

#ГУМАННЫЙ ФИШИНГ

Автор: Раиса Федоровская

#MADE.IN.UA

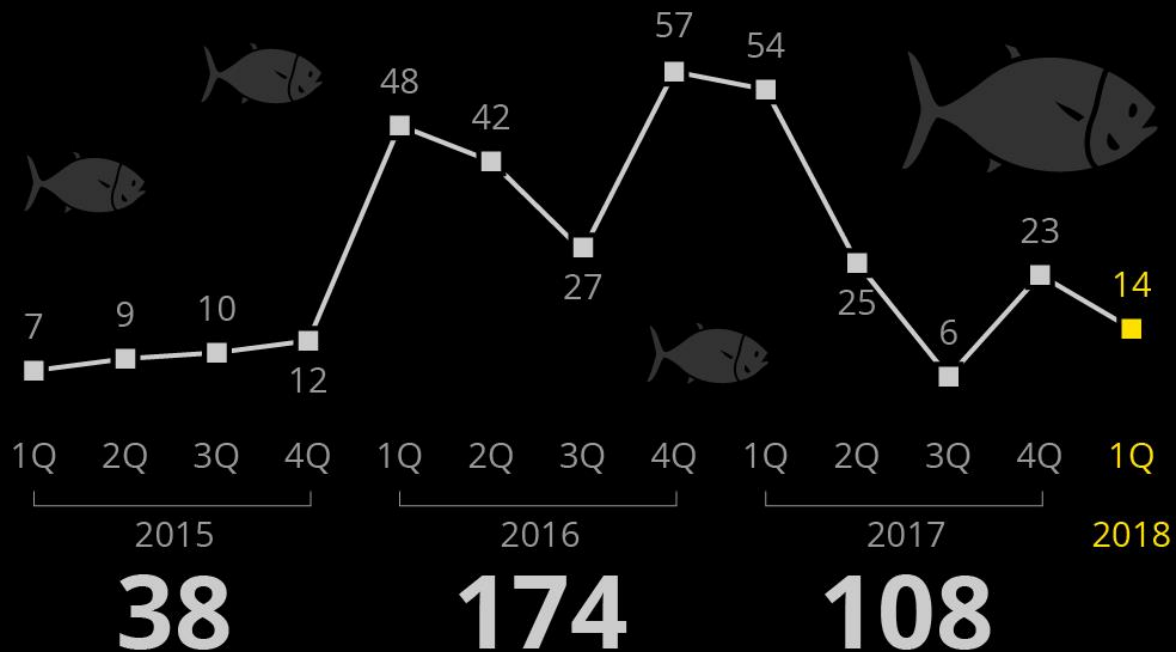
**PHISHING & ANTIPHISHING
HISTORY**

2015 - 2018

14

- 4 — компрометація реквізитів картки
- 4 — підміна номера картки
- 4 — компрометація паролей від інтернет-банкінгу
- 2 — (мобільні застосунки) компрометація реквізитів картки та паролей від інтернет-банкінгу

ФІШИНГОВИХ САЙТІВ



BLOCKED

в 4,5 раза



количество фишсайтов

#SAFECARD

в 3 раза



число людей,
игнорирующих
правило
использования
только известных
платежных сервисов

ГУМАННЫЙ
ЛНИТІФ

каждый 2-й
держатель является
потенциальной
жертвой фишсайта

2015

2016

2017

2018

Образовательный проект

ГУМАННИЙ
ДНІПІФ



WHAT IS IT? AND WHAT FOR?

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 распознаванию фишсайтов

- **ПОПАДЕНИЕ В ЦЕЛЕВУЮ АУДИТОРИЮ**

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

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

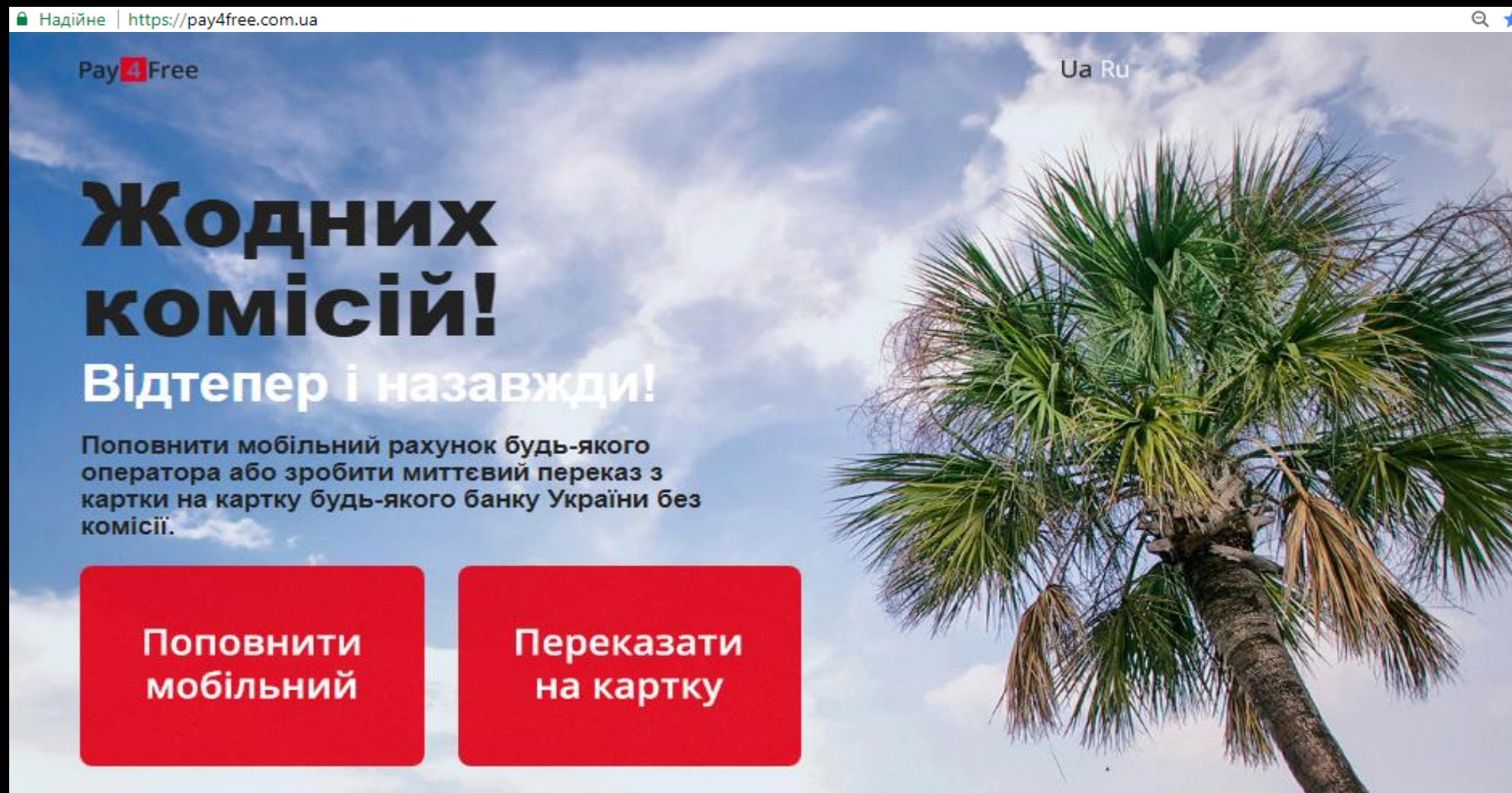
0,69 UAH – стоимость обучения 1 держателя



WWW.PAY4FREE.COM.UA

ЗАПУСК ПРОЕКТА

Зарабатываем не на комиссии, а на доверии людей!



Надійне | <https://pay4free.com.ua> 🔍

Pay4Free Ua Ru

Жодних комісій! Відтепер і назавжди!

Поповнити мобільний рахунок будь-якого оператора або зробити миттєвий переказ з картки на картку будь-якого банку України без комісії.

Поповнити мобільний **Переказати на картку**

Зарабатываем не на комиссии, а на доверии людей!

Надійшло | <https://pay4free.com.ua>

Pay4Free Ua Ru

Жодних комісій!

Відтепер і назавжди!

Поповнити мобільний рахунок Київстар, Vodafone, Life без комісії:

Номер платіжної картки:

Термін дії: CVV2/CVC2:

Номер мобільного:

+380

Сума, грн:

☐ Я приймаю [Умови користування сервісом](#)

ПОПОВНИТИ

Зарабатываем не на комиссии, а на доверии людей!

Надійшло | <https://pay4free.com.ua>

Pay 4 Free Ua Ru

Жодних комісій!

Відтепер і назавжди!

Зробити переказ з картки на картку будь-якого банку України без комісії:

Номер картки відправника:

Термін дії: CVV2/CVC2:

Номер картки одержувача:

Сума, грн:

☐ Я приймаю [Умови користування сервісом](#)

ПЕРЕКАЗАТИ

AFFIRMATIVE

“Hasta la vista, baby”

Pay4Free

Будь ласка, позначте, чи приймаєте ви умови користування нашим сервісом

ОК

Жодних комісій!

Відтепер і назавжди!

Поповнити мобільний рахунок Київстар, Vodafone, Life без комісії:

Номер платіжної картки:

Термін дії:

CVV2/CVC2:

➔

Номер мобільного:

+380

Сума, грн:

☐ Я приймаю [Умови користування сервісом](#)

ПОПОВНИТИ

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

считывает и отправляет длину введенной строки

Пример:

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

СЧАСТЛИВЫЙ ФИНАЛ

Вас приветствует Школа Кибербезопасности

ШКОЛА
КІБЕРБЕЗПЕКИ

Ua Ru

Увага!

Тільки що ви ледь не втратили ваші кошти! Це могло статися тому, що ви власноруч ввели дані вашої платіжної картки на сайті, що не є платіжним сервісом!

Вам пощастило, що ви натрапили саме на наш сайт, а не на шахрайський. Наш сайт створено не для крадіжки карткових даних, а для попередження громадян України про небезпеку фішингових сайтів та запобігання випадкам кібершахрайства.

Ми не отримали та не зберегли жодних введених вами карткових даних. Але існує багато сайтів, що видають себе за платіжні сервіси «на вигідних умовах», та насправді вони крадуть ваші карткові дані, а згодом і гроші з ваших карток!

Захистіться:

- › Перевіряйте репутацію сайту, якому збираєтесь довірити свої карткові дані, перегляньте відгуки про нього в Інтернет. Особливо пильними будьте до інформації з позначкою «Реклама».
- › Перевіряйте вік та термін реєстрації доменного імені на [whois](#) і зверніть увагу на дати "created" та "expires". У шахрайських сайтів зазвичай недавня дата реєстрації та зареєстровані вони лише на 1 рік.
- › Пам'ятайте, 100% надійним сьогодні може бути лише платіжний сервіс, що розташований у зоні .ua. Наприклад: назвасайту.ua. Всі інші доменні зони, зокрема .com.ua, kiev.ua, ip.ua, com тощо — можуть бути зареєстровані будь-ким без жодних обмежень.
- › Перевіряйте платіжні сайти, послугами яких збираєтесь скористатися, на наявність у [Списку шахрайських сайтів](#).
- › Встановіть ліміти на операції в Інтернет за вашою картою.
- › Користуйтеся тільки перевіреними платіжними сервісами:



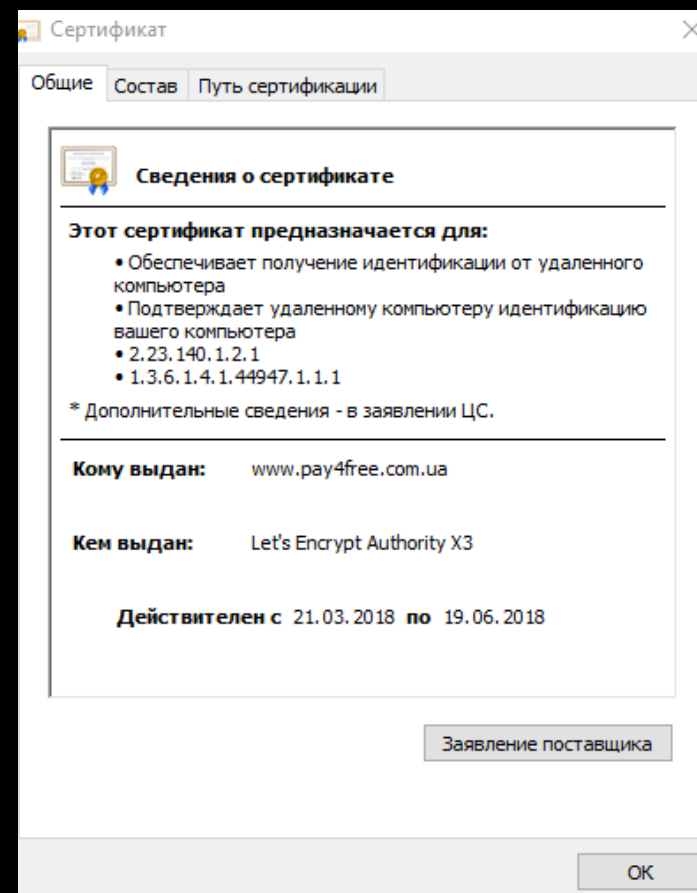
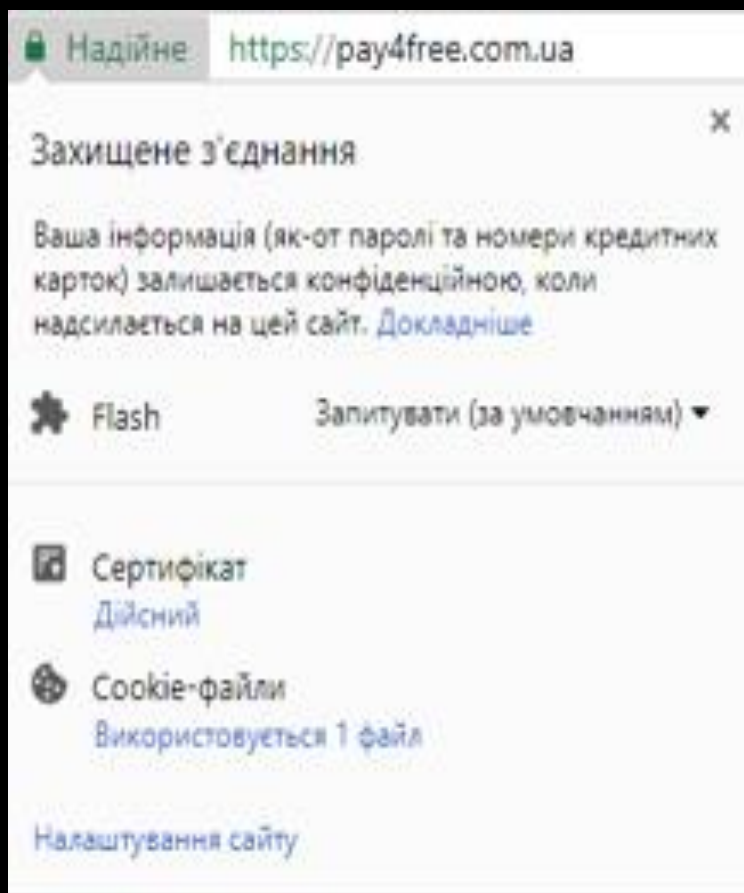
Ваша безпека залежить тільки від вас!

Більше про кіберзахист:



РАДИ ЧИСТОТЫ ЭКСПЕРИМЕНТА

Бесплатный сертификат Let's Encrypt



ЭТО СЛАДКОЕ СЛОВО SEO

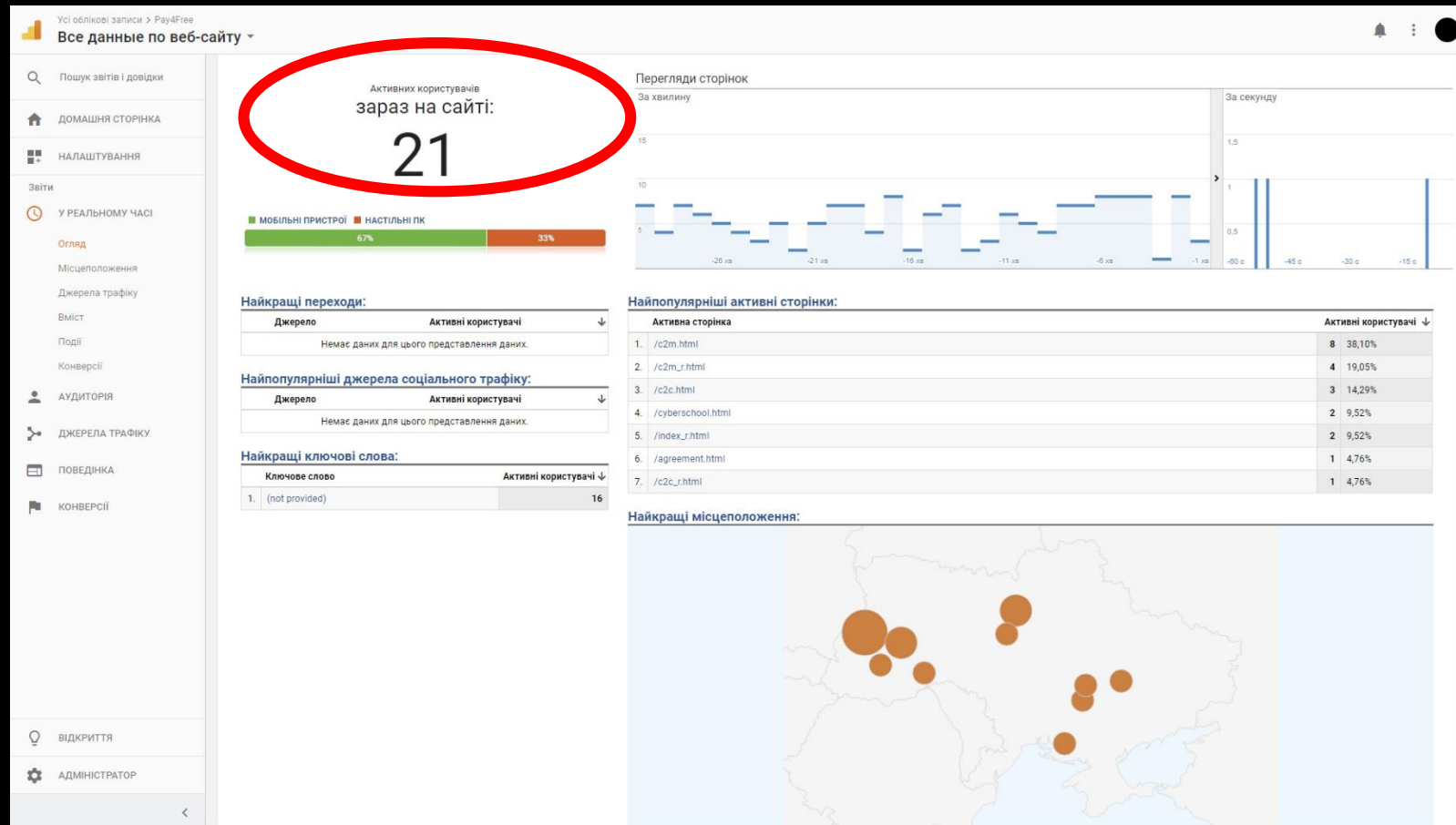
SEO Score

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)

93%

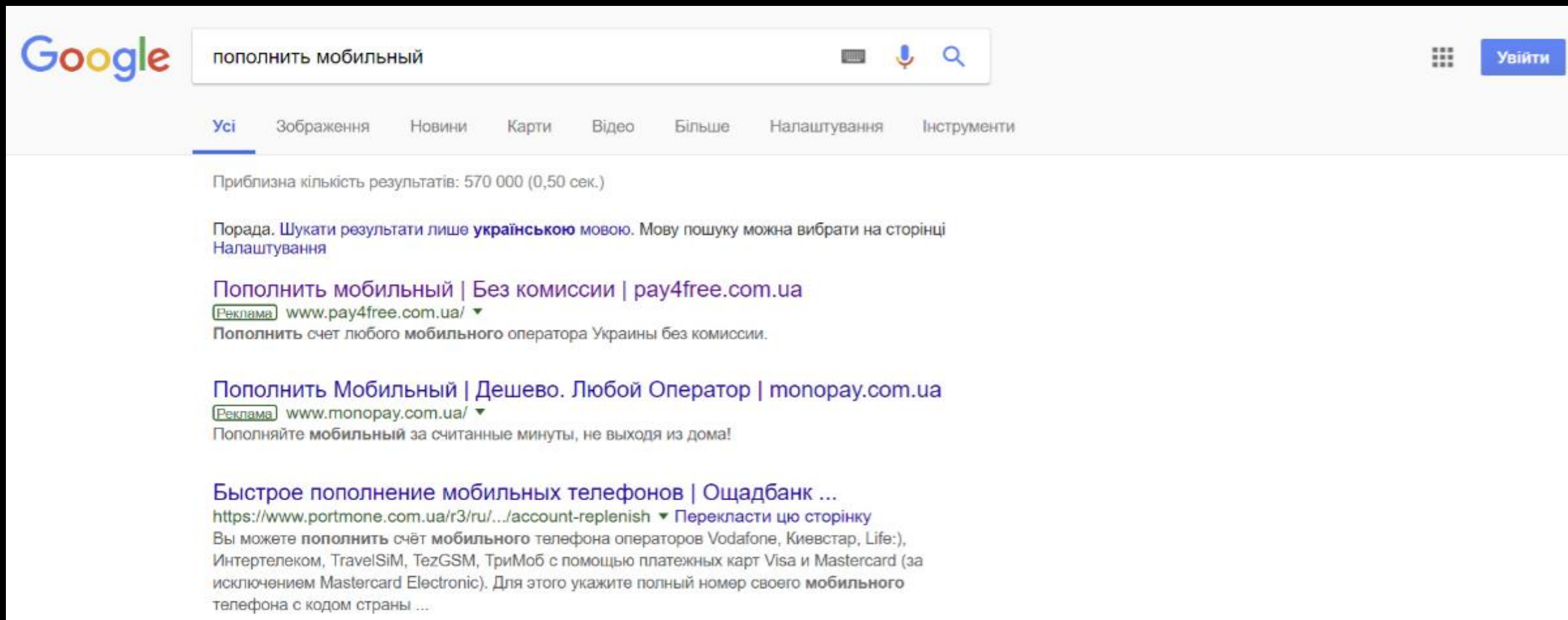
НА СТАРТ, ВНИМАНИЕ, МАРШ!

29 марта 2018 – «ну, понеслась!»



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%
tachcard.com	< 10%
easypay.ua	< 10%
neteller.com	< 10%

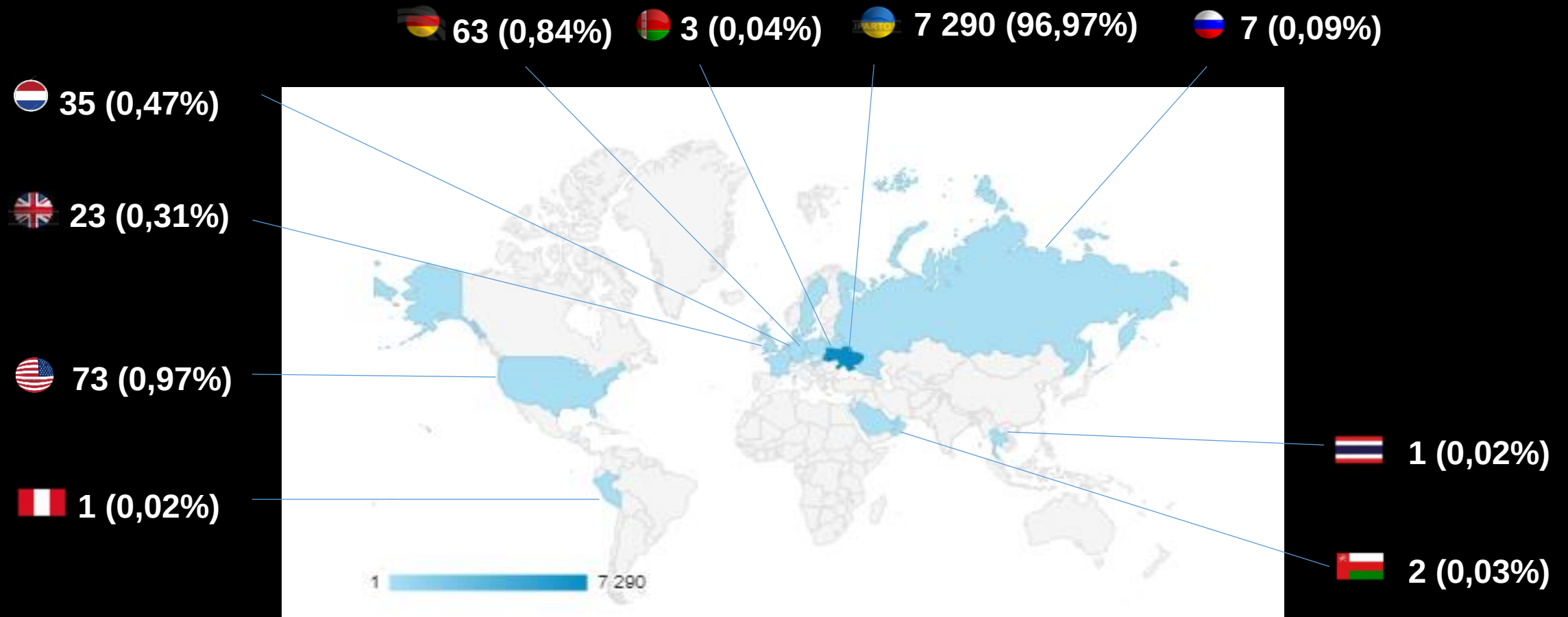


WWW.PAY4FREE.COM.UA

**АУДИТОРИЯ САЙТА и
ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ**

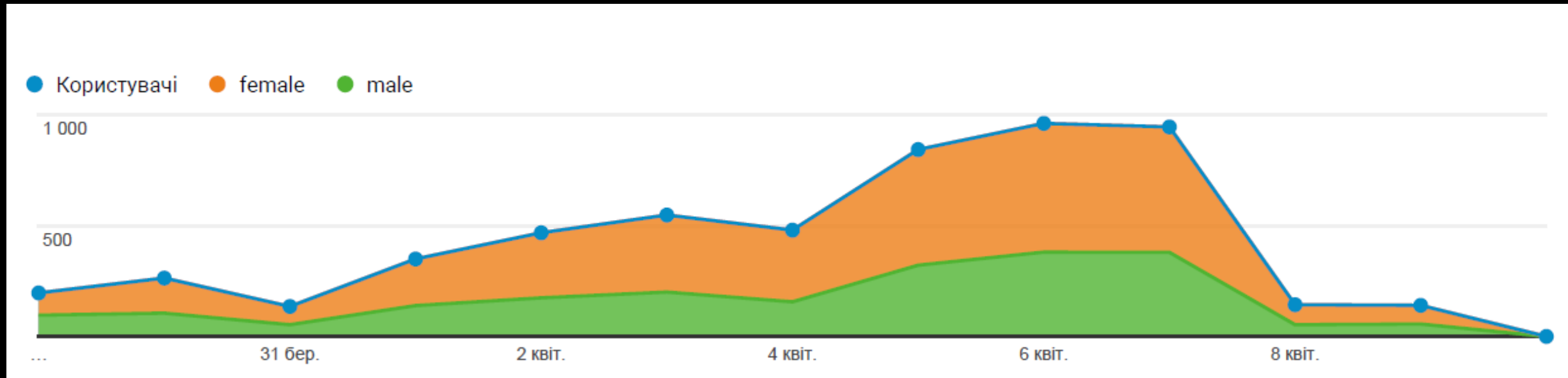
АУДИТОРИЯ САЙТА

Источники трафика



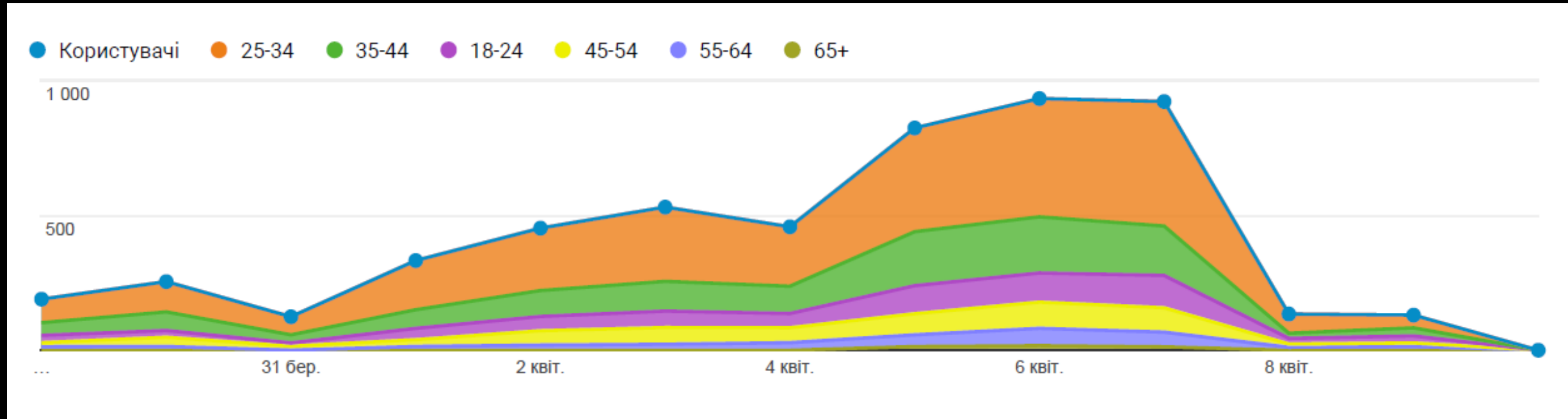
АУДИТОРИЯ САЙТА

Дифференциация по полу



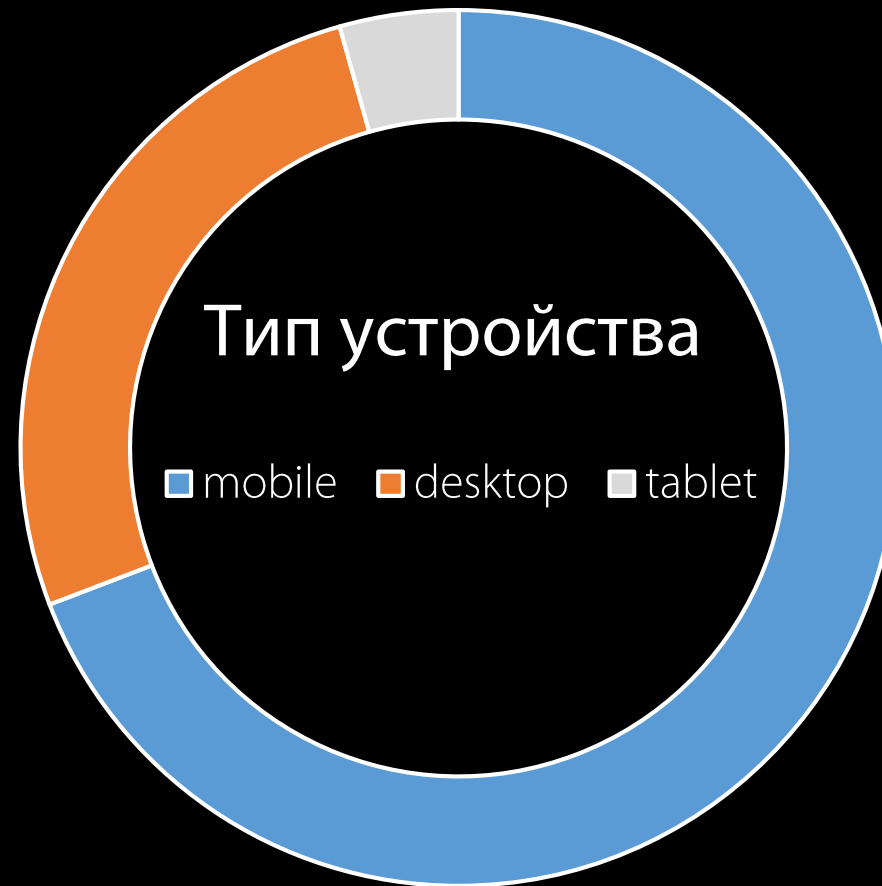
АУДИТОРИЯ САЙТА

Дифференциация по возрасту



АУДИТОРИЯ САЙТА

Дифференциация по типу устройства



АУДИТОРИЯ САЙТА

Дифференциация по операции



ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Возвращение на сайт



ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Средняя длительность сеанса

00:02:20

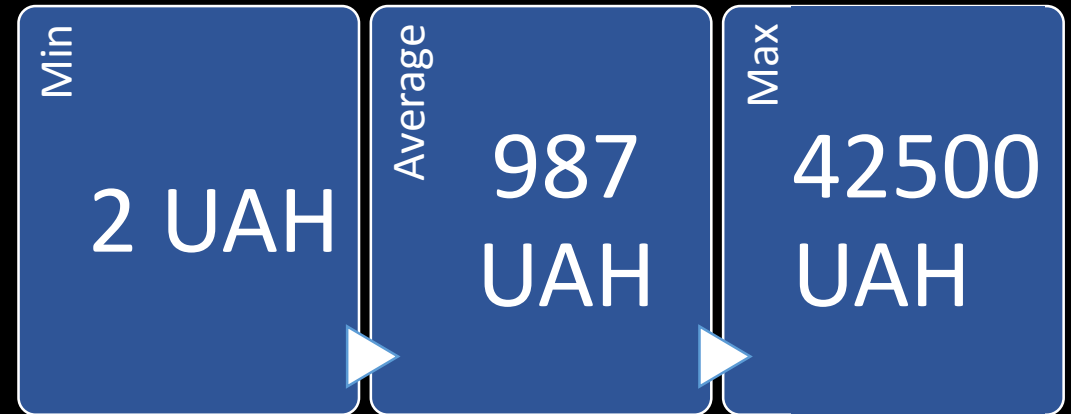
ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Сумма пополнения

C2M



C2C



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%

поставили ✓, не читая
Условия пользования сервисом

ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

«Хотим стать вашим агентом» (с)



БДИТЕЛЬНОСТЬ

сотрудников банков и Киберполиции

Сайт посетили 7 банковских сотрудников и 1 сотрудник Киберполиции

Сообщение #39097 30.03.2018 13:29

Ответить с цитатой Ответить



On Левченков Артем

Организация
Проминвестбанк
Должность
Старший специалист
Телефон: 3646777
Email: fraudmonitoring@pib.ua

Добрый день!

Находился сегодня на просторах интернета и набрёл на такой вот сайт <https://pay4free.com.ua>. Думал, фишинговый и решил протестировать на своей закрытой карте. Ввёл реквизиты, сумму, нажал "перевести" и в итоге моему взору предстал такой вот текст (см. рисунок во вложении).

Удивился и улыбнулся. Приятно видеть такое:)

Школа кібербезпеки ...





WWW.PAY4FREE.COM.UA

**ПОДВЕДЕНИЕ ИТОГОВ и
ОЦЕНКА РЕЗИСТЕНТНОСТИ**

ПОДВЕДЕНИЕ ИТОГОВ

проведения контекстной PPC «рыбалки» в Google

29.03 – 10.04.2018

7516 рыбок
заплыло на псевдо-фишсайт

4172 рыбок
поймано и отпущено после
инструктажа по технике безопасности

ПОДВЕДЕНИЕ ИТОГОВ

А если задуматься?!

4172 держателей

оставили реквизиты карт

на непроверенном веб-сайте

ПОДВЕДЕНИЕ ИТОГОВ

Себестоимость обучения / мошенничества

СРС = 0,69 UAH

ОЦЕНКА РЕЗИСТЕНТНОСТИ К ФИШСАЙТАМ

лат. «resistentia» —сопротивление, противодействие

РЕЗИСТЕНТНОСТЬ К ФИШСАЙТАМ

Сопротивляемость (устойчивость, невосприимчивость, иммунитет) граждан к воздействию фишинговых сайтов вследствие их умения распознать и защититься от мошенничества в Интернет или отсутствия интереса к онлайн-платежам.

Оценка резистентности граждан, воспользовавшихся www.pay4free.com.ua:

- **высокая резистентность** – граждане, не вводившие реквизиты карт
- **низкая резистентность** – граждане, вводившие реквизиты карт

ОЦЕНКА РЕЗИСТЕНТНОСТИ К ФИШСАЙТАМ

Граждане с высокой и низкой резистентностью

44,5 %

Граждане с **высокой**
резистентностью

55,5 %

Граждане с **низкой**
резистентностью

ОЦЕНКА РЕЗИСТЕНТНОСТИ К ФИШСАЙТАМ

Резистентность по регионам

Чернивецкая обл. – 40 %
Херсонская обл. – 40,8 %
Закарпатская обл. – 42,5 %
Ив.-Франковская обл. – 43,1 %
Одесская обл. – 44 %
Тернопольская обл. – 44,9 %

Днепропетровская обл. – 54,8 %
Сумская обл. – 54,4 %
Кировоградская обл. – 53,9 %
Житомирская обл. – 52,6 %
Черкасская обл. – 50 %
Ровенская обл. – 49,3 %
Харьковская обл. – 49,2 %
Волинская обл. – 48,8 %
Киевская обл. – 46,9 %
Полтавская обл. – 46,9 %
г. Киев – 46,2 %
Запорожская обл. – 46,1 %
Львовская обл. – 45,7 %
Винницкая обл. – 45,5 %

Николавская обл. – 58,9 %
Хмельницкая обл. – 58,1 %
Черниговская обл. – 56,8 %

Резистентность $\leq$ 45%

Резистентность = 45-55%

Резистентность $\geq$ 55%

ГРАЖДАНЕ С НИЗКОЙ РЕЗИСТЕНТНОСТЬЮ

Дифференциация по полу

40 %

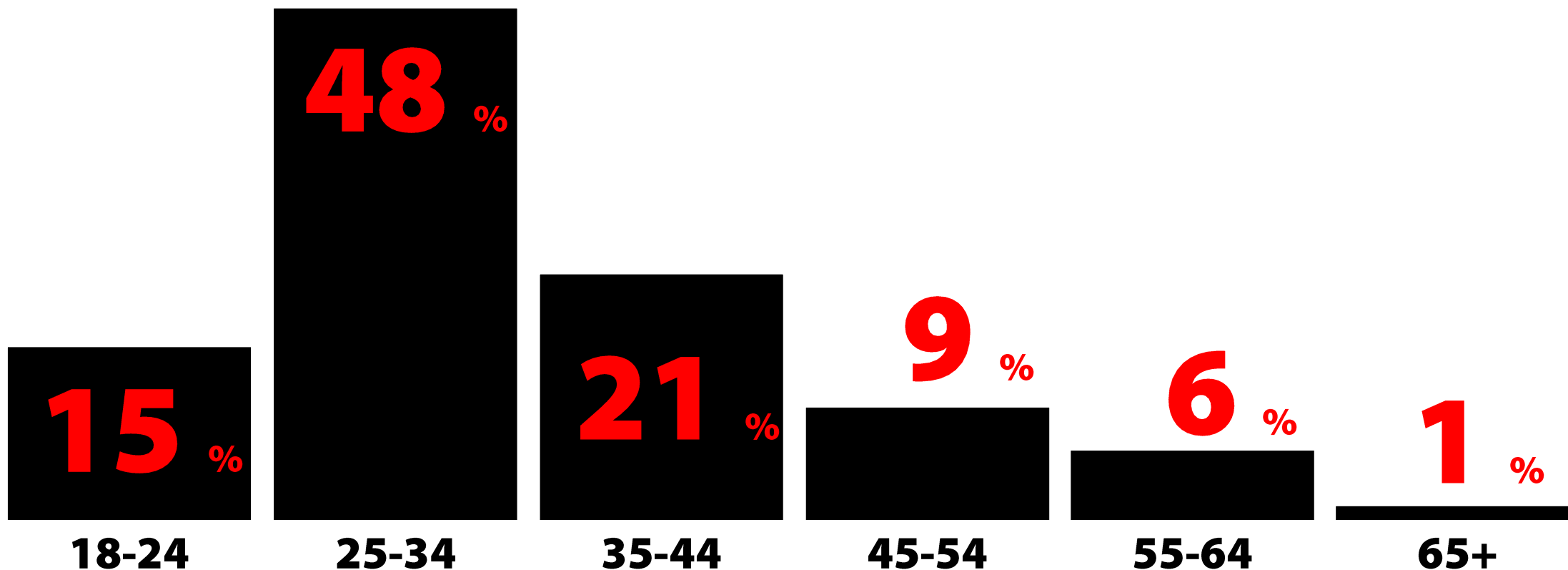
Мужчины

60 %

Женщины

ГРАЖДАНЕ С НИЗКОЙ РЕЗИСТЕНТНОСТЬЮ

Дифференциация по возрастным категориям



ВЫВОДЫ

Учиться, учиться и еще раз учиться! (с)

Больше половины украинцев
демонстрируют рискованное
поведение в Интернет и
нуждаются в продолжении
КиберЛикБеза



ВЫВОДЫ

Планы ШКБ

- Гуманный фишинг
- Гуманный смифинг
- Гуманный кеш-треппинг
- Гуманный скимминг
- Зачеты по кибербезопасности

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

