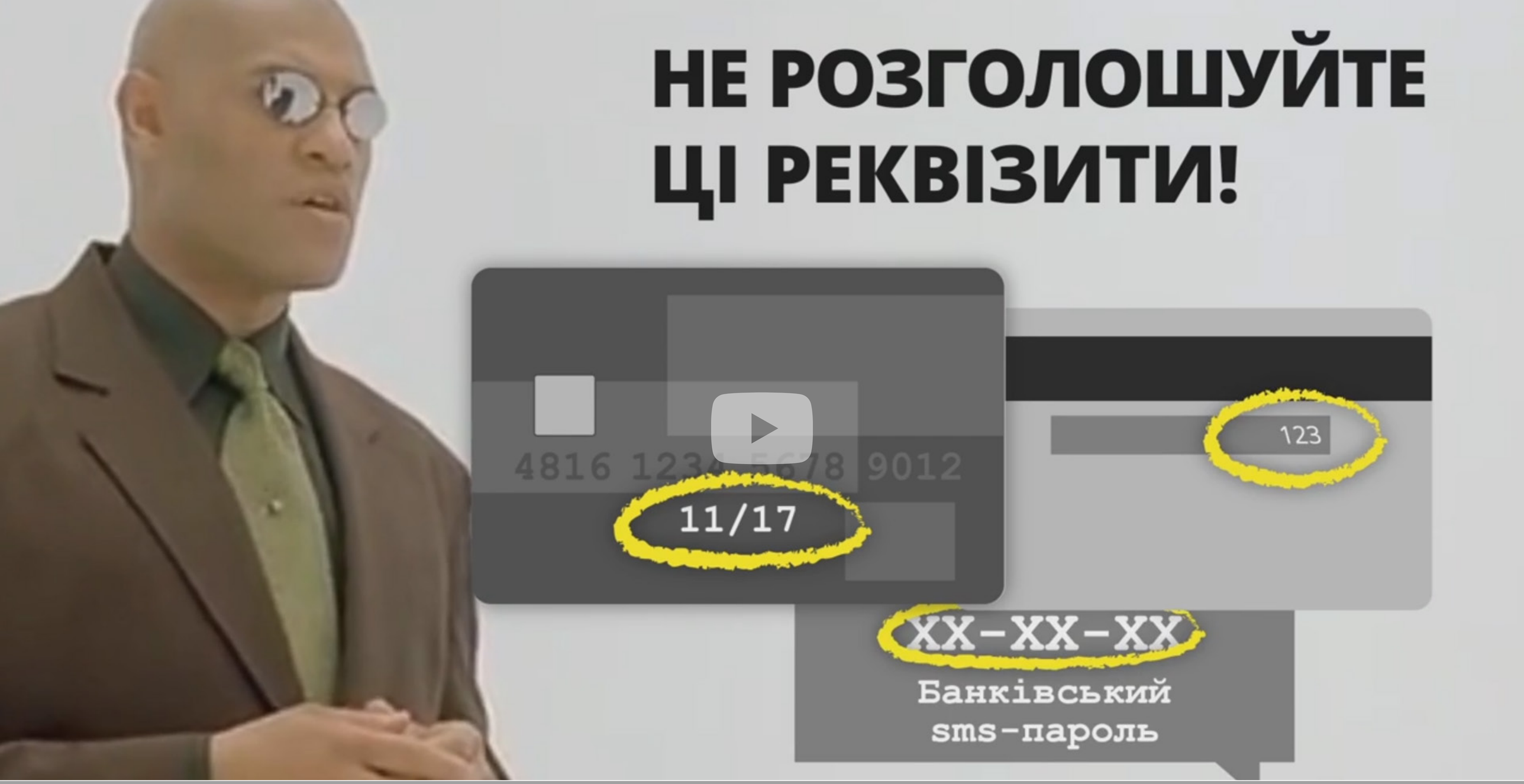
5 образовательных видеороликов — 300 000+ просмотров

#SAFECARD | КАНАЛЫ КОММУНИКАЦИИ

ПОЗВОНИЛИ МОШЕННИКАМ

750 000 просмотров
и 15 000 репостов на Facebook

НАШИ МЕТОДЫ



Синематограф

ДОСТАТНЬО НОМЕРА КАРТКИ!

Гипноз

25-й кадр

Потомствєнна цілителька!

ВОРОЖІННЯ НА ПЛАТІЖНИХ КАРТКАХ!

- пороблено?
- приворожили гроші з картки?
- комп’ютерна порча?
- віруси-рекетири (Пєтя А, Пєтя Б)?
- кинули з передплатою?

Использование девиантных образов

КОД ЗІ ЗВОРОТУ КАРТКИ — ЦЕ ЧИСЛО ЗВІРА!

Использование религиозных суеверий

ВСОВУЙ ВІДПОВІДАЛЬНО!

Призыв к ответственности

КОМУ ЩЕ
СКАЗАТИ ЦИФРИ
ЗІ ЗВОРОТУ МОЄЇ КАРТКИ?

Стій біля банкомату!
Телефонуй в банк!

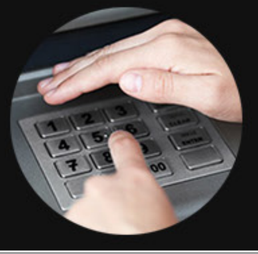
Риторические угрозы и армейские команды

Плакатное искусство

**Всім, хто послав шахраїв у дупу,
ми даруємо цукерок купу!**

«Сладкий» подкуп

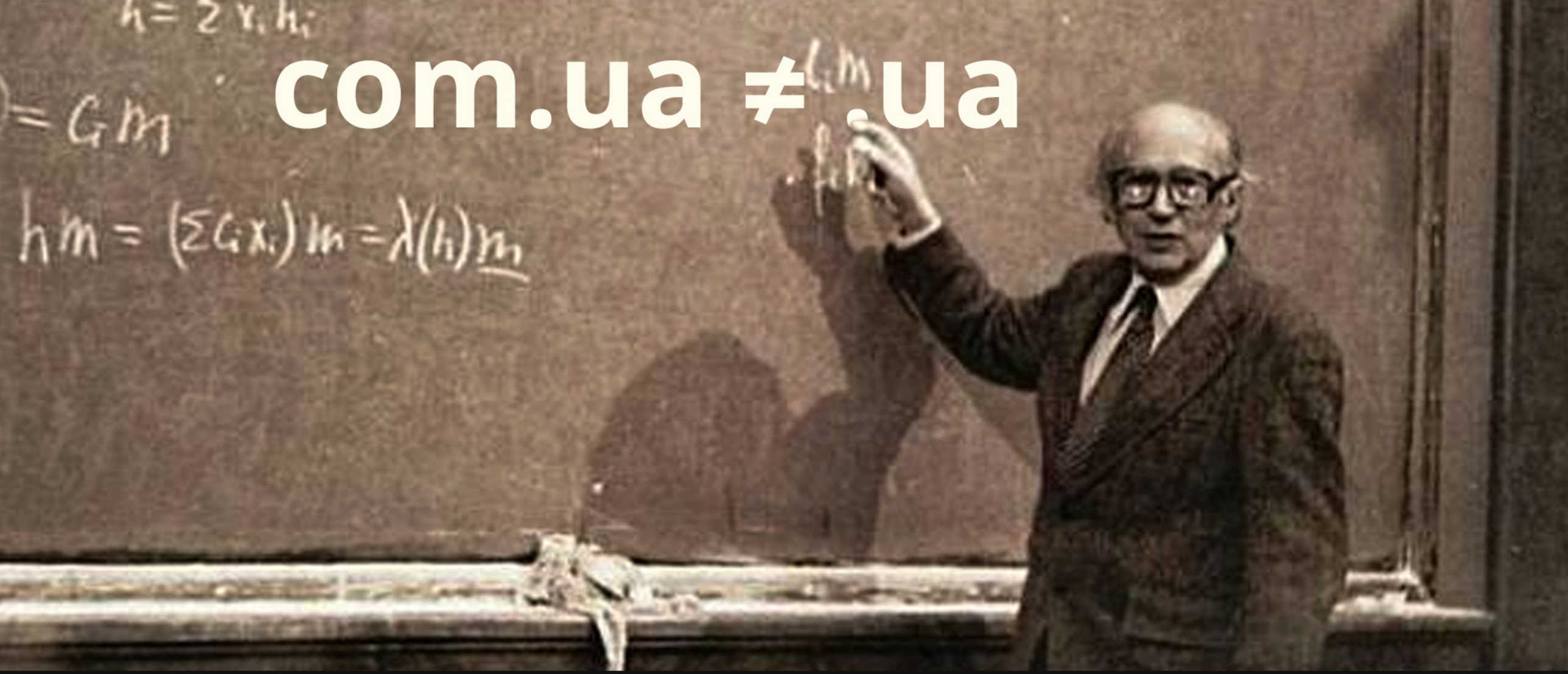
Прикрий свій ПІН!



Воздействие на основные инстинкты

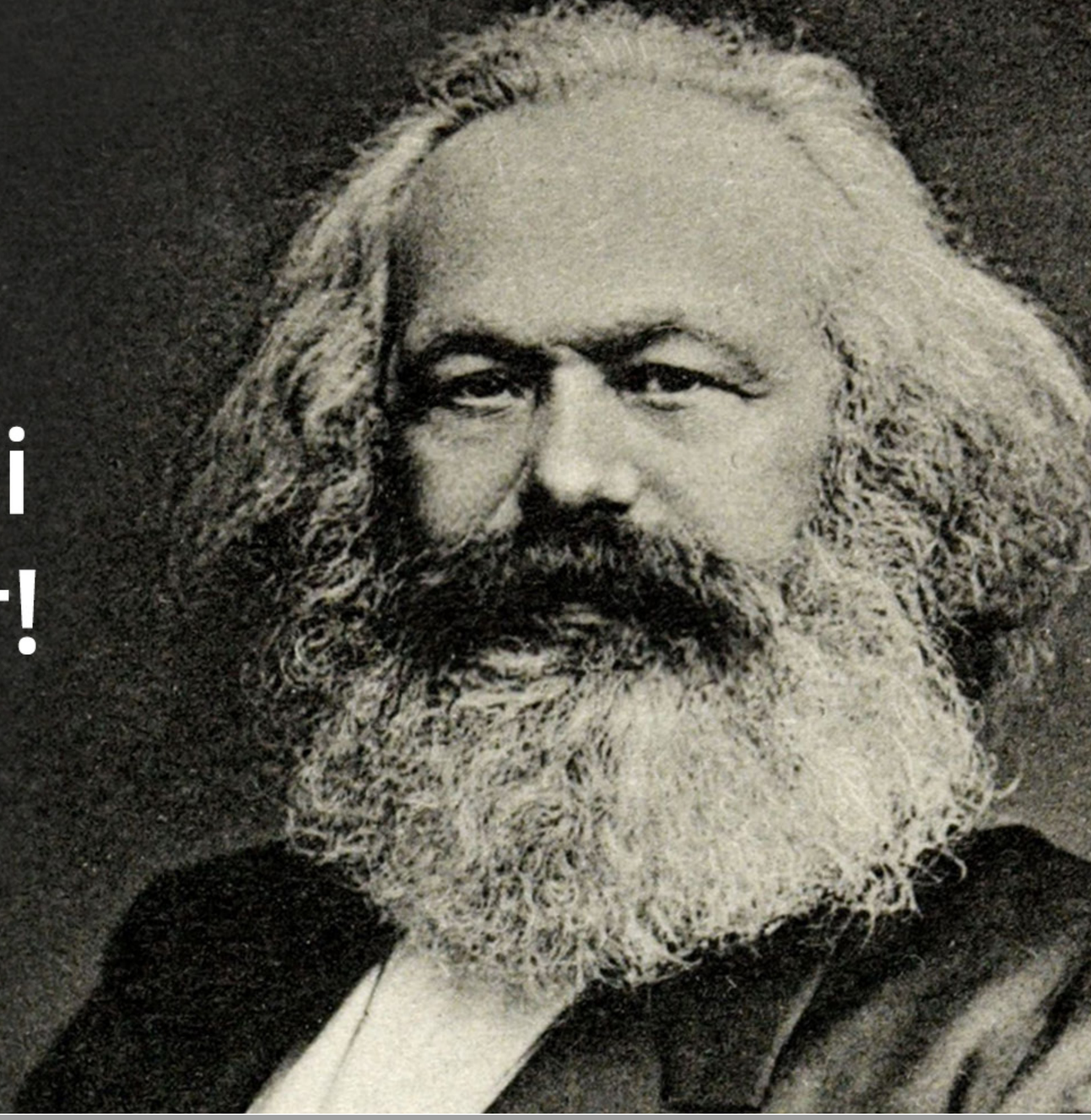
Ти не прикриваєш свій ПІН-код?

Стремление к общности с другими



Математические неравенства

Клара у Карла
вкрала картку,
у Карла на картці
встановлен ліміт!



Скороговорки

Крошка сын к отцу пришел,
и сказала кроха:
номер карты — хорошо!
sms-код — плохо!

Агитпроп стихотворения

Дао де ПІН

Мистецтво #cashless

«Най тобі джіба цицьку дасть, а не до банкоматоу» — відповів суворий дядько з міста Во, що у горах, коли «Співробітник банку» запропонував зробити перерахунок кредиту за допомогою банкомату.

POST-СОЦОПРОС

ОЦЕНКА ОСВЕДОМЛЕННОСТИ ГРАЖДАН О МОШЕННИЧЕСТВЕ В СФЕРЕ БЕЗНАЛИЧНЫХ РАСЧЕТОВ

сентябрь – ноябрь, 2017

CARD FRAUD RATE В УКРАИНЕ

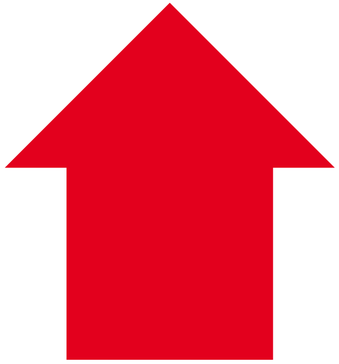
доля граждан, осознающих, что столкнулись с мошенничеством

CARD FRAUD RATE В УКРАИНЕ

доля граждан, которые не слышали о мошенничестве

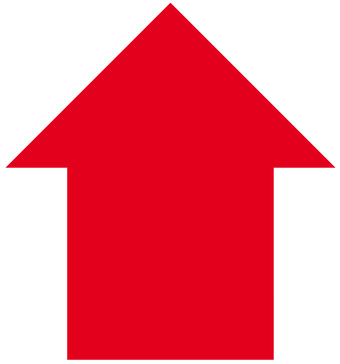
РАСПОЗНАНИЕ МОШЕНИЧЕСТВА

НА 1/3



число людей, считающих рискованным использовать отечественный платежный сервис, зарегистрированный не на домене .ua

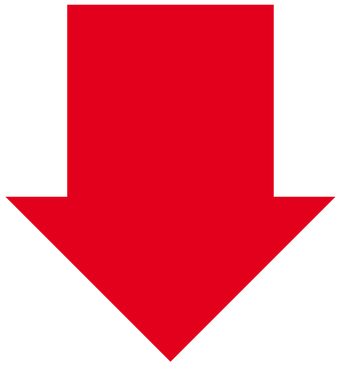
НА 1/3



число людей, считающих рискованным отходить от банкомата, если деньги не были выданы

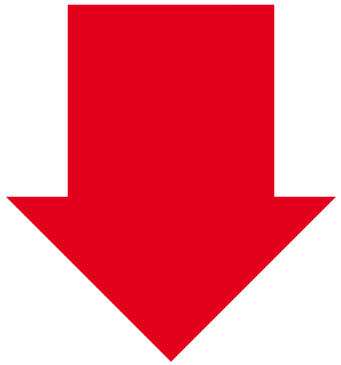
РИСКОВАННОЕ ПОВЕДЕНИЕ

В 4 РАЗА



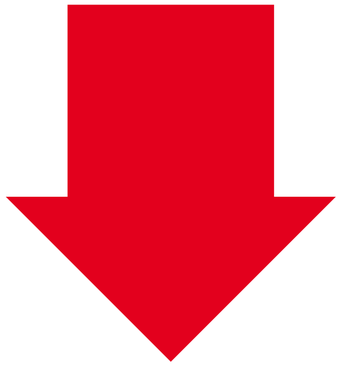
Число людей, игнорирующих правило неразглашения секретных реквизитов карты и банковских смс-кодов

В 3 РАЗА



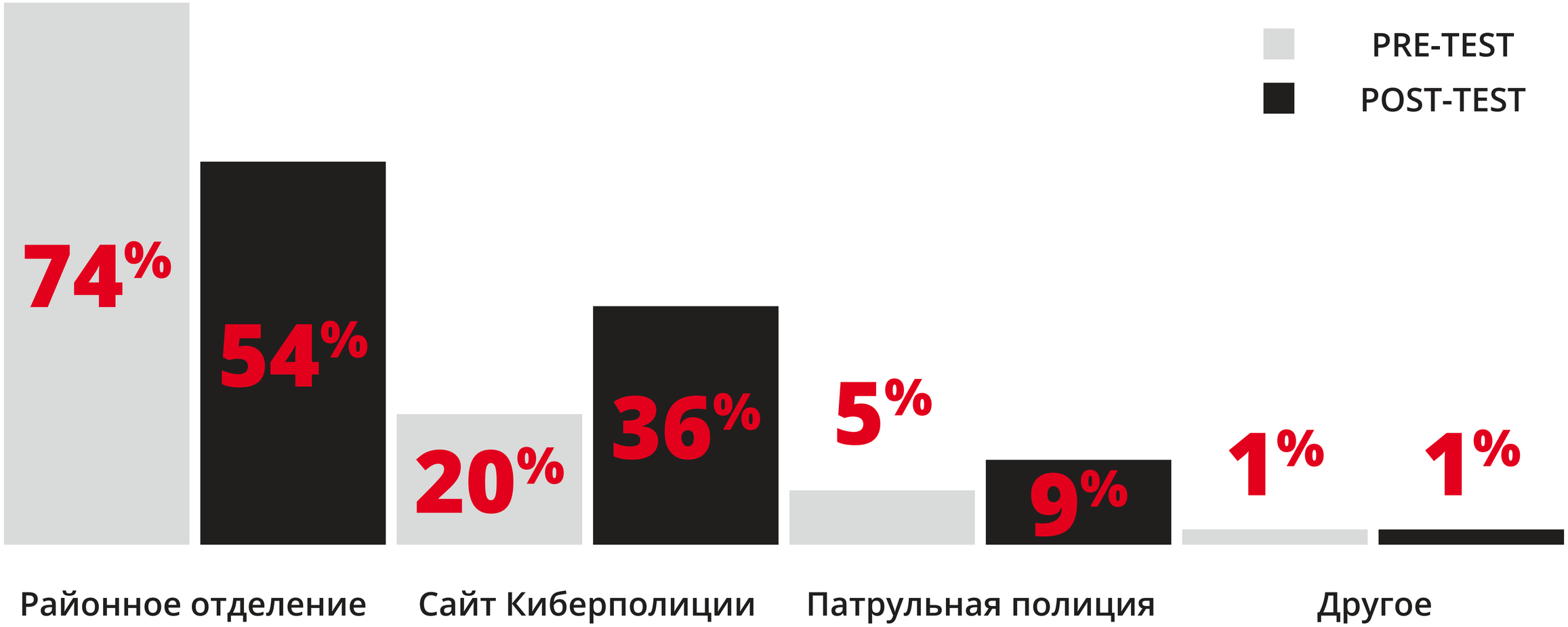
Число людей, игнорирующих правило использования только известных платежных сервисов

В 2 РАЗА



Число людей, игнорирующих правило прикрытия ПИН-кода в банкомате

КАНАЛЫ ОБРАЩЕНИЯ В ПОЛИЦИЮ



ЕСТЬ ЛИ ЖИЗНЬ ПОСЛЕ ГРАНТА?

ШКОЛА
КІБЕРБЕЗПЕКИ

Школа кибербезопасности

Мошенничество в Интернет

Телефонное мошенничество

Смс-мошенничество

Банкоматное мошенничество

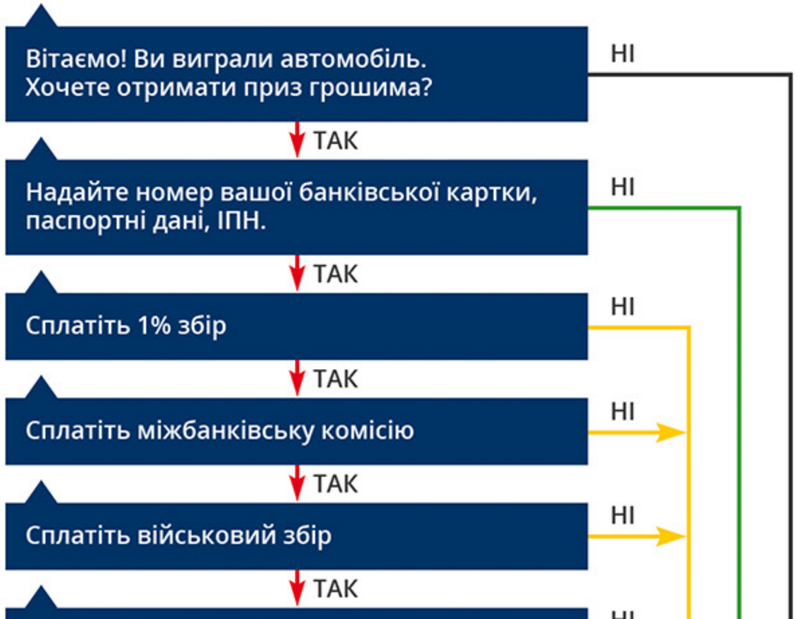
Вредоносные программы

Не становись дропом

Мошенничество в интернет | СМС мошенничество | Телефонное мошенничество

SMS-лотерея. Как получить Автомобиль?

Выиграть авто в Акции — проще простого. Сидишь себе на диванчике перед телевизором, не напрягаясь и даже не подозревая о том, что участвуешь в лотерее, как вдруг БАЦ: «Вітаємо! Ваш мобільний номер виграв авто! Заберіть грошима!» Вот тут-то и начинается самое интересное. Что же в самую первую очередь нужно сделать, чтоб не провтыкать, а получить-таки столь желанный приз? Пошаговая инструкция:



Мошенничество в интернет

Реально ли заработать на наборе текста в эпоху голосового набора?

Интернет кишит предложениями о работе, суть которой заключается в наборе текста в Word на дому. На первый взгляд, хорошая тема для тех, кто пока еще не имеет других полезных навыков и мечтает о легком заработке, не отходя от домашнего компьютера. Тем более, что создастся ощущение, что «заказчик» тупо тупит. Зачем платить по 100-200 грн за набор страницы текста с бумажного скана, если уже более 15 лет как существуют системы оптического распознавания текста? А в современных смартфонах — и вовсе, голосовой набор реализован.

В итоге у читателя может сложиться впечатление, что «заказчик» какой-то отсталый от прогресса лох. А раз так, то грех его неосведомленностью не воспользоваться, заработав парутройку тысяч по-быстрому, пока лавочка не закрылась. Но такое впечатление — в корне ошибочно. Ибо «заказчик» вовсе не лох. Точнее, лох вовсе не «заказчик».

Схема развода настолько стара и проста, что диву даешься, как находятся еще люди, готовые поверить, что могут что-то с этого поиметь.

Если исполнитель «клюнул» на заманчивое предложение и обратился к «заказчику» за заданием, то ему (исполнителю), прежде чем «заказчик» вышлет материалы для набора, необходимо оплатить «страховой взнос», якобы для того чтобы исполнитель не «забил» на работу, и который типа вернется с первой получкой. Сумма «взноса», как правило, не очень большая — в пределах 100-200 грн.

Результат: после отправки «страхового взноса» вы останетесь «с носом» и от «заказчика» больше ничего не получите и ничего от него не услышите. Все.

Вместо эпилога, или мошенник мошеннику глаз выклюет.

Удивительно, но тема все-таки популярна, так как появились даже варианты мошеннической франшизы. Суть в том, что мошенники на форумах предлагают другим, склонным к мошенничеству гражданам, заняться этим «бизнесом». Организатор раскрывает схему, описывает

Мошенничество с билетами и арендой

Не «оплачивайте» отпуск мошенникам!

Лето – сезон прибыли для «отпускных» мошенников, которые особенно успешно обманывают своих жертв, продавая несуществующие туры, путевки, билеты и жилье. Попасть в сети злоумышленников может любой отдыхающий. Учимся распознавать признаки самых популярных ловушек.

В зоне риска онлайн-бронирование и покупка билетов, туров, апартаментов и коттеджей, а также билетов на развлекательные мероприятия. Все аферистские предложения имеют общие черты: они либо очень дешевые (ощутимо ниже средней цены по рынку), либо предлагают слишком заманчивые условия. Как только у вас появляется ощущение в духе «Вот это повезло!» — сразу же есть смысл насторожиться и перепроверить информацию. Мошенники могут придумать любое «сказочное» предложение, чтобы только заставить жертву купить «липовые» билеты или заплатить предоплату за несуществующие услуги.

Самые популярные сферы «отпускного» мошенничества:

Онлайн-покупка транспортных документов (билетов на самолет, поезд или пароход, а также билетов на трансфер до курортных мест, отелей и т.д.).

Онлайн-бронирование жилья, как в отелях или пансионатах, так и жилья у владельцев-физлиц;

Онлайн-бронирование автомобилей напрокат;

Онлайн-покупка и бронирование туристических путевок, туров, экскурсий;

Онлайн-покупка билетов на развлекательные поездки, мероприятия, посещения достопримечательностей;

Ukrainian Interbank Payment Systems Member Association "EMA"

@ema.com.ua

Головна
Інформація
Дописи
Відео
Світлини
Події

Вподобано | Відстежується | Поширити | ...

Дізнатися більше

Створити допис | Наживо | Подія | Пропозиція | Робота

Напишіть допис.

Світлини/Від... | Отримуйте п... | Почуття або дії | ...

Огляд
Реклама
Читачі
Вподобання
Охоплення
Переглядів сторінки
Page Previews
Дії на сторінці
Дописи
Події
Відео
Розповіді
Люди
Повідомлення

Щоденні дані записуються за Північноамериканським тихоокеанським часом.

1T 1M 1K

Початок: 6.4.2017

Кінець: 6.4.2019

Total Page Followers as of Today: 3 841

МІРКА
Порівнюйте свою продуктивність у часі.

Total Page Followers

Net Followers

Net followers shows the number of new followers minus the number of unfollows.

Ukrainian Interbank Payment Systems •••
Member Association "EMA"

Вподобана сторінка · 6 вересня 2018 р. ·

ПОРЯДНІ ДІВЧАТА ЦЕЙ НОМЕР НЕ ДАЮТЬ!

Фінансовий номер — один з ваших секретних ключів до банківських рахунків та карток. Не менш важливий, ніж ПІН-код чи «код зі звороту». Саме тому, він цікавий також і любителям ваших грошей — шахраям. Його (сам номер, а не сім-картку) теж можуть вкрасти!

Як це відбувається? Як унеможливити крадіжку вашого фінансового номера? Що робити, якщо раптом вже...? Відповіді-поради — у статті на нашому сайті: https://ema.com.ua/devushka-mozhno-vash-telefonchik/

Позначити ... | Додати роз... | Редагу...

11 073 Охоплення аудиторії

1 424 Engagements

Boost Again

Boosted on 6 вер 2018 р. Заверше
By Артем Денисов

Охоплення аудиторії **8,7 тис.**

Взаємодія з дописом 38

Переглянути результа

87 5 коментарів 39 поширень

Подобається Коментувати Поширити

Найвідповідніші

Ukrainian Interbank Payment Systems
Member Association "EMA" Що саме

Ukrainian Interbank Payment Systems •••
Member Association "EMA"

Вподобана сторінка · 4 січня ·

#шахрайськийсайт
«АКТИВНЕ З'ЄДНАННЯ З ТЕРМІНАЛОМ»

Абсурдна вигадка шахраїв: ви отримуєте sms про виграш авто у лотереї, в якій навіть не брали участі, а для отримання «призу» вам начебто потрібно лише сплатити «держмито» (1-2% від суми виграшу). При цьому платіж цей «обов'язково» потрібно зробити через так зване «активне з'єднання», коли жертва робить платіжну операцію через банкомат чи термінал,... Показати більше...

Позначити ... | Додати роз... | Редагу...

19 897
Охоплення аудиторії

1 608
Engageme

Рекламувати допис

348 25 коментарів 185 поширень

Подобається Коментувати Поширити

Найвідповідніші

Віталій Брик Бідність та жадібність крокують поруч... 15

Подобається · Відповісти · Написати · 13 тиж.

Ukrainian Interbank Payment Systems Member Association "EMA" •••

Вподобана сторінка · 26 грудня 2018 р. ·

#шахрайськийсайт
ТОП ШАХРАЙСЬКИХ САЙТІВ від ЗЛОГО САНТИ. Вже є купа постраждалих! Тому, навіть не намагайтеся перевіряти на власній шкурі чи платіжних картках!
Та якщо ви будете дуже неслухняними, а також:
1. ви ще не були жертвою підступного бажання купити дешевий айфон, то шахраї спеціально для вас зробили такі сайти: http://appl-good.com/, http://iphone-markt.us/, http://himobile.kiev.ua/;... Показати більше... — разом із Олексій Сіяница.

Позначити ... | Додати роз... | Редагу...

6 993 Охоплення аудиторії

508 Engageme

Рекламувати допис

213 10 коментарів 48 поширень

Подобається | Коментувати | Поширити

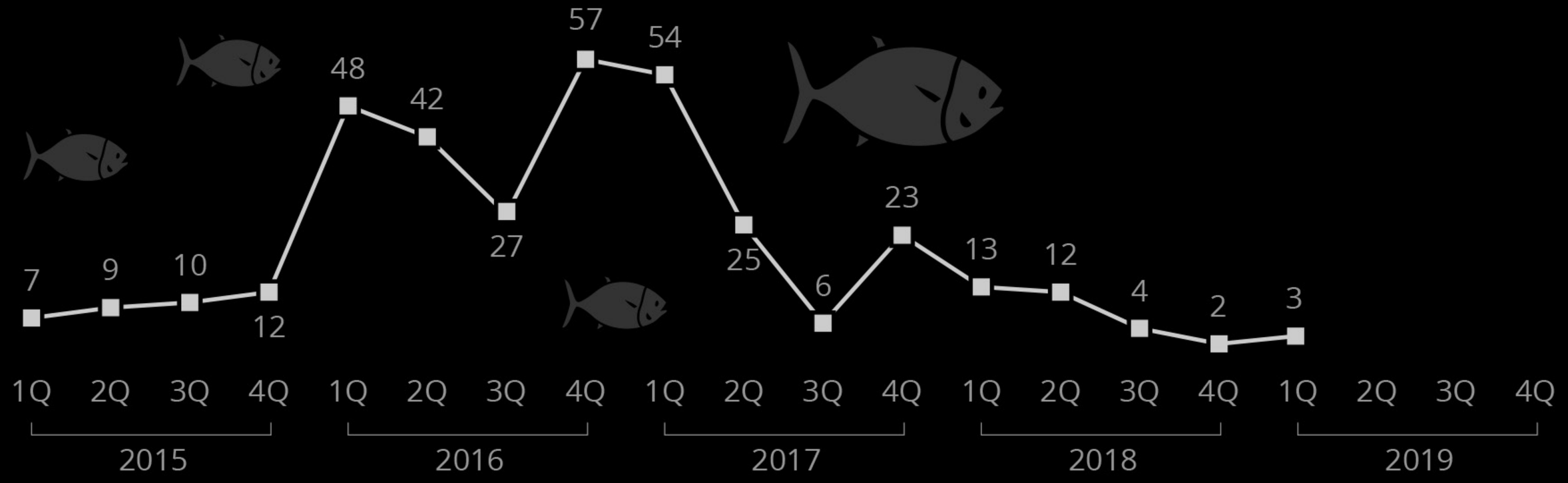
Найвідповідніші

Ukrainian Interbank Payment Systems Member Association "EMA" Всі наведені сайти шахрайські. Перевірено! Зробите

ГУМАННИЙ
ЛНИПІФ

ФИШИНГ 2015-2019

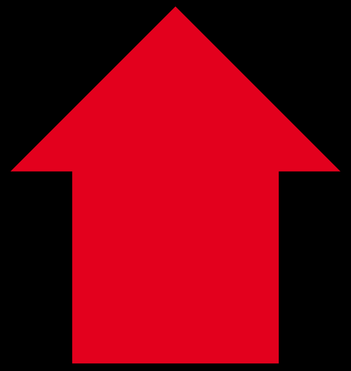
Количество фишинговых веб-ресурсов, выманивающих карточные реквизиты и пароли к Интернет-банкингу украинских граждан, 2015-2018



38 **174** **108** **31**

Блокировка
2015-2016

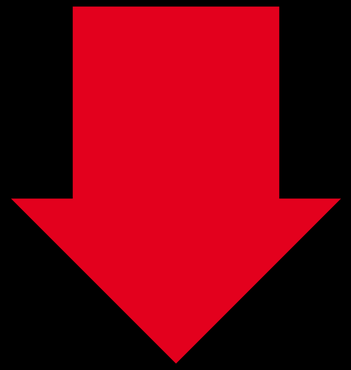
В 4.5 РАЗА



количество фишсайтов

#Safecard
2017

В 3 РАЗА



число людей, игнорирующих правило использования только известных платежных сервисов

ГУМАННИЙ ФІШИНГ
2018

КАЖДЫЙ ВТОРОЙ

держатель является потенциальной жертвой фишсайта

ЧТО?
И ЗАЧЕМ?

СОЦИССЛЕДОВАНИЕ & ОБУЧЕНИЕ ГРАЖДАН

СОЦИССЛЕДОВАНИЕ

- **АБСОЛЮТНАЯ ЧЕСТНОСТЬ РЕСПОНДЕНТОВ**

  индекс честности респондентов = 100%

- **«ГУЛЛИВЕРСКАЯ» РЕПРЕЗЕНТАТИВНОСТЬ ВЫБОРКИ**

  больше 7500 респондентов

- **ПОПАДЕНИЕ В ЦЕЛЕВУЮ АУДИТОРИЮ**

  украинские держатели платежных карт, пополняющие счет мобильного и совершающие P2P-операции онлайн

- **«COFFEE-AND-DOUGHNUT» СТОИМОСТЬ ПРОВЕДЕНИЯ**

  200$ - all-in cost

ОБУЧЕНИЕ ГРАЖДАН

- **ОБУЧЕНИЕ НА СОБСТВЕННЫХ ОШИБКАХ**

  имитация фишсайта

- **ГУМАННОЕ ОБУЧЕНИЕ**

  вместо потери денег - рекомендации по распознанию фишсайтов

- **ПОПАДЕНИЕ В ЦЕЛЕВУЮ АУДИТОРИЮ**

  украинские держатели платежных карт, пополняющие счет мобильного и совершающие P2P-операции онлайн

- **«COFFEE-AND-DOUGHNUT» СТОИМОСТЬ ПРОВЕДЕНИЯ**

  0,69 UAH – стоимость обучения 1 держателя

Butterfly
BALLOONS
EMA
WWW.PAY4FREE.COM.UA

Зарабатываем
не на комиссии,
а на доверии людей!

© 2018 by Pay4Free. All rights reserved.
Photoes by Frank McKenna and Jamison McAndie on Unsplash.

Pay4Free

Ua Ru

Никаких комиссий!

Теперь и навсегда!

Пополнить счет мобильного Киевстар, Vodafone, Life без комиссии:

Номер платежной карты:

Срок действия: / CVV2/CVC2:

Номер мобильного:

+380

Сумма, грн:

Я принимаю Условия использования сервиса

ПОПОЛНИТЬ

Pay4Free

Ua Ru

Никаких комиссий!

Теперь и навсегда!

Совершить мгновенный перевод с карты на карту любого банка Украины без комиссии:

Номер карты отправителя:

Срок действия: / CVV2/CVC2:

Номер карты получателя:

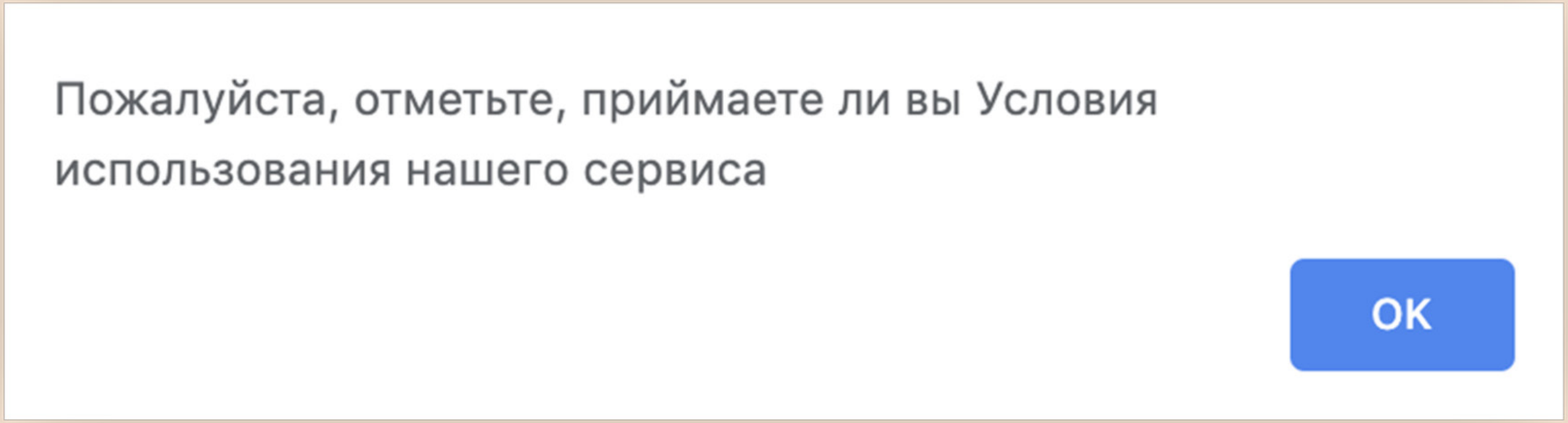
Сумма, грн:

Я принимаю Условия использования сервиса

ПЕРЕВЕСТИ

AFFIRMATIVE

“Hasta la vista, baby”



ПУБЛИЧНЫЙ ДОГОВОР

Вы согласны с этим Публичным договором и обязаны ознакомиться с его условиями:

3. ПРЕДМЕТ ДОГОВОРУ

3.1. Цей договір визначає умови роботи Сайту, що не є платіжним сервісом та не призначений для здійснення операцій з переказу коштів з використанням ЕПЗ (реквізитів ЕПЗ) в мережі Інтернет.

3.2. Сайт не містить файлів та ПЗ, що збирає, реєструє та/або накопичує реквізити ЕПЗ.

3.3. Сайт створений в рамках проекту Асоціації «Гуманний фішинг», метою якого є попередження громадян України про небезпеку існування фішингових веб-ресурсів та підвищення обізнаності щодо ефективних способів захисту власної інформації та правила безпечного використання ЕПЗ в Інтернет.

3.4. За умовами Публічного договору Споживач, натиснувши кнопку «Переказати» або «Поповнити», засвідчує повне і беззастережне прийняття умов цього Публічного договору (акцепт оферти), а також свідчить, що Споживач розуміє значення своїх дій, всі умови договору йому зрозумілі, він не перебуває під впливом помилки, обману, насильства, погрози тощо, і з цього моменту визначається як Платник.

СКРИПТ

«Я чту Уголовный кодекс. Это моя слабость»

**Не считывает и не сохраняет введенные цифры.
Только длину строки.**

ПРИМЕР:

2018-03-19 11:30:17 c2c ru 4-4-4-4 2/2 [3] 2 grn 4-4-4-4

ШКОЛА КІБЕРБЕЗПЕКИ

Ua Ru

Внимание!

Только что вы чуть не потеряли ваши деньги! Это могло произойти потому, что вы собственноручно ввели данные вашей платежной карты на сайте, который не является платежным сервисом!

Но вам повезло, что вы попали именно на наш сайт, а не на мошеннический. Наш сайт создан не для кражи карточных данных, а для информирования граждан Украины про опасность фишинговых сайтов и предупреждения случаев кибермошенничества.

Мы не получили и не сохранили никаких введенных вами карточных данных. Но существует множество сайтов, выдающих себя за платежные сервисы «на выгодных условиях», но на самом дле крадущих ваши карточные данные, а потом и денежные средства с ваших карт!

Защититесь:

- Проверяйте репутацию сайта, которому собираетесь доверить свои карточные данные. Просмотрите отзывы про него в Интернет. Особенно будьте бдительны к информации с пометкой «Реклама».
- Проверяйте возраст и срок регистрации доменного имени на whois и обратите внимание на даты "created" и "expires". У мошеннических сайтов обычно недавняя дата регистрации и зарегистрированы они лишь на 1 год.
- Запомните, 100% надежным сегодня может быть лишь платежный сервис, размещенный в зоне .ua. Пример: названиесайта.ua. Любые другие доменные зоны, в том числе .com.ua, kiev.ua, in.ua, com и др. — могут быть зарегистрированы кем угодно без ограничений.
- Проверяйте платежные сайты, услугами которых собираетесь воспользоваться, на наличие в Списке мошеннических сайтов.
- Установите лимиты вашей карты на операции в Интернет.
- Пользуйтесь только проверенными платежными сервисами:

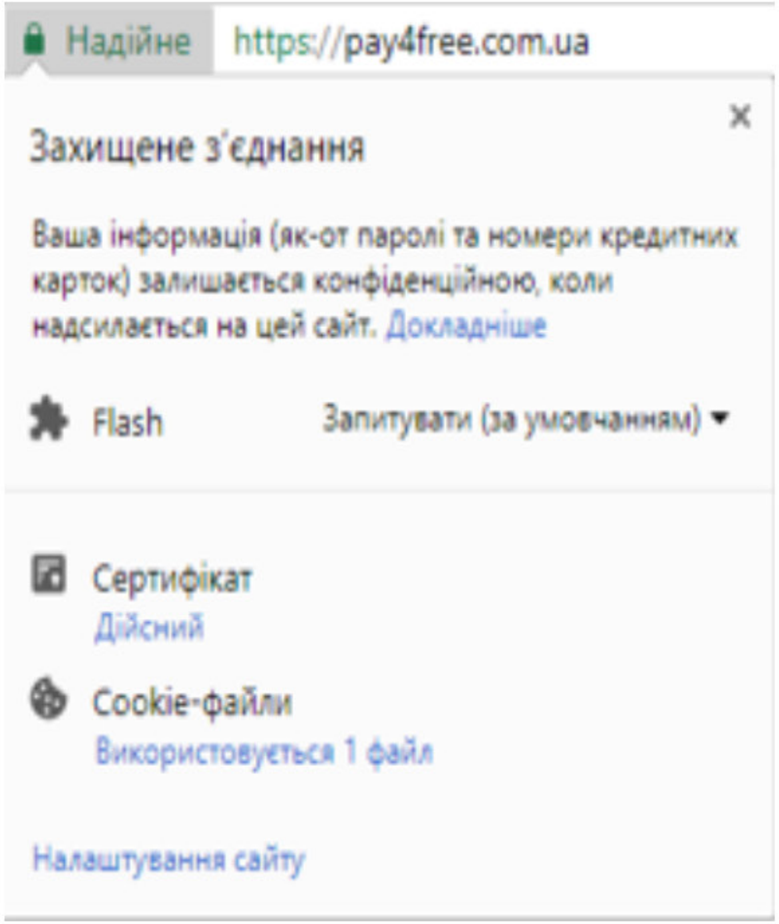
easypay | MOSST | PayPong | Platon | portmone.com | UA pay

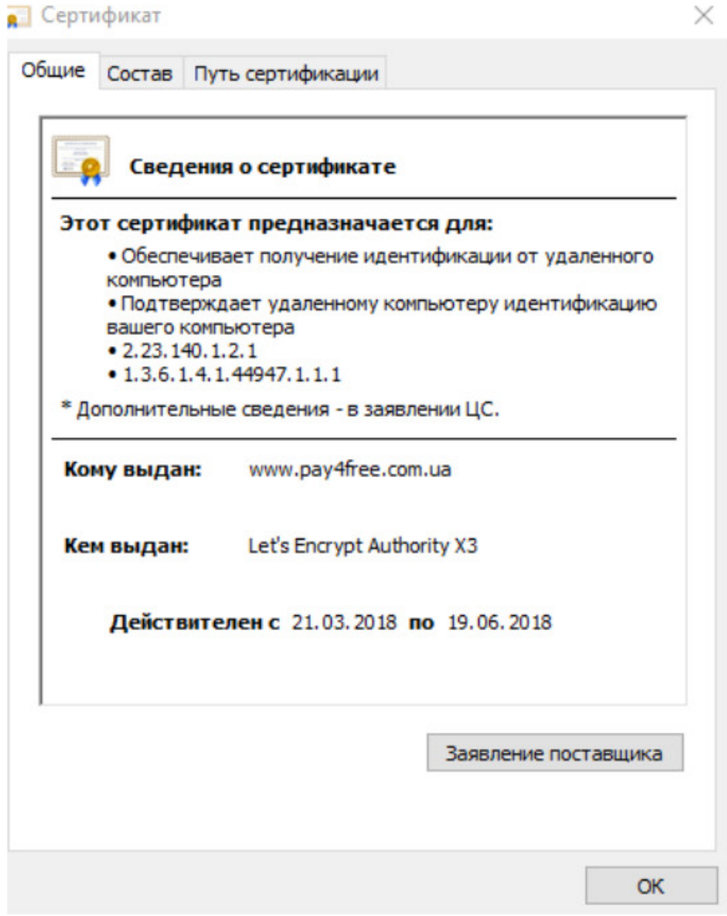
Ваша безопасность зависит только от вас!

Больше про киберзащиту:

РАДИ ЧИСТОТЫ ЭКСПЕРИМЕНТА

Бесплатный сертификат Let’s Encrypt





ЭТО СЛАДКОЕ СЛОВО SEO

SEO Score

93%

Whois Record for Pay4Free.com.ua

DOMAINTOOLS for Windows Download Now
Access domain ownership records from your desktop

Domain Profile

Registrar	ua.imena IANA ID: – URL: – Whois Server: –
Registrar Status	
Tech Contact	–
IP Address	185.68.16.60 - 825 other sites hosted on this server
IP Location	- Kyiv - Kiev - Hosting Ukraine Ltd
ASN	AS200000 UKRAINE-AS, UA (registered Nov 07, 2013)
Whois History	3 records have been archived since 2018-03-12

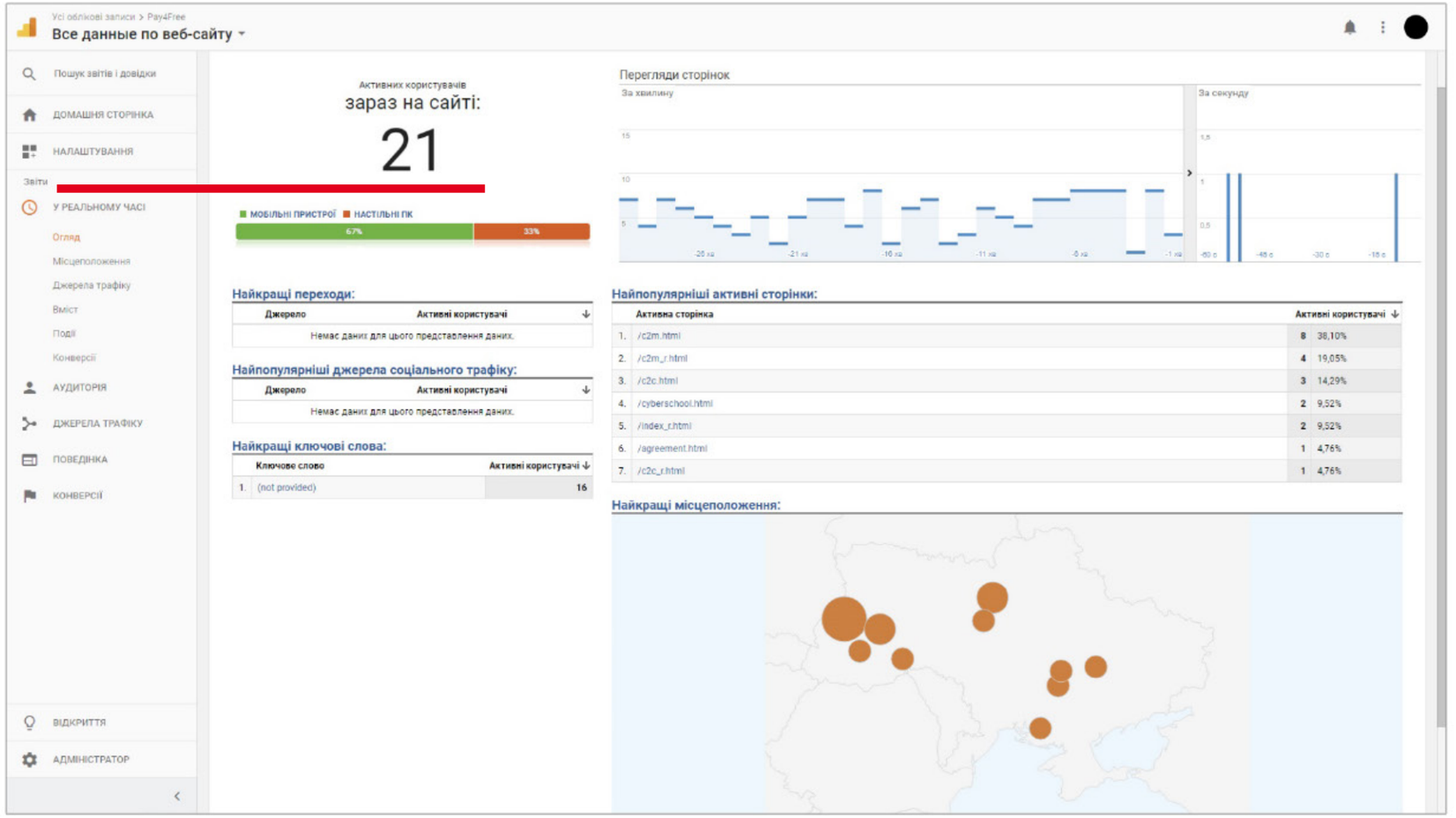
Website

Website Title	Школа Кібербезпеки
Server Type	nginx
Response Code	200
SEO Score	93%
Terms	173 (Unique: 137, Linked: 4)
Images	18 (Alt tags missing: 6)
Links	12 (Internal: 1, Outbound: 11)

НА СТАРТ, ВНИМАНИЕ, МАРШ!

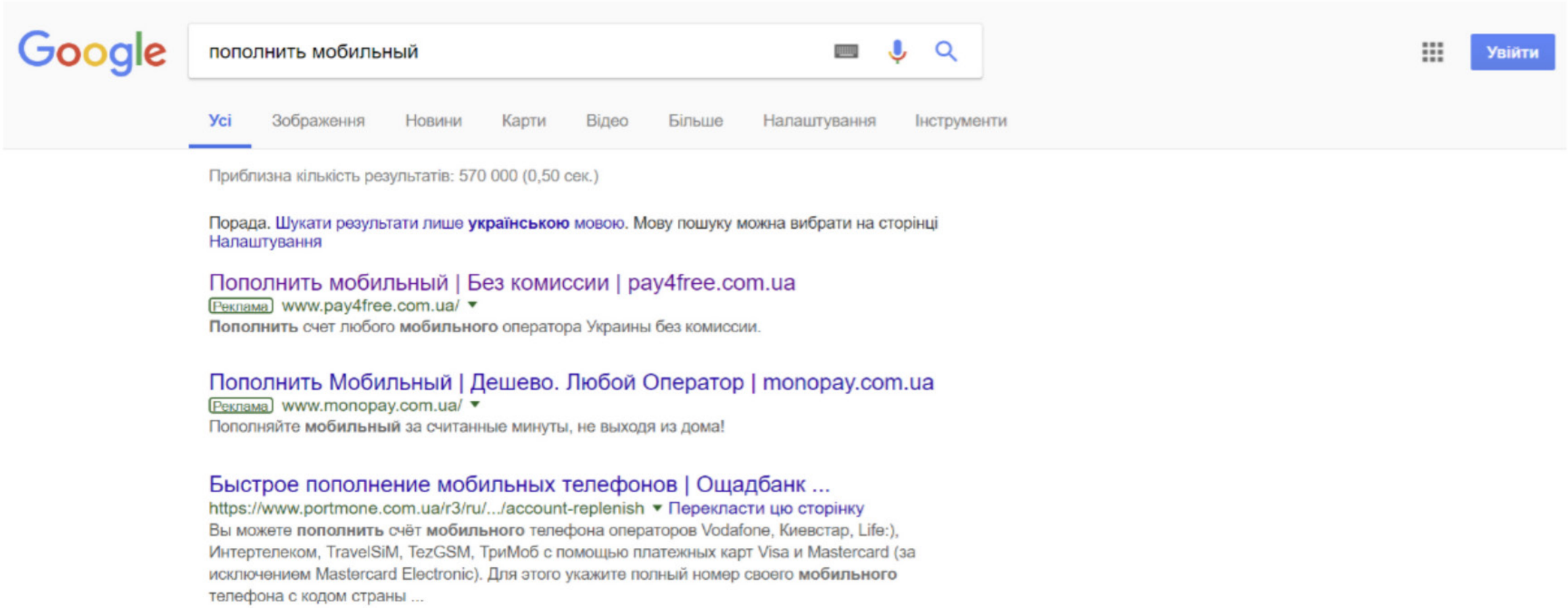
29 марта 2018 – «ну, понеслась!»

21



ВСЯ СИЛА В РЕКЛАМЕ, БРАТ!

Первые в поисковой выдаче



ВСЯ СИЛА В ХАЛЯВЕ, БРАТ!

Рекламные объявления

- **Пополнить мобильный. Без комиссии.**
  pay4free.com.ua | Пополнить счет любого мобильного оператора Украины без комиссии.
- **Поповнити мобільний. Без комісії.**
  pay4free.com.ua | Поповнити мобільний рахунок будь-якого оператора України без комісії.
- **Переказ з картки на картку. Без комісії.**
  pay4free.com.ua | Миттєвий переказ з картки на картку будь-якого банку України без комісії.
- **Перевод с карты на карту. Без комиссии.**
  pay4free.com.ua | Мгновенный перевод с карты на карту любого банка Украины без комиссии.

ВСЯ СИЛА В ПОЛНОЙ ХАЛЯВЕ, БРАТ!

Популярные ключевые слова

Ключове слово	Кліки	Покази	CTR	Сер. ціна за клік	Вартість
поповнити мобільний	3 625	27 451	13,21%	0,43 грн.	1 567,65 грн.
пополнить без комиссии	1 997	17 262	11,57%	0,52 грн.	1 036,98 грн.
пополнить мобильный	1 832	17 640	10,39%	0,52 грн.	957,39 грн.

ДЕНЬГИ И РУЧНОЙ ТРУД ВСЕ ПЕРЕТРУТ!

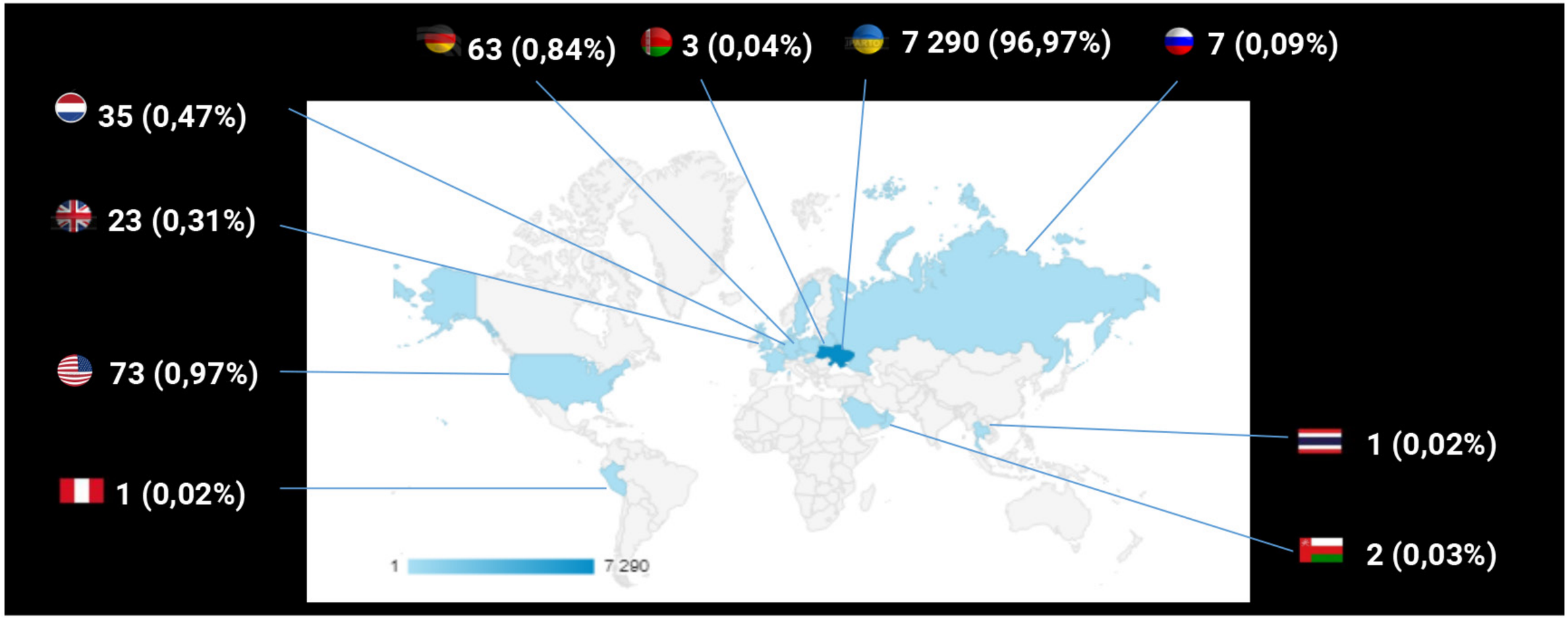
Статистика аукциона

Домен відображуваної URL-адреси	Частка показів
portmone.com.ua	34,50%
Ви	11,99%
ipay.ua	< 10%
gopays.in.ua	< 10%

АУДИТОРИЯ САЙТА И ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

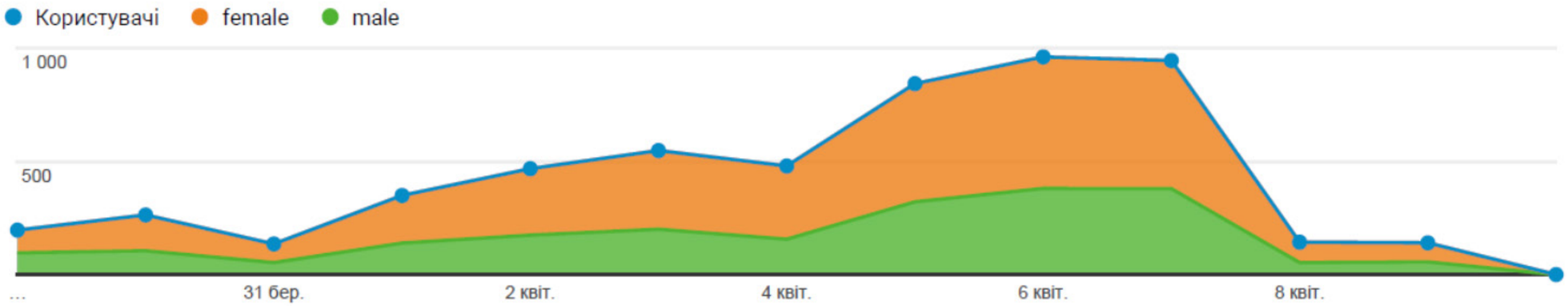
АУДИТОРИЯ САЙТА

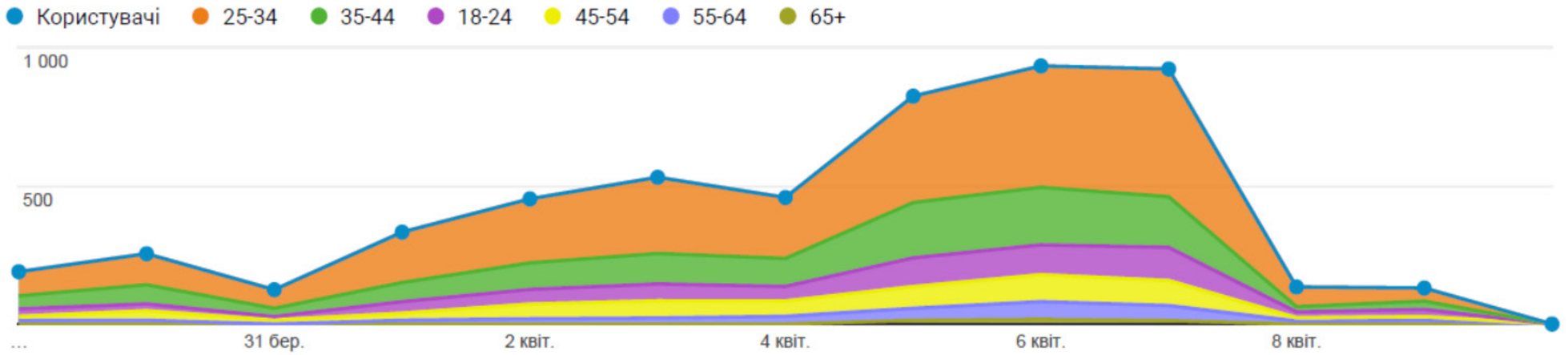
Источники траффика



АУДИТОРИЯ САЙТА

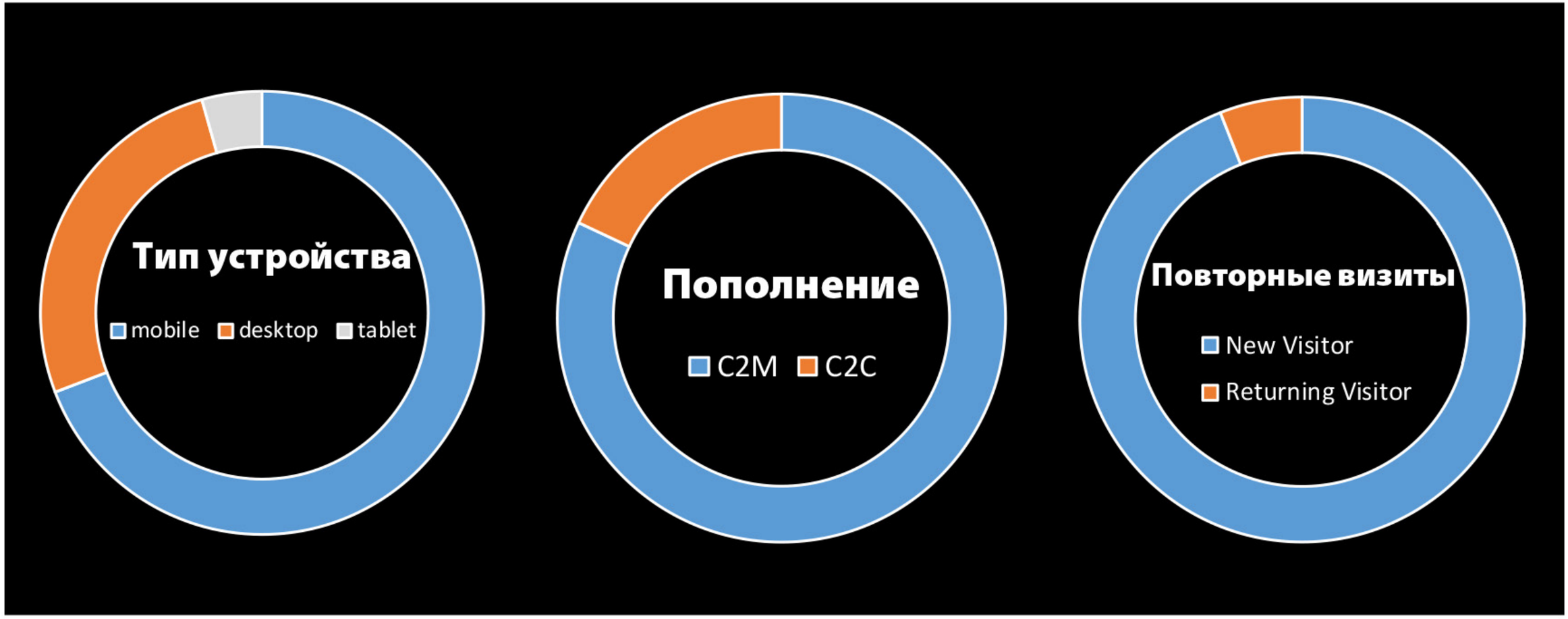
Дифференциация по полу и возрасту





АУДИТОРИЯ САЙТА

Тип устройства, операция, возвращение на сайт



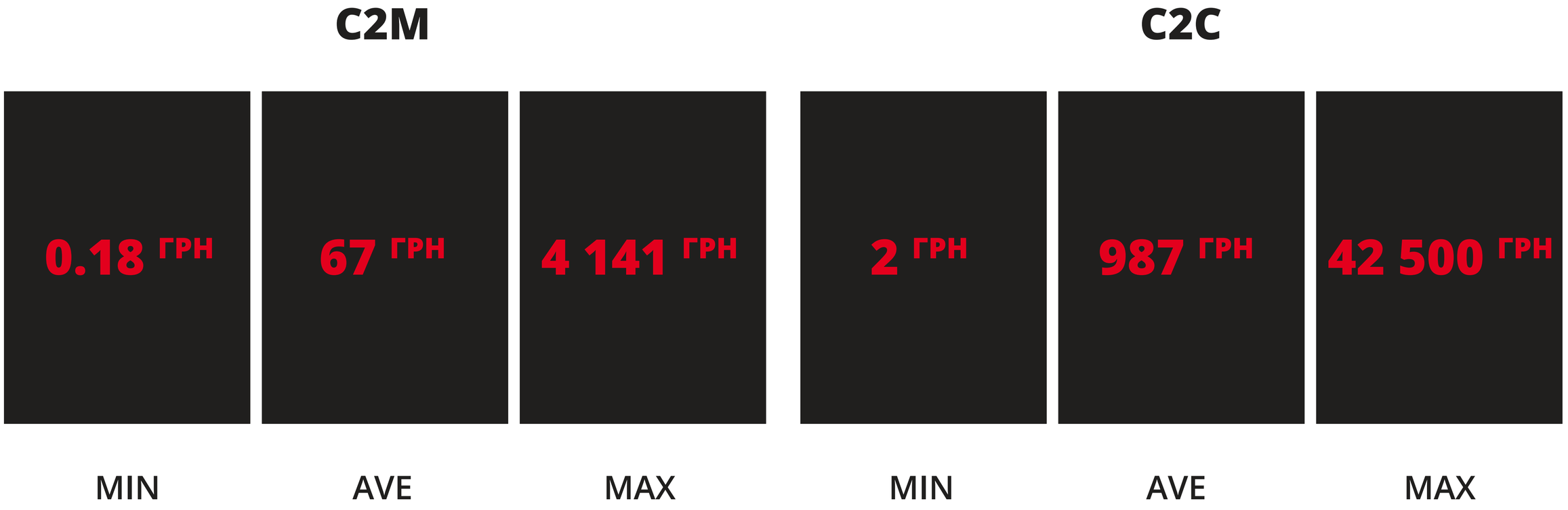
ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Средняя длительность сеанса

00:02:20

ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Сумма пополнения



ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Лидер гонки

2018-03-31 15:12:39	4-4-4-4	2/4	4-4-4-4	N/A	3	200
2018-03-31 15:18:29	4-4-4-4	2/4	3	9	N/A	50
2018-03-31 16:42:28	4-4-4-4	2/4	4-4-4-4	N/A	3	42500
2018-03-31 17:05:24	4-4-4-4	2/4	3	9	N/A	35
2018-03-31 17:06:59	0-0-0-0	2/4	0	9	N/A	20
2018-03-31 17:08:50	4-4-4-4	0/0	4-4-4-4	N/A	3	500
2018-03-31 17:16:35	4-4-4-4	2/4	4-4-4-4	N/A	3	500
2018-03-31 17:19:52	4-4-4-4	2/4	4-4-4-4	N/A	3	60
2018-03-31 17:23:57	4-4-4-4	2/4	4-4-4-4	N/A	3	900

ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

«Галочка» для галочки

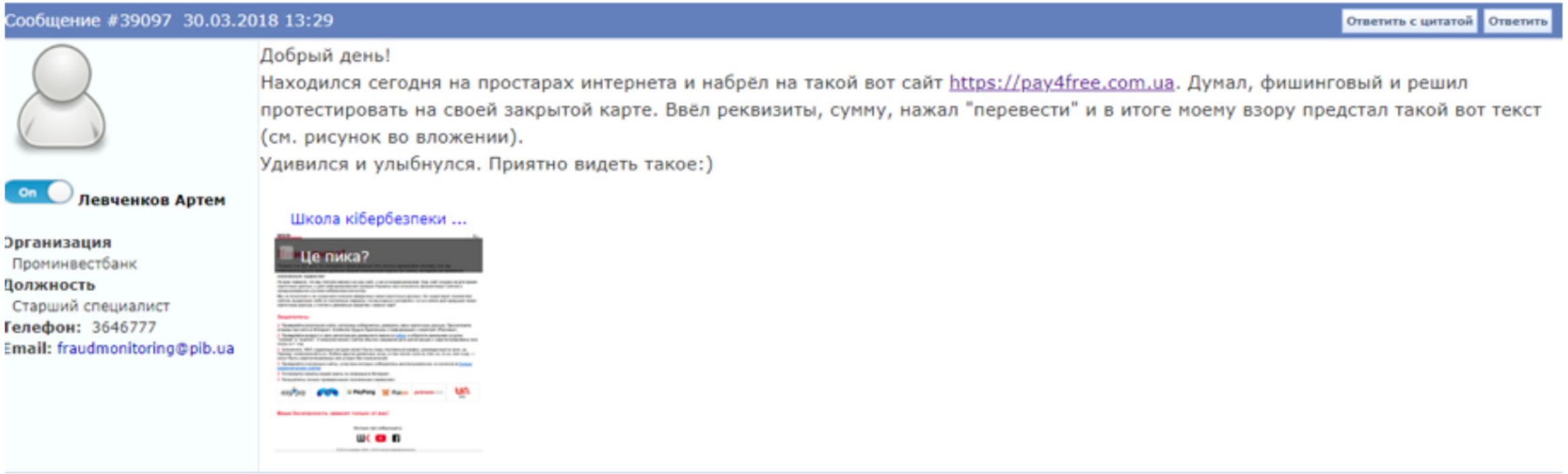
77.6%

Согласились с условиями
не читая самих условий пользования сервисом

«Хотим стать вашим агентом» (с)

БДИТЕЛЬНОСТЬ

сотрудников банков и Киберполиции



Сайт посетили 7 банковских сотрудников и 1 сотрудник Киберполиции

ИТОГИ

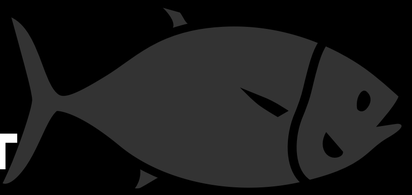
#ГУМАННЫЙ ФИШИНГ | PAY4FREE.COM.UA

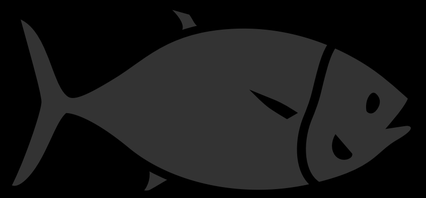
ПОДВЕДЕНИЕ ИТОГОВ

проведения контекстной PPC «рыбалки» в Google (29.03-10.04.18)

7 516

рыбок
заплыло на псевдо-фишсайт и попло в расставленные сети





7 172

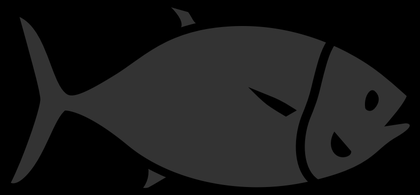
рыбок
поймано и отпущено на волю после инструктажа по технике безопасности

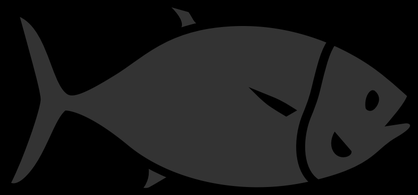
ПОДВЕДЕНИЕ ИТОГОВ

А если задуматься?!

4 172

держателей
оставили реквизиты карт
на непроверенном веб-сайте

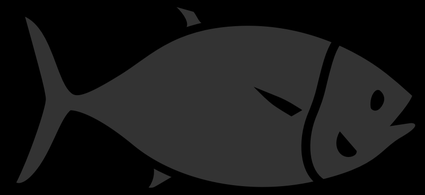


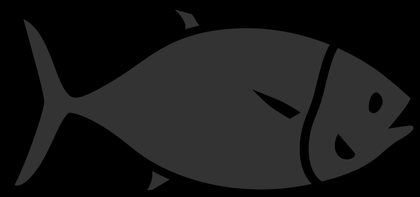


ПОДВЕДЕНИЕ ИТОГОВ

Себестоимость обучения / мошенничества

CPC = 0,69 UAH





ОЦЕНКА РЕЗИСТЕНТНОСТИ К ФИШСАЙТАМ

44.5%

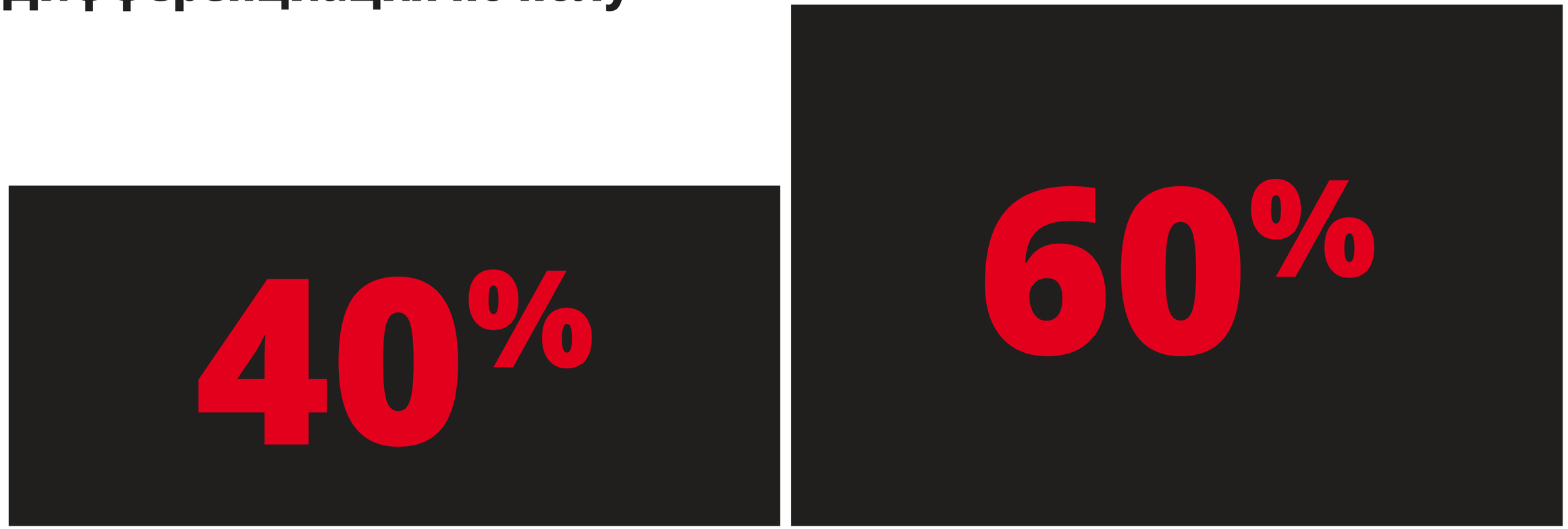
Граждане с высокой резистентностью

55.5%

Граждане с низкой резистентностью

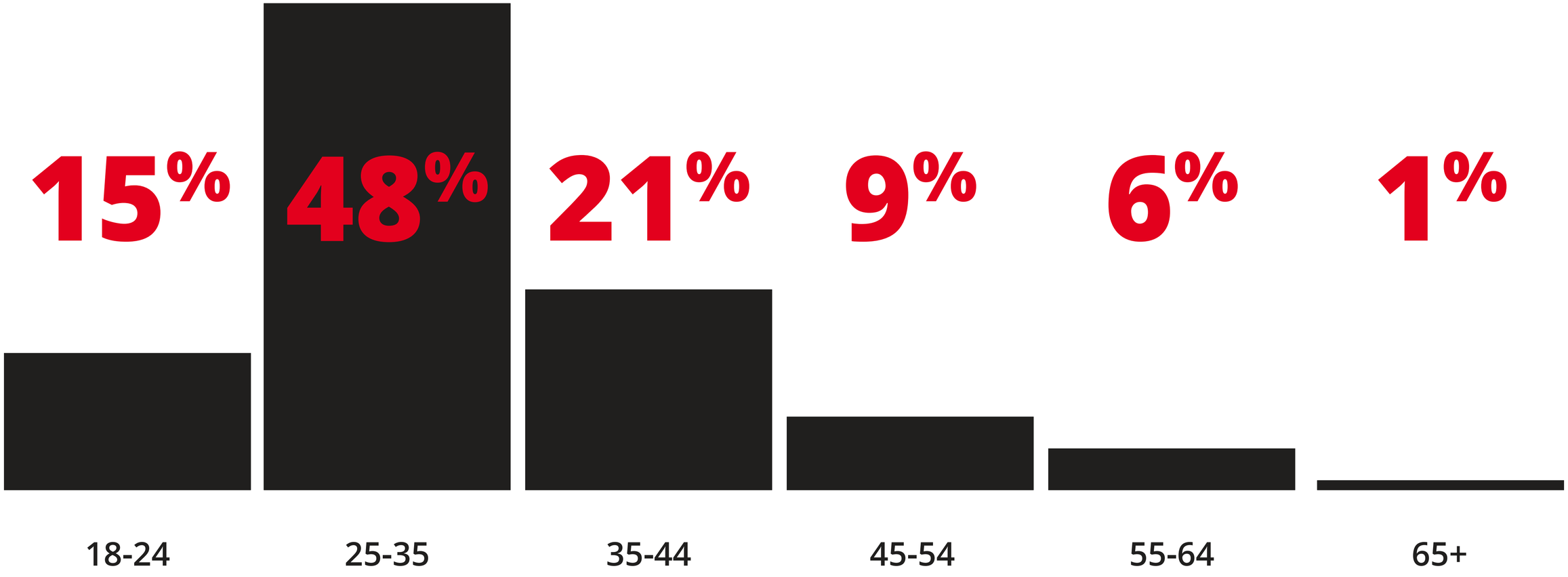
НИЗКАЯ РЕЗИСТЕНТНОСТЬ

Дифференциация по полу



НИЗКАЯ РЕЗИСТЕНТНОСТЬ

Дифференциация по возрастным категориям



BLACK SQUIRREL

ПЕРЫЙ АНТИМОШЕННИЧЕСКИЙ ТЕЛЕСЕРИАЛ

Неподконтрольная территория

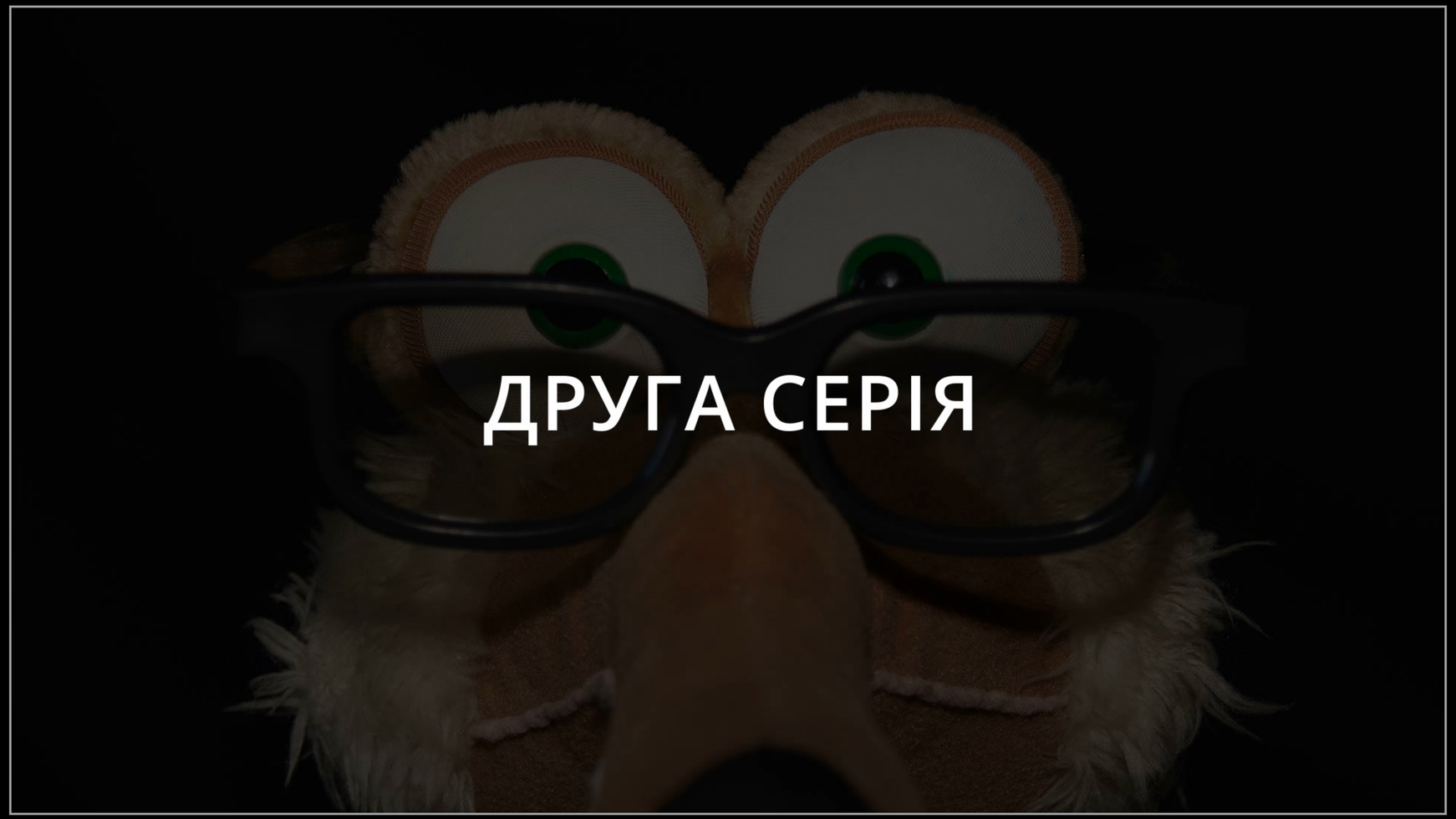
Страх потеряли

Посадить сложнее, чем Falcon 9

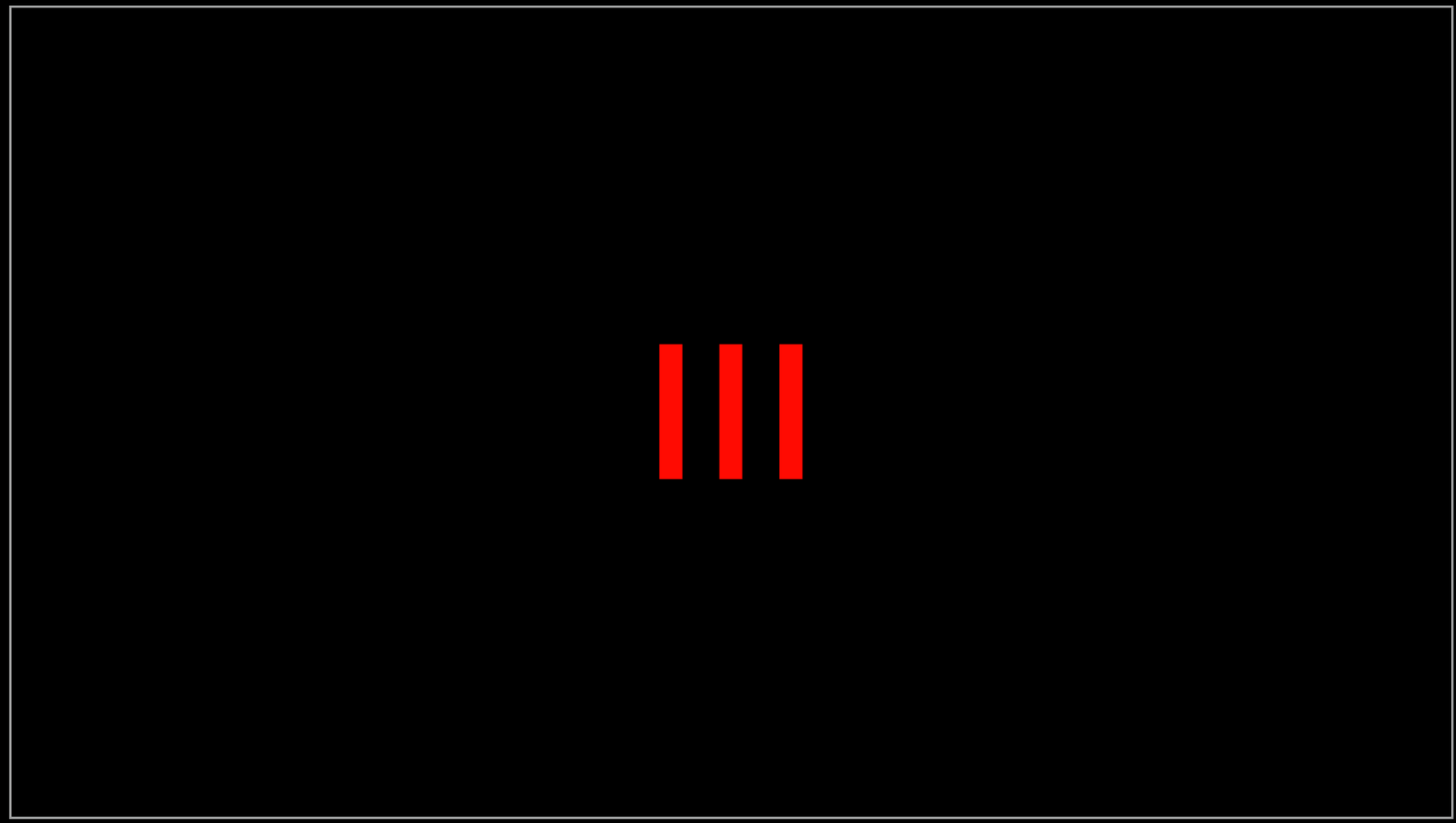
«... он же памятник...»

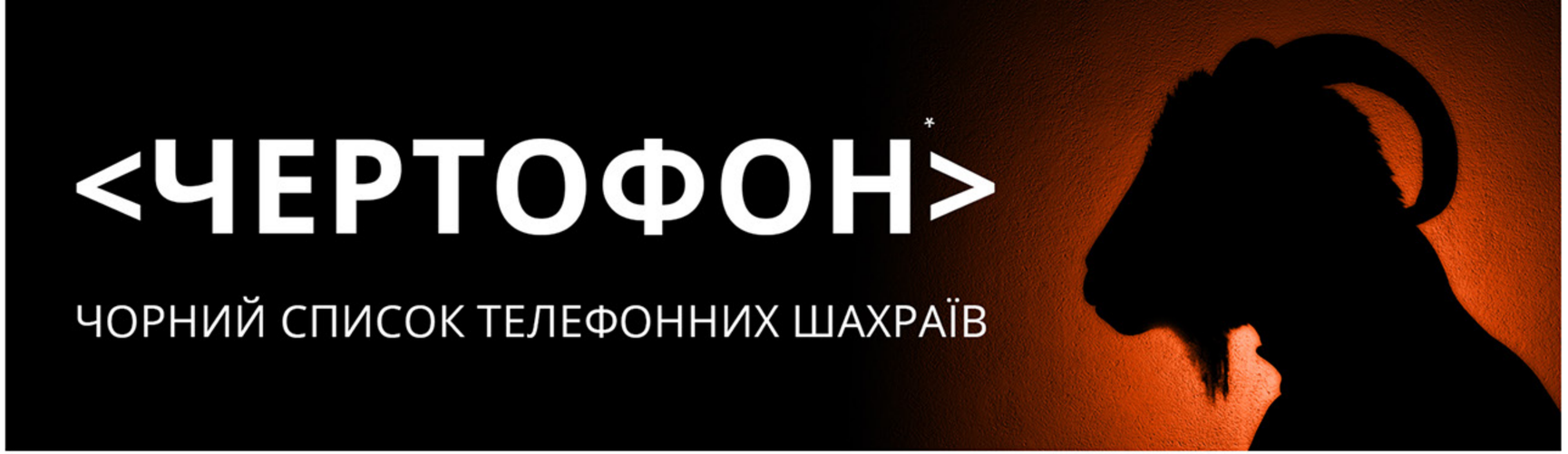
1. НБУ, Число зверя и «пластиковый держатель»

2. Досвидос



3. Chertofon





Шахраї, назвавшись представивником банку, телефонують або розсилають sms, лякаючи тим, що вашу платіжну картку нібито заблоковано. Після чого під виглядом уточнення інформації, випитують секретні дані картки (термін дії, тризначний код зі звороту та банківські sms-паролі). Повідомивши ці дані шахраям, легковірні громадяни власноруч відкривають зловмисникам доступ до свого рахунку та коштів на ньому.

191	Шахрайське смс з **066 682 09 43**. «Raiffaizen Bank Aval Vashu kartku zablokovano. Dlia rozblokuvannia dzvonit` za nomerom **094 127 22 70**».
190	Шахрайське СМС з **050 207 62 89**. «Ваша картка буде заблокована терміново пройдіть авторизацію, по номеру: **044 599 52 00**, **066 394 11 46**».
189	Шахрайське смс з номеру **067 381 80 13**: "Oschadbank" vasha kartka zablokovana. Za informaciey zvertaytes za nomerom **099 354 18 65**, **044 229 08 36** abo na sayti online.oschadbank.ua.
188	Шахрайське СМС з **099 452 38 75**. «Ваша карта заблокирована банком, пройдите авторизацию: **044 227 63 00**, **044 383 28 08**».
187	Шахрайське СМС з **095 345 40 78** . «Ваша карта заблокирована банком, пройдите авторизацию или перезвоните

Google

094 620 69 47

Усі | Карти | Зображення | Новини | Відео | Більше | Налаштування | Інструменти

Приблизна кількість результатів: 8 290 000 (0,54 сек.)

Какой оператор имеет код 094? Что это такое и для чего он нужен.

https://trushenk.com/konvergentnyj-nomer.../comment-page... ▾ Перекласти цю сторінку

094 - что за оператор? ... Преимущества и недостатки номера с кодом **094** ... Например номер 044-5920000 будет выглядеть как **094**-8920000. ... **094** 885 **69** 50 еще один разводила представляется как Дмитрий Одинцов. Не ведитесь. ... в черный список добавьте и эти номера: **094** 884-16-45, **094 620**-67-14, ...

CHERTOFON - Чорний список телефонних шахраїв

chertofon.com/ ▾

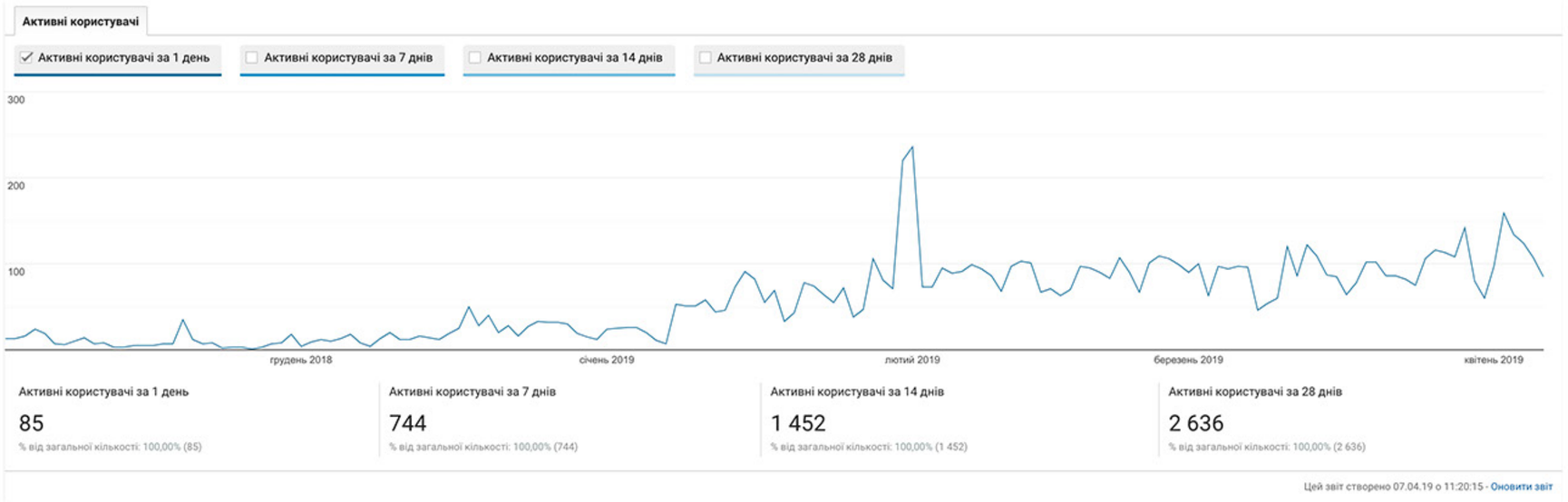
81, 18.11.2018 Дзвінок з 044 332 96 63, **094 620 69 47**. .... 35, СМС з номера 099 926 69 33 «Вашу банківську картку буде заблоковано, потрібно пройти ...

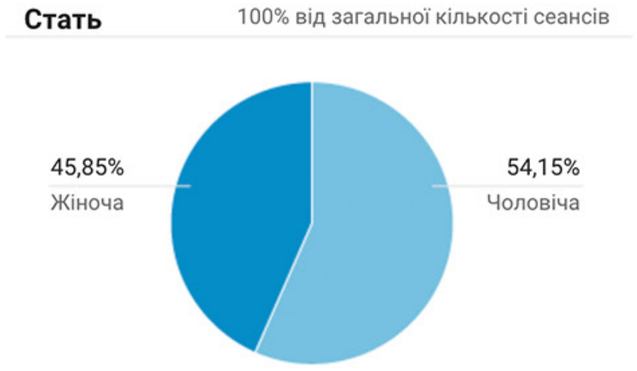
+380 (95) - Блог OLX.UA

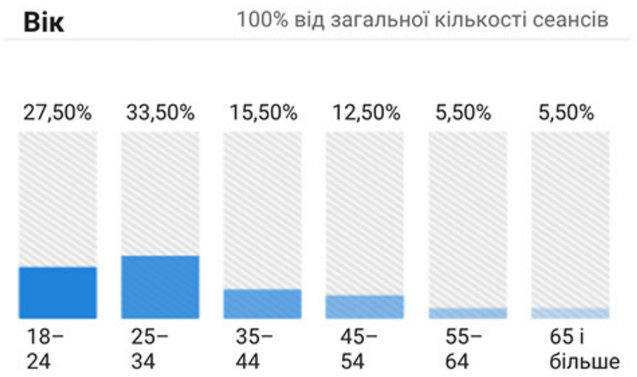
blog.olx.ua/ru/6433/ostorozhno-telefonnyie-moshenniki/ ▾ Перекласти цю сторінку

2 лип. 2014 р. - ... с городского номера 056 785 93 **69** типа представитель приват банка Будьте осторожны!!!! .... Оксана • 22.07.2014 в 20:**47** ..... Мне звонили с номера интертелоком: **094** 911 04 61. .... Андріана • 16.01.2015 в 02:**47**.

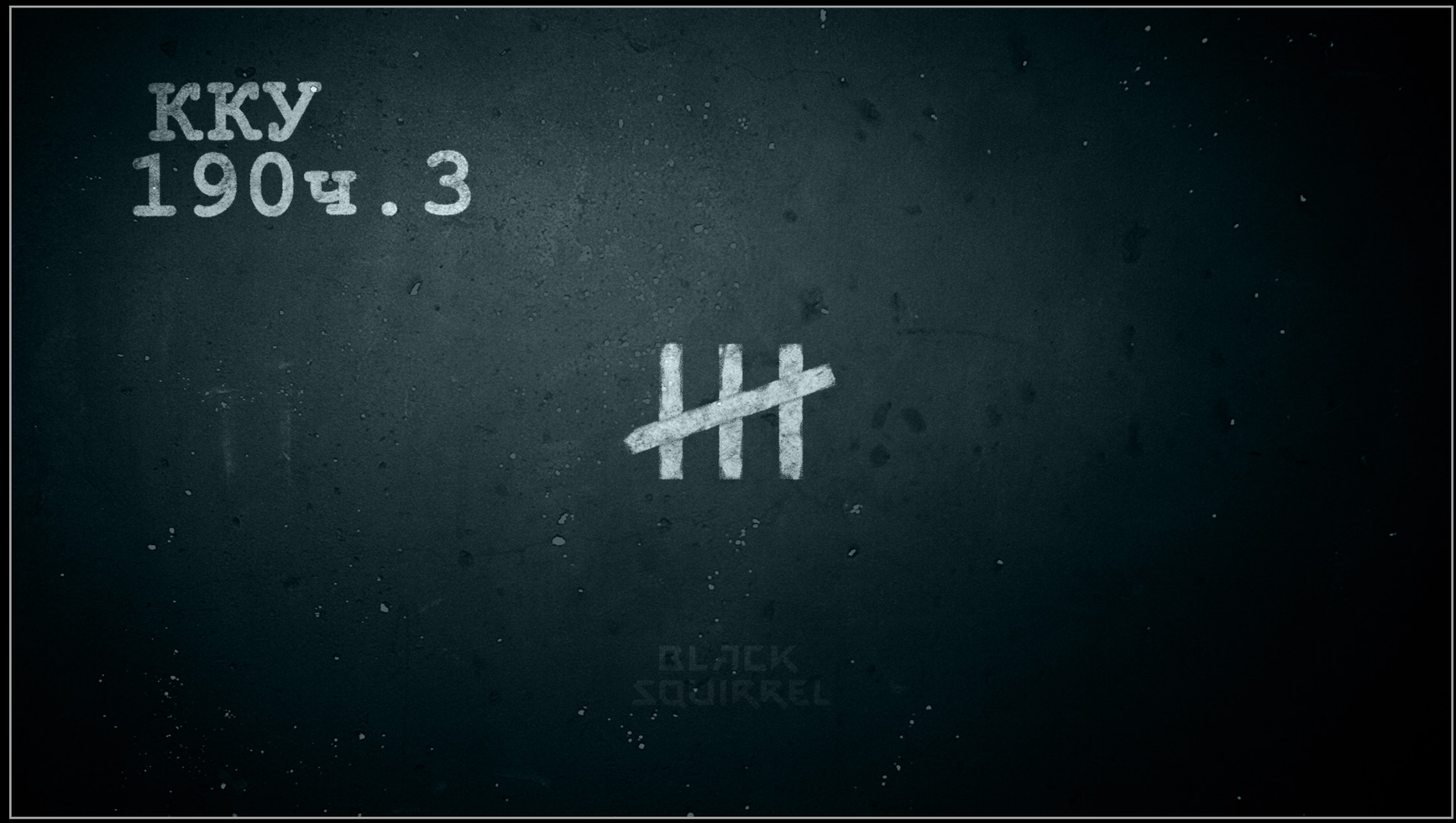
ЧЕРТОФОН / СТАТИСТИКА







4. ККУ 190 ч.3

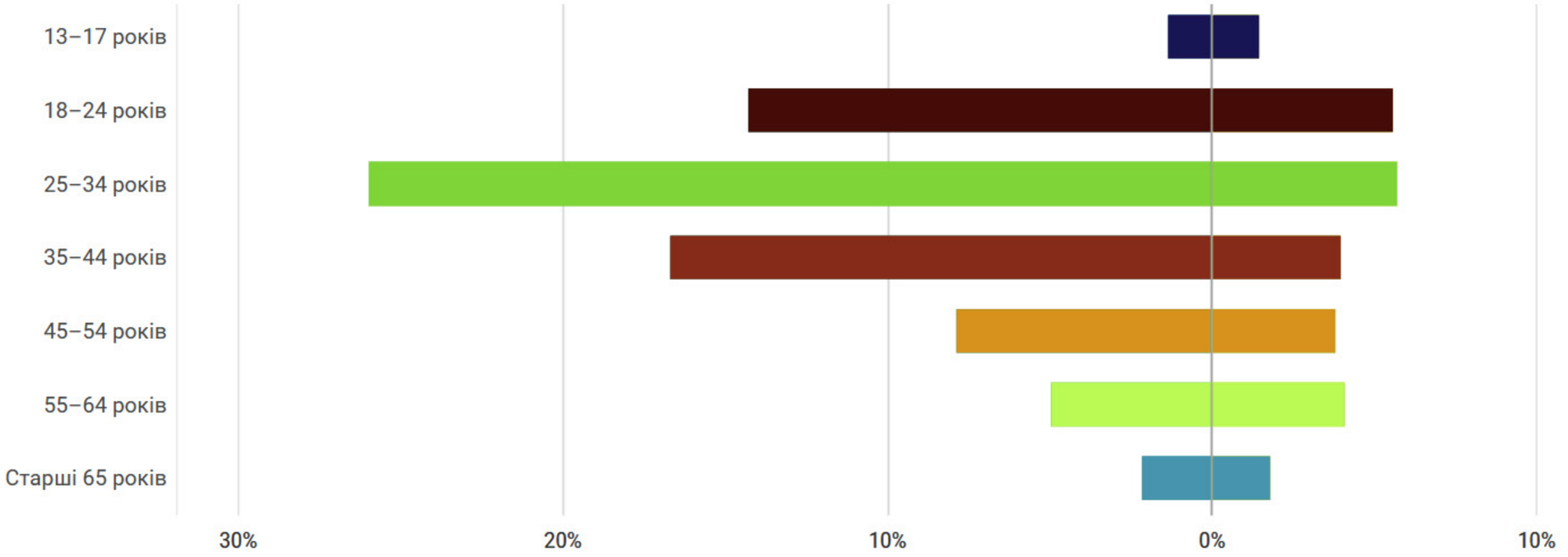


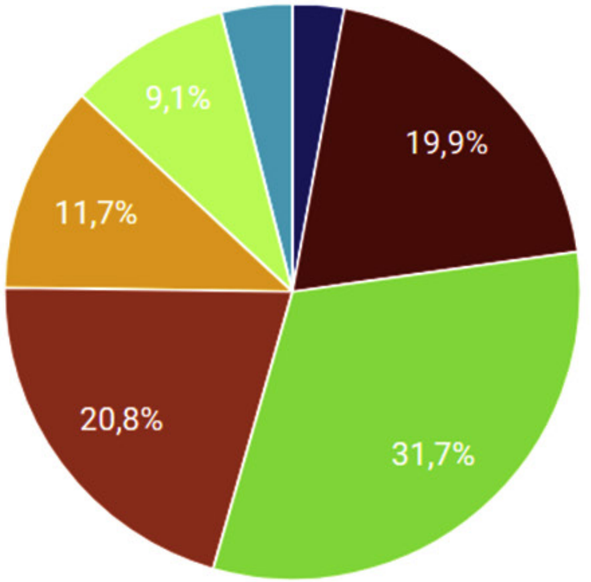
350 000

ПРОСМОТРОВ

26158 вовлечение, 3600 реакций

BLACK SQUIRREL / СТАТИСТИКА / АУДИТОРИЯ (YOUTUBE)

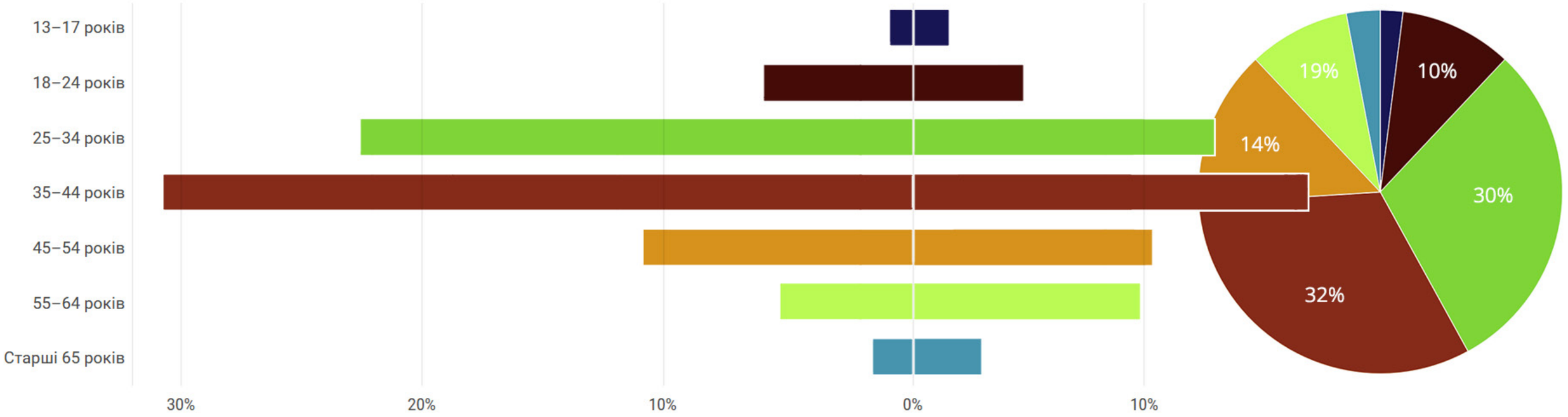




М

Ж

BLACK SQUIRREL / СТАТИСТИКА / АУДИТОРИЯ (FACEBOOK)



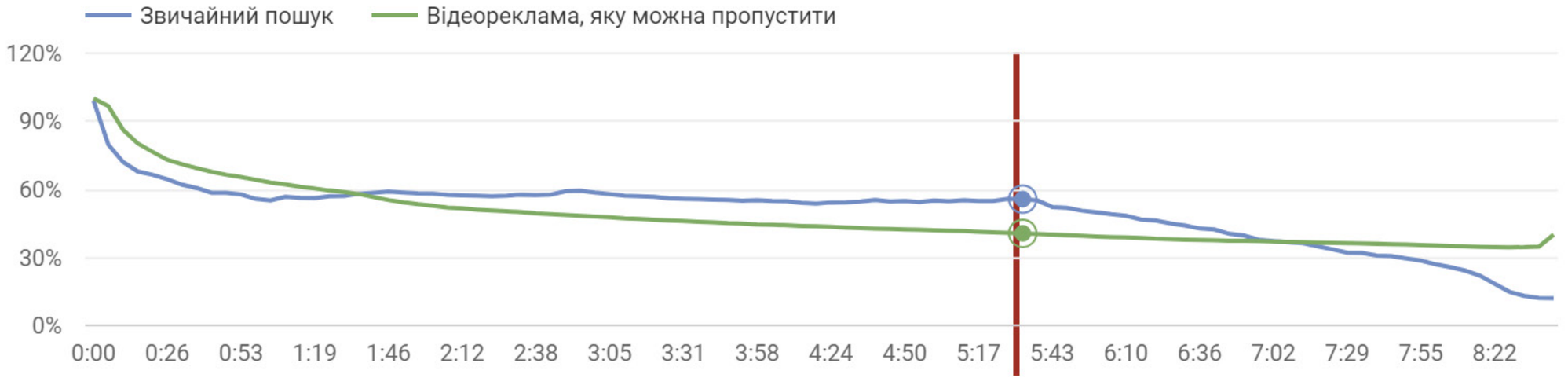
М Ж

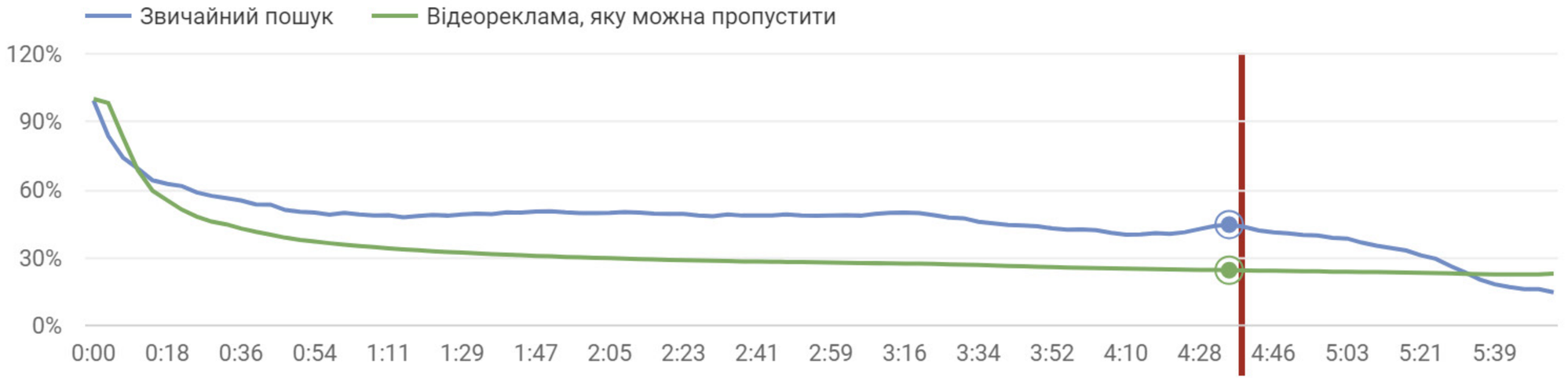
BLACK SQUIRREL / СТАТИСТИКА

Донецька область, Україна	Перегляди
Донецьк	1 309
Маріуполь	955
Краматорськ	540
Макіївка	493
Слов'янськ	316
Горлівка	233
Бахмут	206
Костянтинівка	182
Покровськ	159
Єнакієве	125
Мирноград	120
Добропілля	119
Дружківка	111
Волноваха	95
Харцизьк	80
Торецьк	69
Курахове	69
Шахтарськ	68
Чистякове	63

Луганська область, Україна	Перегляди
Луганськ,	752
Сєвєродонецьк, Луганська область, Україна	293
Лисичанськ, Луганська область, Україна	282
Алчевськ, Луганська область, Україна	167
Рубіжне, Луганська область, Україна	133
Сорокине, Луганська область, Україна	109
Хрустальний, Луганська область, Україна	90
Старобільськ, Луганська область, Україна	85
Сватове, Луганська область, Україна	80
Ровеньки, Луганська область, Україна	79
Довжанськ, Луганська область, Україна	78
Антрацит, Луганська область, Україна	72
Кадіївка, Луганська область, Україна	58
Брянка, Луганська область, Україна	57
Кремінна, Луганська область, Україна	52

BLACK SQUIRREL / СТАТИСТИКА / УДЕРЖАНИЕ ВНИМАНИЯ





BLACK SQUIRREL / СТАТИСТИКА / УДЕРЖАНИЕ ВНИМАНИЯ

BLACK SQUIRREL

Ukrainian Interbank Payment Systems Member Association "EMA"
Опублікував Артем Денисов [?]
Вподобана сторінка · 19 листопад ·

#відсічшахраям
УВАГА! КОНКУРС!

Ukrainian Interbank Payment Systems Member Association "EMA", спільно з сайт «Чертофон» та Black Squirrel, оголошують конкурс на кращий тролінг шахрая!

Свіженькі номери шахраїв завжди тут: http://chertofon.com/ Приклад тролінгу: https://youtu.be/yj2_yRyh12w або https://youtu.be/brx3pOjANVU.

Необхідно записати аудіо або відео тролінгу шахрая, та надіслати його на адресу fera@ema.com.ua. Тролінги приймаються до 31.12.2018 включно і будуть розміщені на https://www.youtube.com/BlackSquirrel. Переможцем буде оголошено тролінг, який набере найбільшу кількість переглядів станом на 00:00 UTC+2 01 березня 2019 року.

Переможцю — респект, уважуха та Сертифікат* «Лютий Троль 80 левела» за підписом #чорнийбілка та Alexandr Karpov.

*Сертифікат можна буде поствити у серванті щоб всі бачили. Це нереально круто! Хай заздрять!

Позначити ... | Додати роз... | Редагув...

4 460 Охоплення
405 Engagement
Рекламувати допис

Напишіть коментар...

Anjick Андрій 1 місяць тому (змінено)

@Black Squirrel дуже красиво і грамотно все розставляєте по поличкам)), цікава фонова музика+ до того всього ще й візуально пояснюєте, що зрозуміє навіть пенсіонер із глухого села), хотілося б у наступних випусках ближче дізнатись як можна себе захистити у випадку інтернет продаж наприклад ОЛХ і тому подібних, і якшо вже таке сталось що робити, щоб отримати свої кошти назад?...дуже дякуємо за ваші старання, Чорний Білка скоро виявиться страшним чорним сном для шахраїв))...

Показати менше

2 ВІДПОВІСТИ

Стас А 3 тижні тому

Підтримаю Андрія. На мою думку, ролики про шахрайство на OLX були би актуальні. Хоть і інформації вистачає в мережах, і кожен бажаючий може її знайти, але у таких справах чим більше навчальних уроків є, тим краще. Ну і Білка буде мати контент) Дякуєм за Вашу працю!)

1 ВІДПОВІСТИ

Марина Секретченко 5 місяців тому

Спасибо большое, очень познавательно.Был уже опыт,просили срочно идти к банкомату, и перезвонить. А они расскажут , что нужно нажать, чтобы предотвратить снятие денег с карты кем-то. Не повелась,так как карта была дома и денег на ней было 17 грн. После звонка в банк ,сказали ,что это мошенники.

1 ВІДПОВІСТИ

Як крадуть гроші через інтернет
Телеканал 1+1
87 тис. переглядів

НБУ, Число звіра і «пластиковый...
Black Squirrel
7,9 тис. переглядів

Угорськомовні українці висловили свою думку...
ТСН
78 тис. переглядів

Chertofon. Третя серія
Black Squirrel
6,8 тис. переглядів

Як живуть волохи на Закарпатті
Gazeta UA
91 тис. переглядів

ПОКАЗАТИ БІЛЬШЕ

конкурс тролінгів

Шахрай до 2025 року

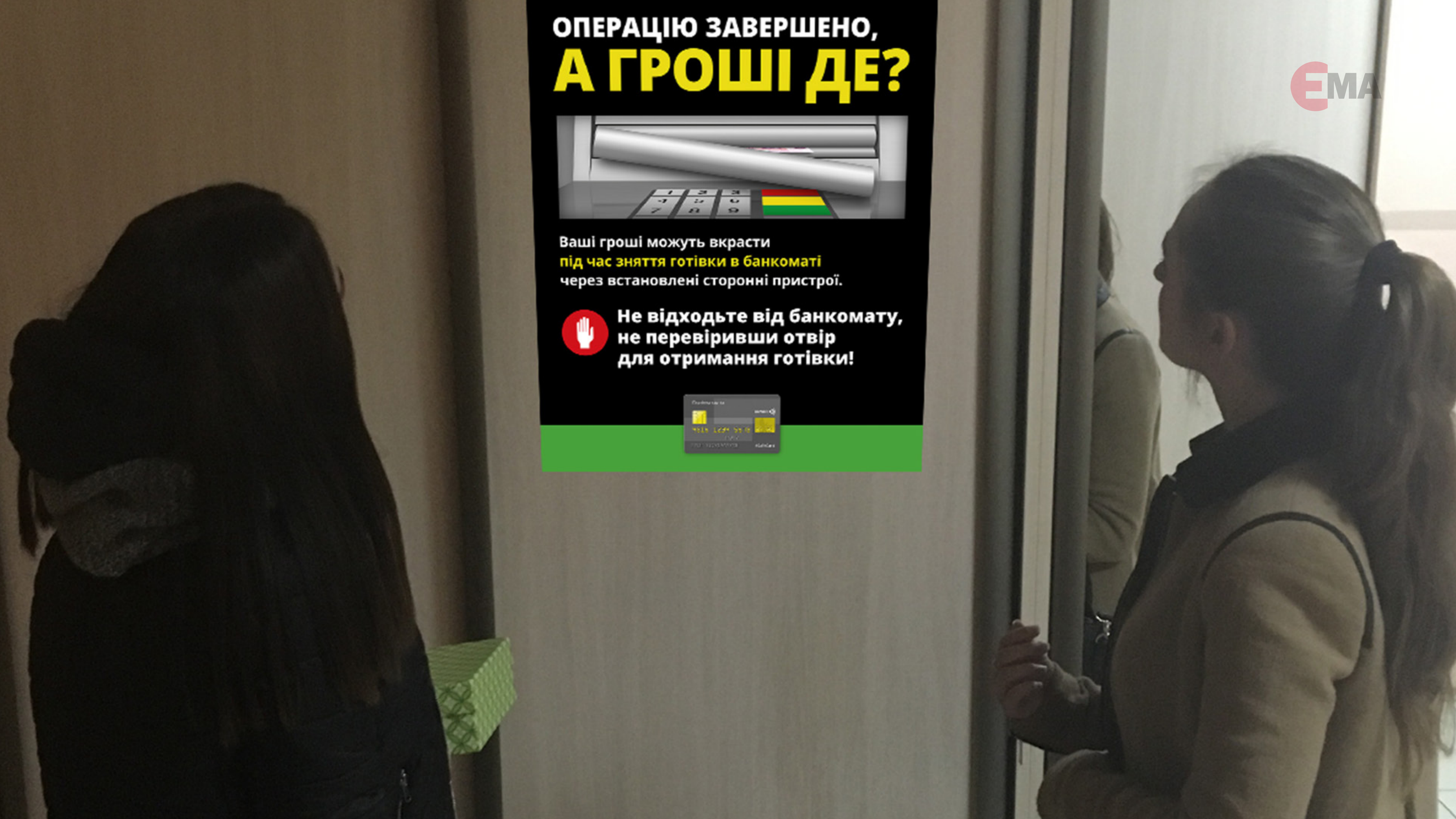
автор-троль: Сергій Іванович

#004

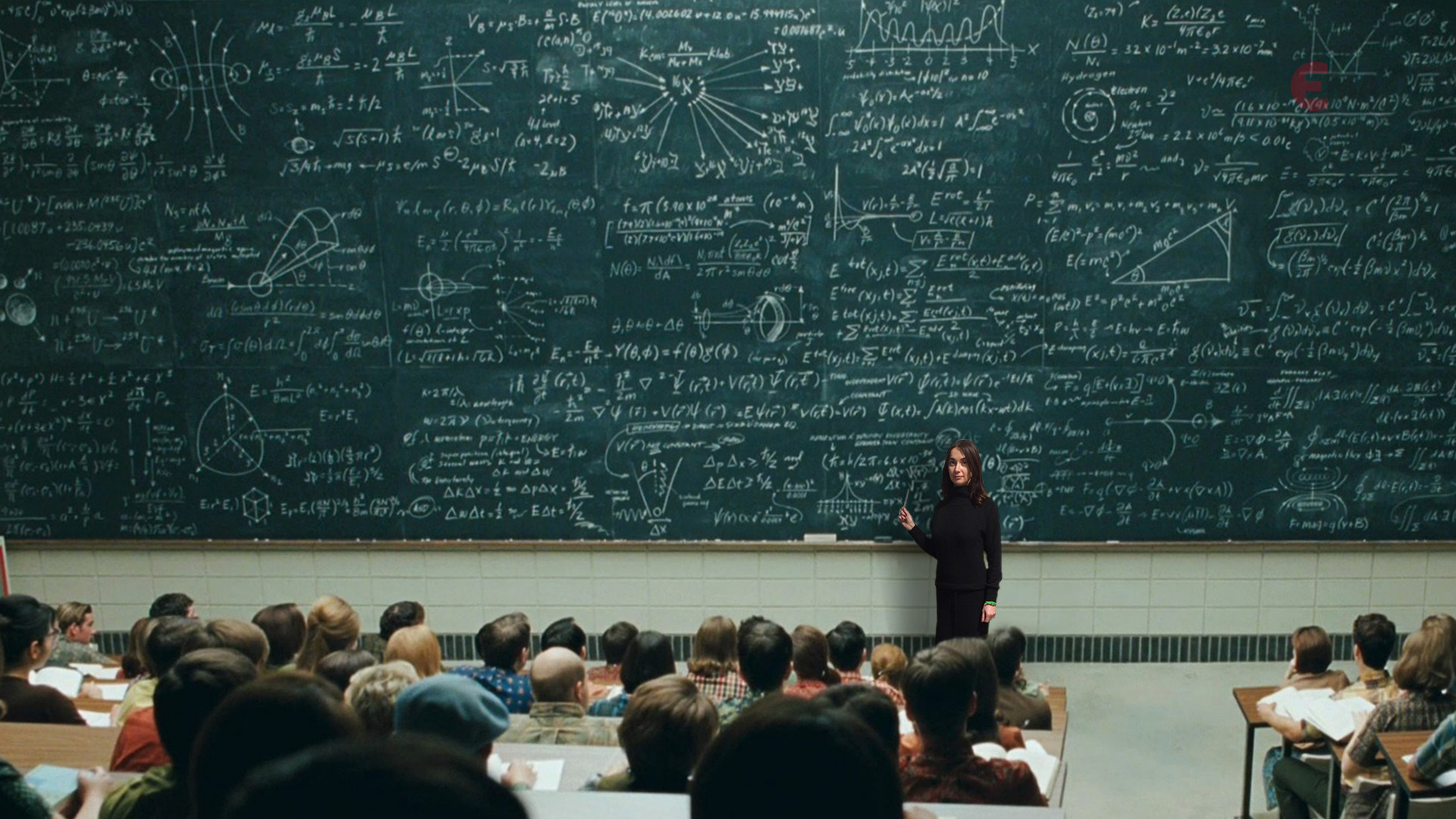
ОБУЧЕНИЕ СТУДЕНТОВ И ПЕДАГОГОВ

ОБРАЗОВАТЕЛЬНАЯ КАМПАНИЯ

КИЕВСКИЙ УНИВЕРСИТЕТ ИМЕНИ БОРИСА ГРИНЧЕНКО


ОПЕРАЦІЮ ЗАВЕРШЕНО,
А ГРОШІ ДЕ?
Ваші гроші можуть вкрасти
під час зняття готівки в банкоматі
через встановлені сторонні пристрої.
Не відходьте від банкомату,
не перевіривши отвір
для отримання готівки!

ІНФормація – знання
Календар знаменних і пам'ятних дат
До уваги читачів
Збережи свої гроші!
ЗА ЖОДНИХ УМОВ
НЕ РОЗКРИВАЙТЕ ЦІ РЕКВІЗИТИ СВОЇХ КАРТОК!
Вам телефонують і під різними приводами випитують дані платіжної картки, банківські sms-паролі або змушують зняти ліміти?
Припиніть розмову, бо втратите гроші!
ШУКАЙ ПРАВИЛЬНО!
kubg.edu.ua
ek.kubg.edu.ua
Захисти свої гроші!
ЗАХИСТИ СВІЙ
ПІН-КОД!



КИЕВСКИЙ УНИВЕРСИТЕТ ИМЕНИ БОРИСА ГРИНЧЕНКО

ШКОЛА КІБЕР БЕЗПЕКИ

Cyber-безпека:
як захистити гроші
на вашій платіжній картці

Автор:

Раїса Федоровська

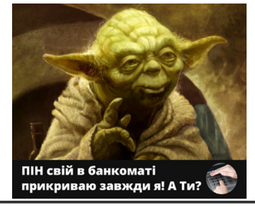
Вступ

Оплата карткою – це безпечно,
але за умови
її належного захисту

Кейс 2. Правила безпечного користування карткою в банкоматах та терміналах самообслуговування

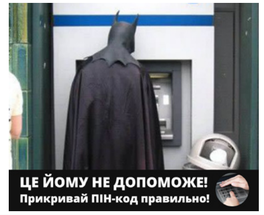
під час введення ПІН-коду:

Прикривайте ПІН-код



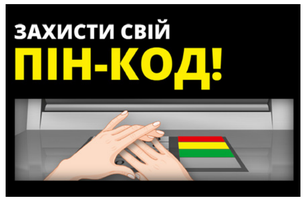
Кейс 2. Правила безпечного користування карткою в банкоматах та терміналах самообслуговування

Прикривайте ПІН-код правильно!



Кейс 2. Правила безпечного користування карткою в банкоматах та терміналах самообслуговування

Прикривайте ПІН-код правильно!



Кейс 2. Правила безпечного користування карткою в банкоматах та терміналах самообслуговування

В разі непередбачуваної ситуації:
банкомат не видав гроші без пояснення причини

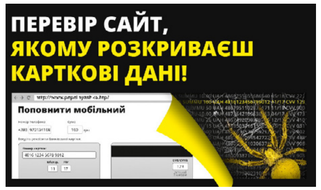
Перевірте отвір для видачі готівки

Кейс 3. Правила безпечного користування карткою в Інтернет

Використовуйте відомі та надійні
платіжні сервіси

Кейс 3. Правила безпечного користування карткою в Інтернет

Перевіряйте репутацію
платіжного сайту



Кейс 4. Правила надання інформації про картку телефоном

Кейс 4. Правила надання інформації про картку телефоном

Зателефонували «з банку», «Податкової», «НБУ»
тощо та запитують карткові реквізити?

Негайно припиніть розмову та самостійно
зателефонуйте до свого банку за номером,
що вказаний на вашій банківській картці

Я вам пізніше
сам зателефоную
за номером, що вказаний
на моїй банківській картці

Кейс 5. Дії у випадку зіткнення із неправомірними діями із платіжною карткою

Послідовність дій у випадку зіткнення
із спробою незаконних дій із картою

1. Заблокувати картку
2. Сповістити банк
3. Звернутися до Кіберполіції

Кейс 5. Дії у випадку зіткнення із неправомірними діями із платіжною карткою

1. Заблокувати картку

зателефонувавши до банку, або самостійно – за допомогою відповідного функціоналу в системі Інтернет-банкінгу

Пересічна жінка з провінції Жи загубила в сумочці свою платіжну картку...
Подумала, що картку поцупив підступний сусід, який приходив відремонтувати кран на кухні.
Вона одразу заблокувала картку через мобільний додаток.
Через місяць ця жінка знайшла свою картку і розблокувала її.
Сусіду вона більше не довіряє.

«ЭКОНОМИЧЕСКИЙ ЭКСПРЕСС»

ЛЕКЦИИ ДЛЯ СТУДЕНТОВ И ПЕДАГОГОВ

ЭКОНОМИЧЕСКИЙ ЭКСПРЕСС | ЛЕКЦИИ ДЛЯ ПЕДАГОГОВ

Раїса Федоровська

ПЛАТІЖНА БЕЗПЕКА
інтенсив

ВАШІ ГРОШІ У БЕЗПЕЦІ?
тест-перевірка

та 13+1 заповідь мудрого параноїка

ВАШ ФІНАНСОВИЙ НОМЕР ТЕЛЕФОНУ

передплачений	контракт
міський номер	я не маю такого номеру

ЗАПОВІДЬ МУДРОГО ПАРАНОЇКА #1:

БЕРЕЖИ ФІНАНСОВИЙ НОМЕР ЗМОЛОДУ

Перейдіть на контрактне обслуговування фінансового номеру

Якщо обрали залишитись на передплаті:

- Ідентифікуйтеся у свого мобільного оператора.
- Зареєструйтесь в персональному кабінеті мобільного оператора.
- Не використовуйте цей номер в оголошеннях та для контактів з контрагентами / клієнтами.

ПІН-КОД ДО ВАШОЇ SIM-КАРТКИ

0000	1111
XXXXXXXX	відсутній

ЗАПОВІДЬ МУДРОГО ПАРАНОЇКА #2:

ВСТАНОВІТЬ ПІН-КОД НА SIM-КАРТКУ

Встановіть 8-значний ПІН-код

Не використовуйте цифри підряд, або дату народження

Запам'ятайте його, а не записуйте

Shanovnyi kliente, vasha kartka zablokovana na 62 dni zgidno z reglamentom banka. Info-centr: +380950870306 www.oshadbank.com

---

ЗАПОВІДЬ МУДРОГО ПАРАНОЇКА #10:

ОКРЕМА КАРТКА ДЛЯ ІНТЕРНЕТ

Для розрахунків в Інтернет використовуйте окрему віртуальну картку

Перед здійсненням покупки перераховуйте на неї необхідну суму з основної картки

ЯК СТВОРИТИ ТА ЗАПАМ'ЯТАТИ СТІЙКИЙ ПАРОЛЬ

«Вареники в сметані»:

- varEniki v smetAni
- varEniki.v.smetAni
- v@rEn1k1.v.smetAn1

«Маруся раз, два, три, калина. Чорнявая дівчина в саду ягоди рвала»:

- V123rxldczh (м123кчдвсяр)
- V123RxLdCZh
- V123RxLdCZh14

ЗАПОВІДЬ МУДРОГО ПАРАНОЇКА #13:

ПРИКРИВАТЕ ПІН-КОД ПРАВИЛЬНО

Прикривайте ПІН-код під час введення так, щоб його неможливо було зчитати за допомогою встановленої поруч мікро-камери

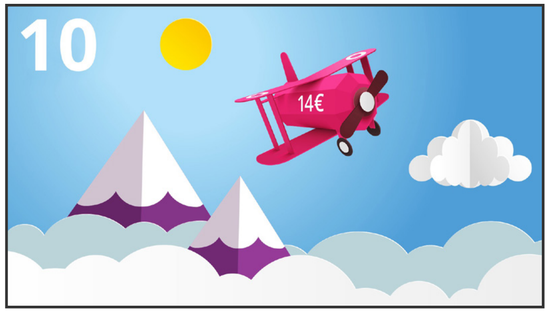
А МОЖНА ПРОДАТИ СВОЮ КАРТУ?

eSл вы Ne naran0їк, to et0 Еще nE ozна4aЄt 4t0 3a v@ми не $ледят!

ЭКОНОМИЧЕСКИЙ ЭКСПРЕСС | ЛЕКЦИИ ДЛЯ СТУДЕНТОВ
ЕМА

ТОП-10 КІБЕРАТАК
НА ГРОМАДЯН УКРАЇНИ

10



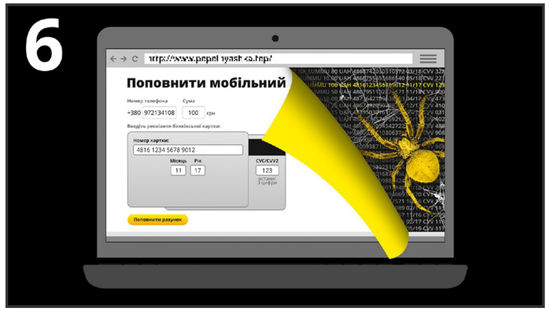
9

EMPLOYMENT FRAUD
Безоплатна праця

8

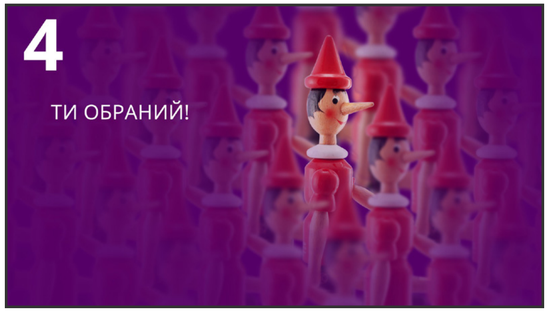
7

6



5

4



3

2

1

Shanovnyi kliente, vasha kartka zablokovana na 62 dni zgidno z reglamentom banka. Info-centr: +380950870306 www.oshadbank.com

С КАЖДЫМ МОЖЕТ СЛУЧИТЬСЯ

14:02	Переказ на картку ПриватБанку через Приват24. Одержувач: П**** Олена Вікторівна. Коментар до платежу: Подзвони в кіберполіцію. Здайся першим. Платник ФЕДОРОВСЬКА РАЇСА	-1.00 грн	1 565.82 грн
13:30	Переказ на картку ПриватБанку через Приват24. Одержувач: П**** Олена Вікторівна. Коментар до платежу: шахраю на цигарки в СІЗО. Платник ФЕДОРОВСЬКА РАЇСА СТАНІСЛАВІВНА	-1.00 грн	1 566.82 грн
12:19	Переказ на картку ПриватБанку через Приват24. Одержувач: П**** Олена Вікторівна. Коментар до платежу: шахраєва ціна. Платник ФЕДОРОВСЬКА РАЇСА СТАНІСЛАВІВНА	-1.00 грн	1 567.82 грн
12:03	Переказ на картку ПриватБанку через Приват24. Одержувач: П**** Олена Вікторівна. Коментар до платежу: отримувач – злочинець. Платник ФЕДОРОВСЬКА РАЇСА СТАНІСЛАВІВНА	-1.00 грн	1 568.82 грн
11:54	Переказ на картку ПриватБанку через Приват24. Одержувач: П**** Олена Вікторівна. Коментар до платежу: премія шахрая. Платник ФЕДОРОВСЬКА РАЇСА СТАНІСЛАВІВНА	-1.00 грн	1 569.82 грн
	Переказ на картку ПриватБанку через Приват24. Одержувач: П**** Олена Вікторівна		

ФИНАНСОВЫЙ SKILLUP. ПОКОЛЕНИЕ БУДУЩЕГО

ШКОЛА ПЛАТЕЖНОЙ ГРАМОТНОСТИ

ВИДЕОРОЛИКИ ДЛЯ ШКОЛЬНИКОВ И СТУДЕНТОВ

mastercard.

mastercard.
EMA

1. Карта первая моя

2. Безопасный платеж

3. Плати в сети

4. NFC. Платить по-новому

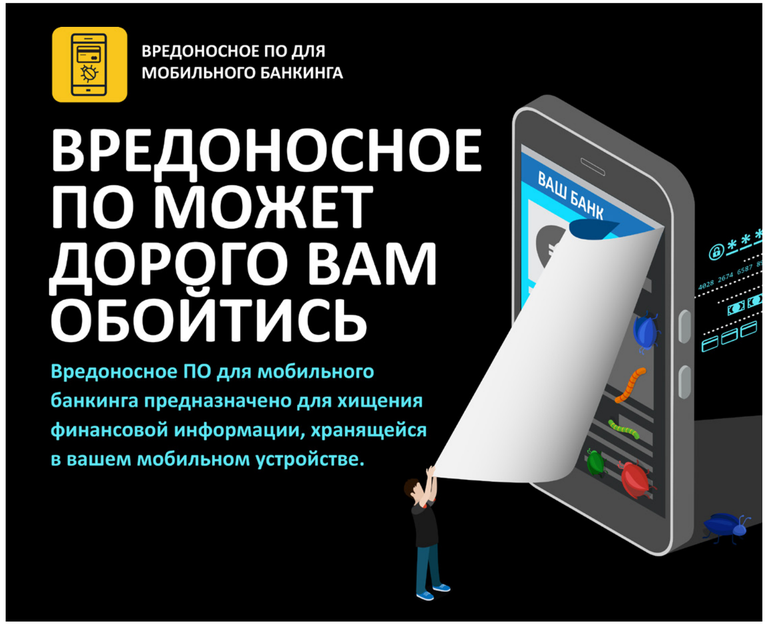
5. Игра и деньги

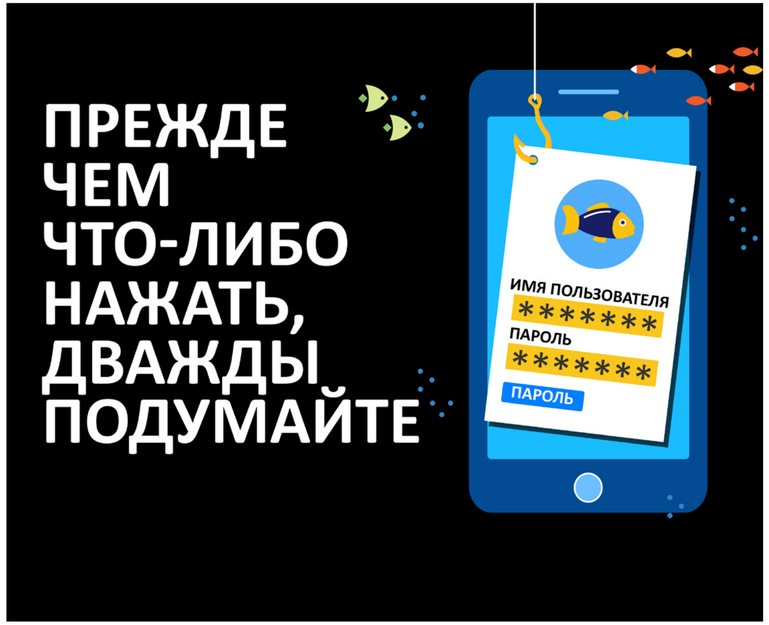
EUROPOL и EBF

ПОДДЕРЖКА ОБРАЗОВАТЕЛЬНЫХ ИНИЦИАТИВ В УКРАИНЕ

ОБРАЗОВАТЕЛЬНАЯ КАМПАНИЯ «ЗАЩИТИ СВОЙ СМАРТФОН!»

октябрь–ноябрь 2016 гг.





20+ банков, 60+ СМИ и Киберполиция поддержали кампанию

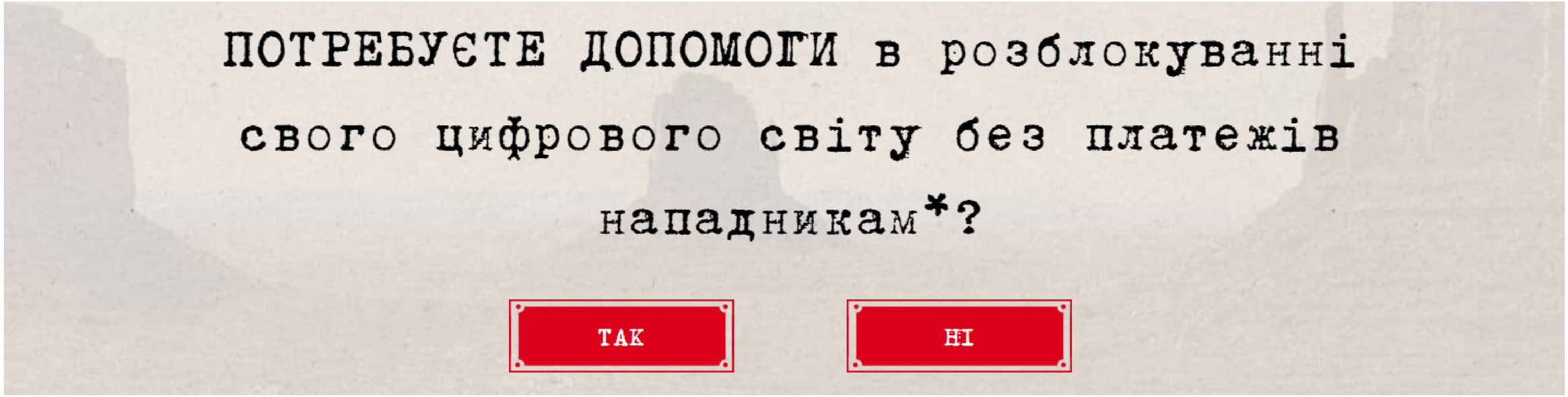
ИНФОРМАЦИОННАЯ КАМПАНИЯ EMMA

«НЕ СТАНОВИСЬ ДРОПОМ!»

2016, 2017 гг.

Более 30+ СМИ и Киберполиция поддержали кампанию

#NOMORERANSOM И #DONTPAY
«НЕТ — ВЫМОГАТЕЛЬСТВУ!»
2016, 2017, 2019 гг.



Более 300 000 посетителей в месяц (2% – из Украины)

FRAUD SCAMS TARGETING EMPLOYEES, 2018

«МОШЕННИЧЕСКИЕ АТАКИ НА ПЕРСОНАЛ КОМПАНИИ»

ШАХРАЙСЬКІ АТАКИ, МІШЕНЬЮ ЯКИХ Є ПЕРСОНАЛ КОМПАНІЇ ЯК СЕБЕ ЗАХИСТИТИ

МІШЕНЬ
Менеджери та фахівці середньої ланки в сфері надання фінансових послуг та матеріально-технічного забезпечення

ВИСОКА ПРИВАБЛИВІСТЬ ЗЛОЧИНУ
Великі прибутки та невеликий ризик бути викритим

Суттєві фінансові наслідки для компаній, що стали об'єктом атаки
ВТРАТИ У РОЗМІРІ МІЛЬЙОНІВ ЄВРО

КАДРОВІ ВТРАТИ
Ганьба, покарання, втрата роботи

ДІЗНАЙТЕСЬ ПРО АКТУАЛЬНІ СХЕМИ ШАХРАЙСТВА

EUROPOL
EMA

ПІД ВИГЛЯДОМ КЕРІВНИКА

КРОК 1
Шахрай телефонує співробітнику, видаючи себе за керівника вищої ланки (напр., керівника або фінансового директора компанії)

КРОК 2
Вимагає здійснити негайний грошовий переказ, наголошуючи на необхідності збереження конфіденційності

КРОК 3
Вимагає здійснити наступний платіж за новими реквізитами

КРОК 4
Співробітник переказує кошти на рахунок, який знаходиться під контролем шахрая. Після того гроші переказуються на інші рахунки, що відкриті закордоном

КРОК 5
Пояснює, як діяти за вказівками,

КРОК 6

ЯК ШАХРАЇ ПРИХОВУЮТЬ ІНФОРМАЦІЮ ПРО СЕБЕ ТА СВОЄ МІСЦЕЗНАХОДЖЕННЯ?

- Використовують підроблені документи, які містять логотип / підписи керівників компанії, зображення яких було знайдено в Інтернет

ПІД ВИГЛЯДОМ ЗЛАМУ СИСТЕМИ

КРОК 1
Шахрай телефонує співробітнику, видаючи себе за IT-спеціаліста компанії (або банківського працівника)

КРОК 2
Повідомляє про здійснення злому системи компанії (або системи Інтернет-банкінгу)

КРОК 3
ВАРІАНТ 1: Вимагає надати фінансову інформацію під приводом перевірки та/або налаштування програми віддаленого адміністрування

ВАРІАНТ 2: Змушує співробітника зателефонувати до банку. Використовує технологію, що дає змогу залишатися на лінії зв'язку після закінчення телефонної розмови, та підслуховує конфіденційну інформацію, що надається співробітником компанії працівнику банку (номери рахунків, паролі)

КРОК 4
Змушує співробітника не дотримуватися встановленої процедури авторизації

ВАРІАЦІЇ
- Вимагає надати інформацію про клієнтів компанії (напр., відомості про всі несплачені рахунки)
- Використовує отриману інформацію для привласнення коштів клієнтів компанії

КРОК 4
Отримана інформація /доступ використовуються для переказу коштів з рахунку компанії на рахунок шахрая

ВАРІАЦІЇ
- Змушує переказати кошти на інший «безпечний» рахунок
- Співробітник переказує кошти на рахунок, який знаходиться під контролем шахрая. Після того гроші переказуються на інші рахунки, що відкриті закордоном

ПІД ВИГЛЯДОМ ПОСТАЧАЛЬНИКА

КРОК 1
Шахрай звертається до співробітника телефоном або електронною поштою, видаючи себе за одного з постачальників компанії (напр., постачальника сировини або послуг)

КРОК 2
Повідомляє про зміну реквізитів рахунку для перерахування коштів постачальнику за послуги / матеріали

КРОК 3
Вимагає здійснити наступний платіж за новими реквізитами

КРОК 4
Співробітник викриває шахрайство, коли отримує скарги від справжнього постачальника про несплачені рахунки

ВАРІАЦІЇ
- Шахрай звертається до постачальника під виглядом представника іноземної підрядної компанії
- Видає себе за стратегічного партнера або відому комерційну компанію
- Замовляє купівлю великого обсягу товарів з відстроченням сплати
- Постачальник товари відвантажує, але гроші за них не отримує

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

ЗАГРОЗА:
Проникає до корпоративної мережі

Отримує доступ до інформації, що підриває репутацію компанії, про:
- протизаконні банківські перекази
- використання банківського рахунку для фінансових махінацій
- промислове шпигунство

Отримує доступ до інформації партнерів/клієнтів для:
- перепродажу (злочини як Послуга);
- шахрайства з використанням платіжних карток

ОТРИМУЄ ДОСТУП ЗА ДОПОМОГОЮ:
- шкідливих програм, що розсилаються електронною поштою
- завантаження співробітником шкідливої програми
- зламу системи безпеки

ЯК РОЗПІЗНАТИ

EUROPOL
EMA

- Несподіваний дзвінок / електронний лист, в якому запитують фінансову інформацію (номери рахунків, паролі)
- Несподіваний дзвінок / електронний лист, в якому запитують інформацію щодо внутрішніх процедур здійснення платежу або поставок
- Наполегливе вимагання виконати прохання/наказ
- Надзвичайна подія

ПІД ВИГЛЯДОМ КЕРІВНИКА

- Особисте спілкування з керівником вищої ланки, з яким ви зазвичай не підтримуєте взаємні стосунки, діловий або дружній зв'язок
- Незвичайне розпорядження, що суперечить внутрішнім процедурам компанії
- Вимога щодо збереження конфіденційності
- Погрози або непритаманні лестощі / обіцянка відзнаки

ПІД ВИГЛЯДОМ ЗЛАМУ СИСТЕМИ

- Тон мовлення IT-співробітника / співробітника служби безпеки, що має викликати тривогу, занепокоєння
- Вимога завантажити програмне забезпечення з підключенням до зовнішньої мережі (напр., під приводом перевірки та/або налаштування програми віддаленого адміністрування)
- Пропозиція переказати кошти на інший «безпечний» рахунок

ПІД ВИГЛЯДОМ ПОСТАЧАЛЬНИКА

- Несподівана зміна контактної інформації / реквізитів рахунку іноземної підрядної компанії (як водиться, про зміну реквізитів рахунку повідомляється заздалегідь, за декілька тижнів / місяців)
- Зміна відбувається невдовзі після отримання великого замовлення або напередодні здійснення оплати

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

- Несподіваний електронний лист зі знеособленим привітанням
- Несподіваний електронний лист, що містить підозрілі гіперпосилання / URL-адреси

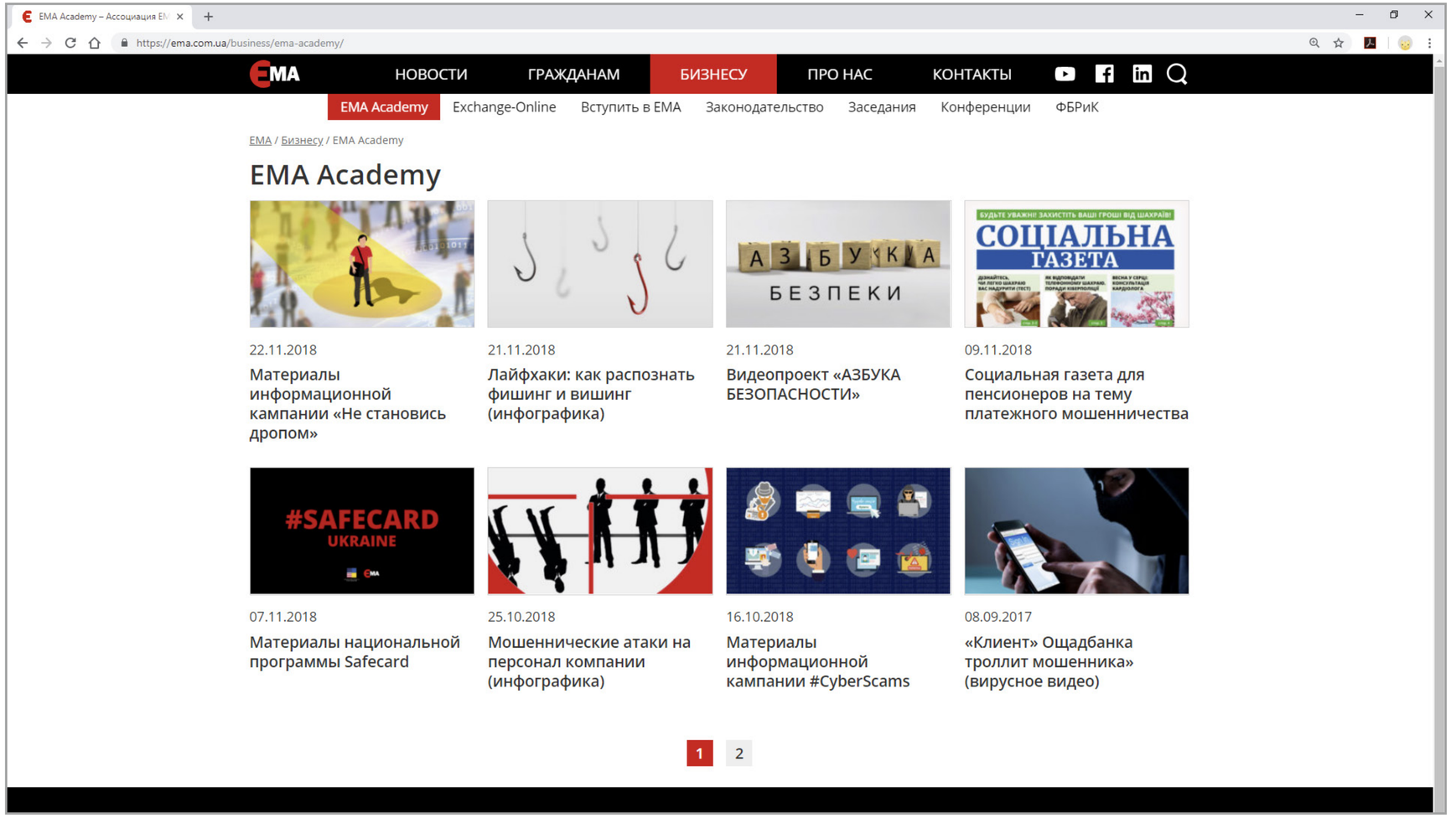
ЯК ДІЯТИ

EUROPOL

#CYBERSCAMS, 2018

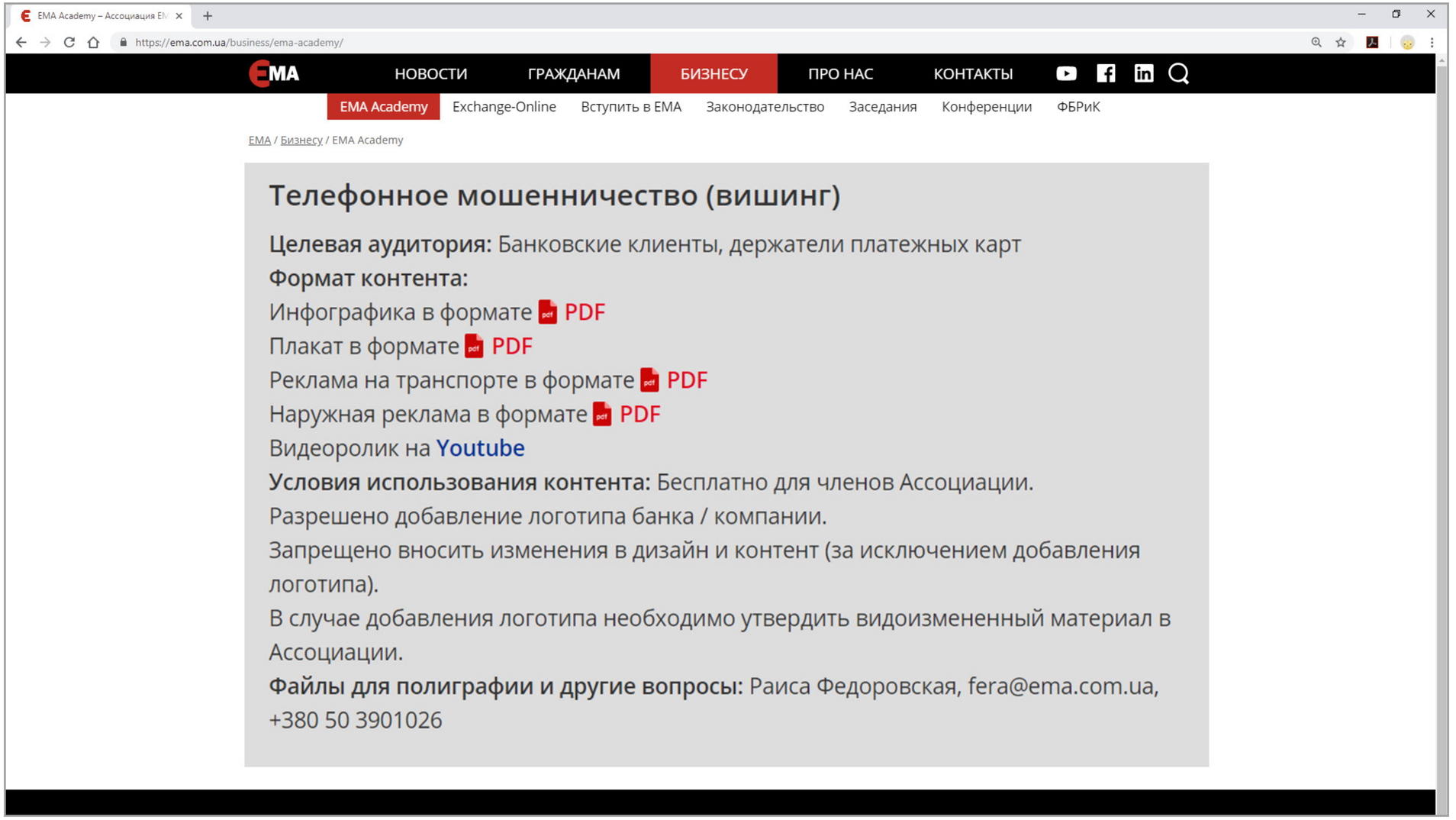
10+ банков, Киберполиция, Платежные сервисы, Новая Почта, 10+ СМИ

#CYBERSCAMS / МАТЕРИАЛЫ ДЛЯ ЧЛЕНОВ АССОЦИАЦИИ



https://ema.com.ua/business/ema-academy/

#CYBERSCAMS / МАТЕРИАЛЫ / УСЛОВИЯ ИСПОЛЬЗОВАНИЯ



ИСПОЛЬЗОВАНИЕ МАТЕРИАЛОВ БАНКАМИ

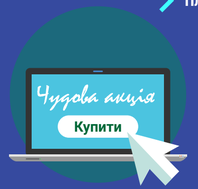
- Публикации в социальных сетях
- Статьи для клиентов на сайте
- E-mail рассылки
- Предоставление материалов ЗКП и Торговцам
- Размещение на интрасайте и дайджестах
- Для тренингов сотрудников ЗКП и Торговцев

ФАЛЬШИВІ ІНТЕРНЕТ-КРАМНИЦІ

Купувати в Інтернеті вигідно, та стережіться шахраїв!

ЯК ДІЯТИ?

- Якщо можна, **купуйте на вітчизняних сайтах** – коли щось піде не так, буде легше врегулювати.
- **Досліджуйте** – читайте відгуки до купівлі товару.
- **Платіть після отримання товару**– замовляйте товари з попереднім внесенням оплати тільки у перевірених та відомих Інтернет-магазинів.
- **Платіть лише через безпечні платіжні сервіси**. Просять переказати гроші на картку чи мобільний телефон? Пильнуйте!
- Платіть лише за наявності **захищеного доступу в Інтернет** – аж ніяк не через відкритий wifi.
- **Платіть лише з захищених пристроїв** – вчасно оновлюйте ОС і програми захисту.



- Уникайте надто привабливих акцій і чудо-товарів – **коли вам щось здається нереальним, так воно і є!**
- Вискакує оголошення: «Ви виграли»? **Пильнуйте**: виграш – програма-шкідник.
- Товар не доставили? Зв'яжіться з продавцем. Не відповідає? **Заявіть у Кіберполіцію**. Якщо оплатили карткою, **повідомте банк**.

У разі підозри шахрайства неодмінно заявіть у Кіберполіцію, навіть якщо ви особисто не постраждали.

#CyberScams

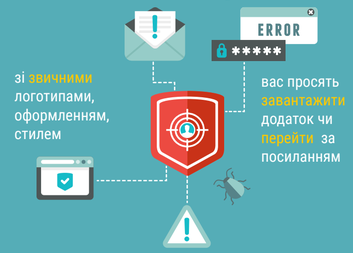
«ЦЕ З БАНКУ»: ФІШИНГ

Фішинг: електронні листи від шахраїв, які хитрощами вивідують особисту, фінансову або конфіденційну інформацію.

ЩО ВІДБУВАЄТЬСЯ?

Прийшов лист:

на перший погляд схожий на листи, які регулярно надходять із банку



зі звичними логотипами, оформленням, стилем

вас просять завантажити додаток чи перейти за посиланням

формулювання свідчать, що справа нагальна

ЯК ДІЯТИ?

- **Оновлювати програмне забезпечення**, зокрема, браузер, антивірус, операційну систему.
- Особливо **пильнувати**, якщо «з банку» вимагають таємну інформацію (скажімо, ваш пароль до системи «Клієнт-Банк»).
- **Ретельно вивчити лист**: порівняти адресу з попередніми справжніми листами з банку. Зважати на помилки в правописі.
- **Не відповідати на підозрілі листи**, натомість пересилати їх у банк, вводячи його адресу вручну.
- **В жодному разі не тиснути на посиланнях та не завантажувати додатки** – вводити адреси в браузері вручну.
- У разі сумніву, **перевірити** відомості на сайті або зателефонувати в банк.

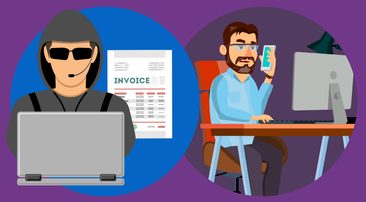
Кіберзлочинці покладаються на зайнятість жертв: на перший погляд фальшиві листи схожі на справжні.

Обережно з мобільними пристроями! Спробу фішингу важче виявити на маленькому екрані телефону та планшеті.

#CyberScams

РАХУНКИ Й ПЛУТНІ

ЩО ВІДБУВАЄТЬСЯ?



- До підприємства звертається нібито представник постачальника товарів/послуг або кредитора.
- Він може зателефонувати, написати листа або звернутися електронною поштою тощо.
- Шахрай наполягає на використанні нових банківських реквізитів (тобто даних одержувача платежу) в майбутніх рахунках-фактурах. Але новий банківський рахунок належить самому шахраю.

ЯК ДІЯТИ?

КЕРІВНИКАМ

Довести до працівників інформацію про цей тип шахрайства та способи протидії.

Наказати відповідальним за оплату рахунків **перевіряти їх усі на коректність**.

Упровадити **регламент перевірки** автентичності платіжних вимог.

Перевірити дані, наведені на веб-сайті компанії, зокрема, про угоди й постачальників. Знеохотити підлеглих наводити зайві відомості про компанію в соцмережах.

СПІВРОБІТНИКАМ

Перевіряти всі запити кредиторів, особливо ті, де вимагається в подальших рахунках змінити банківські реквізити.

Для платежів понад встановлений ліміт **впровадити порядок підтвердження** коректності номера рахунку й одержувача (наприклад, через особисту зустріч).

Не брати контактні дані з листів, факсів, електронної пошти з вимогою змін. Користатися даними з

По оплаті рахунку **повідомляти**

I HAVE
A DREAM!

SQUIZZ

#ВІДСІЧШАХРАЯМ

Чорний Білка у кролячій норі

АНТИШАХРАЙСЬКИЙ ОСВІТНІЙ КВІЗ

у трьох частинах

ПРОКАЧАТИ СКІЛИ

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

Допоможіть Білочці!

Наш герой — відомий шоумен Чорний Білка.

Одного разу, під час прогулянки київським парком,
на ранок після зйомок крайньої серії першого сезону телесеріалу «BLACK SQUIRREL»,
він на власні очі побачив, як три різнокольорові кролики, пробігши повз нього,
пірнули у незвичайну кролячу нору під звичайним кущем.

«Здалося», подумав Білка, та все одно вирішив подивитися що всередині і...

будете сміятися, але Льюїс Керол в труні перевернувся,
а Чорний Білка впав на найнижчий поверх Нори, і має тепер якось звідти вибиратися.

Та, щоб повернутися до звичного світу, він мусить дати
правильні відповіді на всі хитрі кролячі запитання.

Кролики — досвідчені жертви шахраїв. Їх стільки разів розводили,
що вони тепер вже дуже розумні і обачні, і розважаються тим,
що діляться своїм неабияким досвідом з іншими.

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

«Вашу картку заблоковано»

Ви отримали смс повідомлення:

«Шановний клієнт, Ваша картка заблокована на 61 день.
Баланс 0.00 грн. Деталі за номером (044) 222-322-232.

ЗРОБІТЬ ЩОСЬ:

- Зламаю картку. У мене їх декілька
- Зателефоную, за номером банку з смс
- Та пішло воно то смс!
- Піду ногами до відділення
- Сам заблокую картку ще раз
- Зателефоную за номером що, на картці
- Встановлю ліміти

1 2 3 4 5

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

«Вашу картку заблоковано»

Ви зателефонували до служби безпеки Банку!

Для авторизації і вирішення вашої проблеми,
назвіть, будь ласка, номер вашої картки!

ВАШІ ДІЇ:

- ➔ Продиктую паспортні дані
- ➔ Продиктую номер картки
- ➔ Що таке номер картки?
- ➔ Спитаю у оператора, де він сидить?
- ➔ У мене 3 картки. Яку назвати?
- ➔ Ой, мабуть я номером помилився!
- ➔ Спитаю оператора: «Де моя картка?»
- ➔ Зламаю картку. У мене їх декілька.

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

«Вашу картку заблоковано»

Оператор: «Назвіть, будь ласка, номер з смс!»

ВАШІ ДІЇ:

➔ Продиктую номер з смс

➔ Не продиктую номер з смс

❶ ❷ ❸ ❹ ❺

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

Щось пішло не так!

Тільки що Ви власноруч відкрили доступ шахраям до вашого рахунку!

Ви припустилися помилки одразу, коли зателефонували за цим, очевидно, підробним смс. Потім, крім номера картки, Ви назвали невідомій людині термін дії картки та код безпеки. Мало того, ви ще і власноруч підтвердили списання всіх ваших грошей на користь шахраїв, назвавши їм секретний банківський смс-пароль.

ОЙ ЛИШЕНЬКО! А ЩО РОБИТИ?

Ніколи не телефонуйте за номерами із подібних смс-повідомлень!

Банки, Поліція, СБУ, Пенсійний фонд та інші подібні організації, ніколи не випитують дані платіжних карток. Таке роблять лише шахраї!

Навіть для отримання будь-якого переказу на вашу картку, достатньо надати відправнику лише її номер!

ЩЕ РАЗ ПРОЙТИ

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

Добре!

Ви були обережні і не піддалися на шахрайську провокацію!

Не розслабляйтеся, це лише початок.
Попереду чимало випробовувань.

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

SQUIZZ

#ВІДСІЧШАХРАЯМ

ВАШ РІВЕНЬ ЗАХИСТУ ЄМА-3

«Антишахрай третього левела»

ПОДІЛИТИСЯ У FACEBOOK

ЗАВАНТАЖИТИ СЕРТИФІКАТ

Украинская межбанковская ассоциация членов платежных систем ЕМА.
2018 © Все права защищены.

THIS ISN'T THE END, MY FRIEND...

Раиса Федоровская
fera@ema.com.ua
+380 50 390 10 26