средняя и старшая школа

Цифровой ликбез

Ситуация 1

В игровом аккаунте ученик переводил деньги на свой счёт для покупки улучшения для своего героя.

В один день он не смог зайти в свой аккаунт, и деньги со счёта пропали.

Ситуация 2

В социальных сетях от вашего аккаунта всем приходит сообщение с просьбой перевести вам деньги на определённый номер.

Хотя вы этого не делали.

Сегодня поговорим
о такой важной теме

Способы защиты профиля в сети Интернет

Кибер-мошенничество

Это различные способы мошеннических действий, осуществляемых киберпреступниками в интернете.

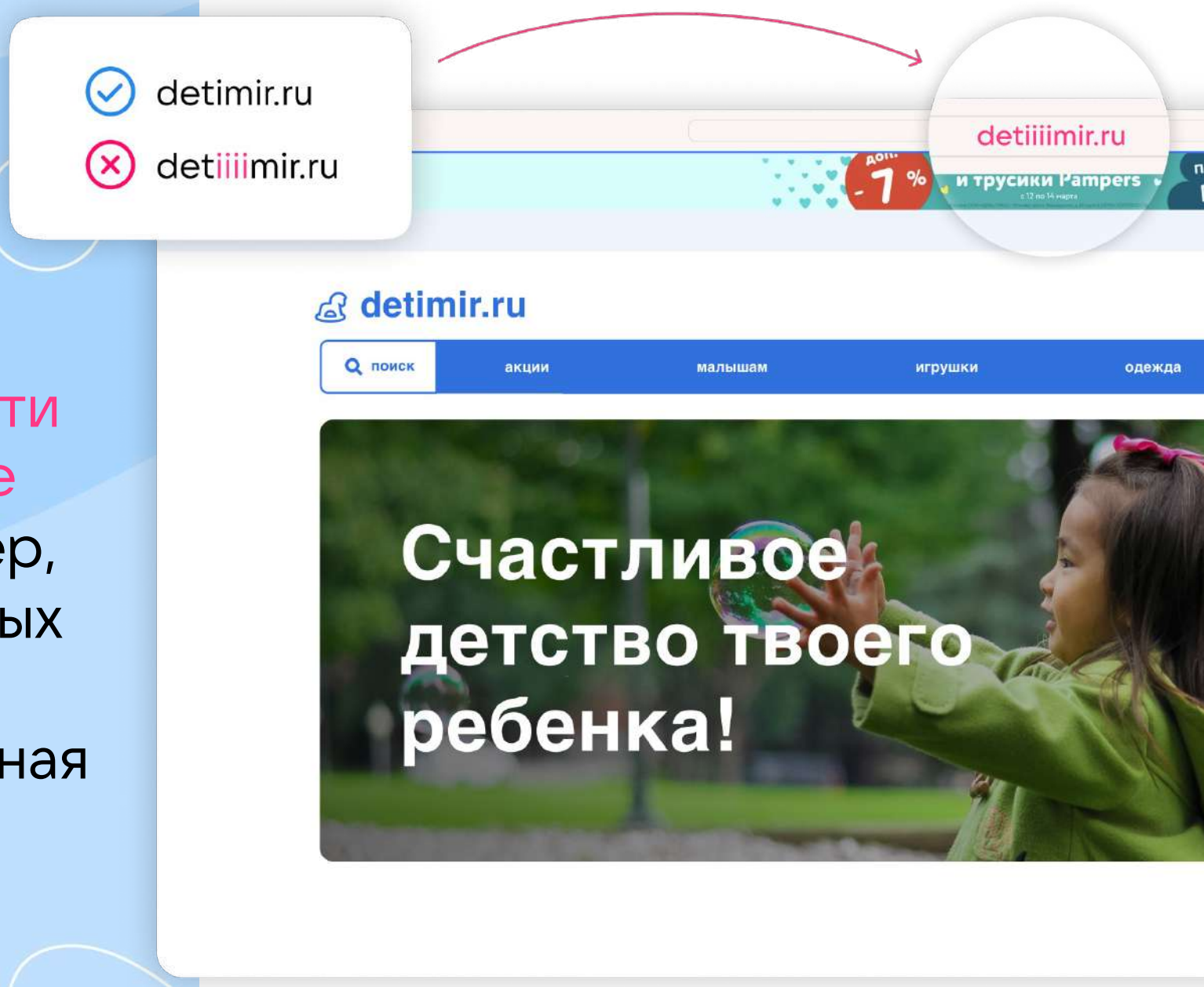
Что могут украсть

- логин и пароль от почты
- данные карточки
- данные профиля социальных сетей
- код из SMS
- ПИН-код
- деньги

Фишинг

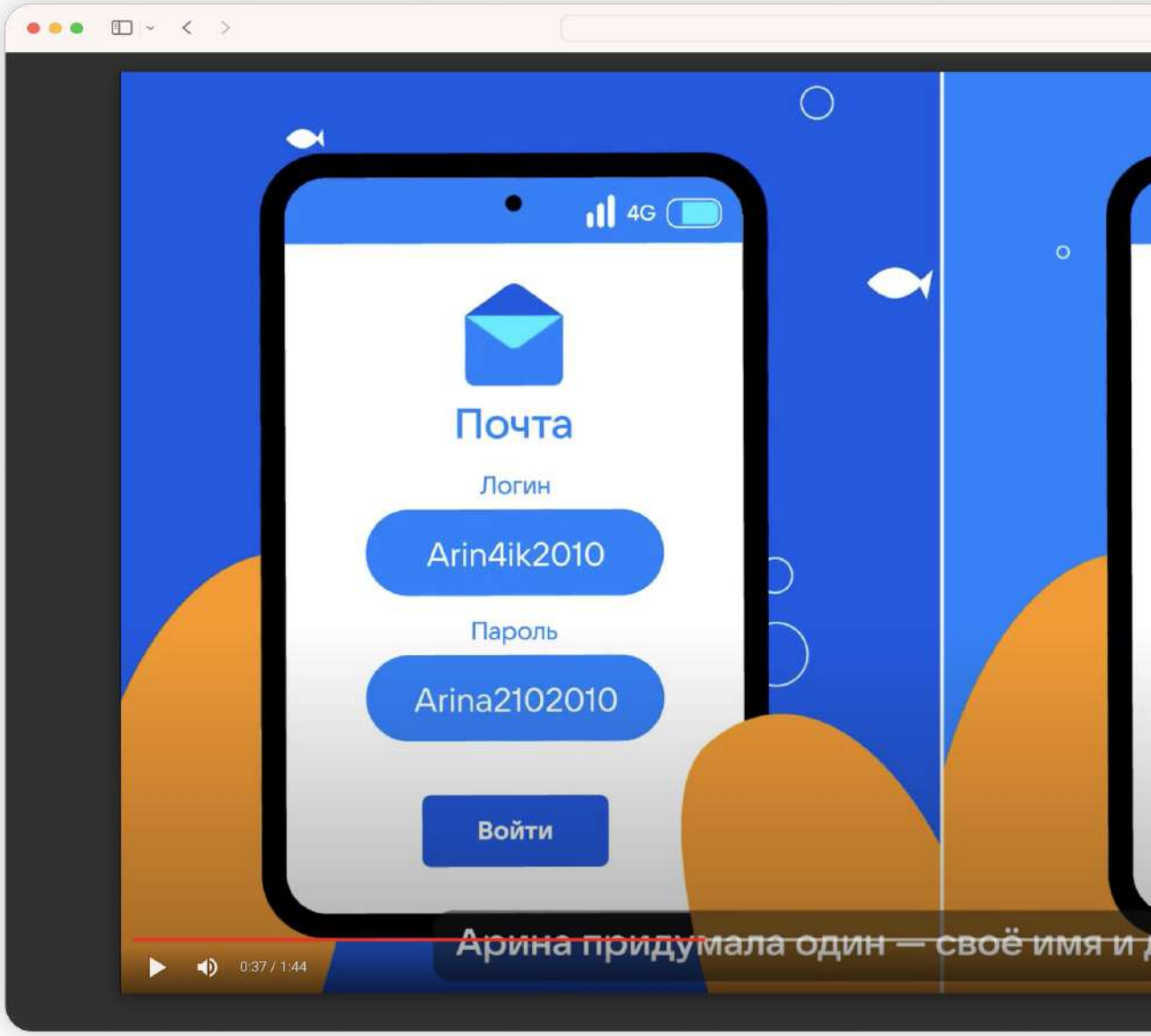
(англ. phishing, от fishing — «рыбная ловля», «выуживание»)

Вид мошенничества в сети с целью получить данные пользователей. Например, пароли, номера кредитных карт, банковские счета и другая конфиденциальная информация.



А что делать, чтобы не украли пароль?

Придумайте три вопроса
по сюжету видеоролика
и запишите их в рабочий лист.



Как работают кибермошенники и на что нужно обращать внимание

Брутфорс — метод подбора паролей.

- Перебор символов.
- Парольные словари и их модификации.
- Слитые базы.

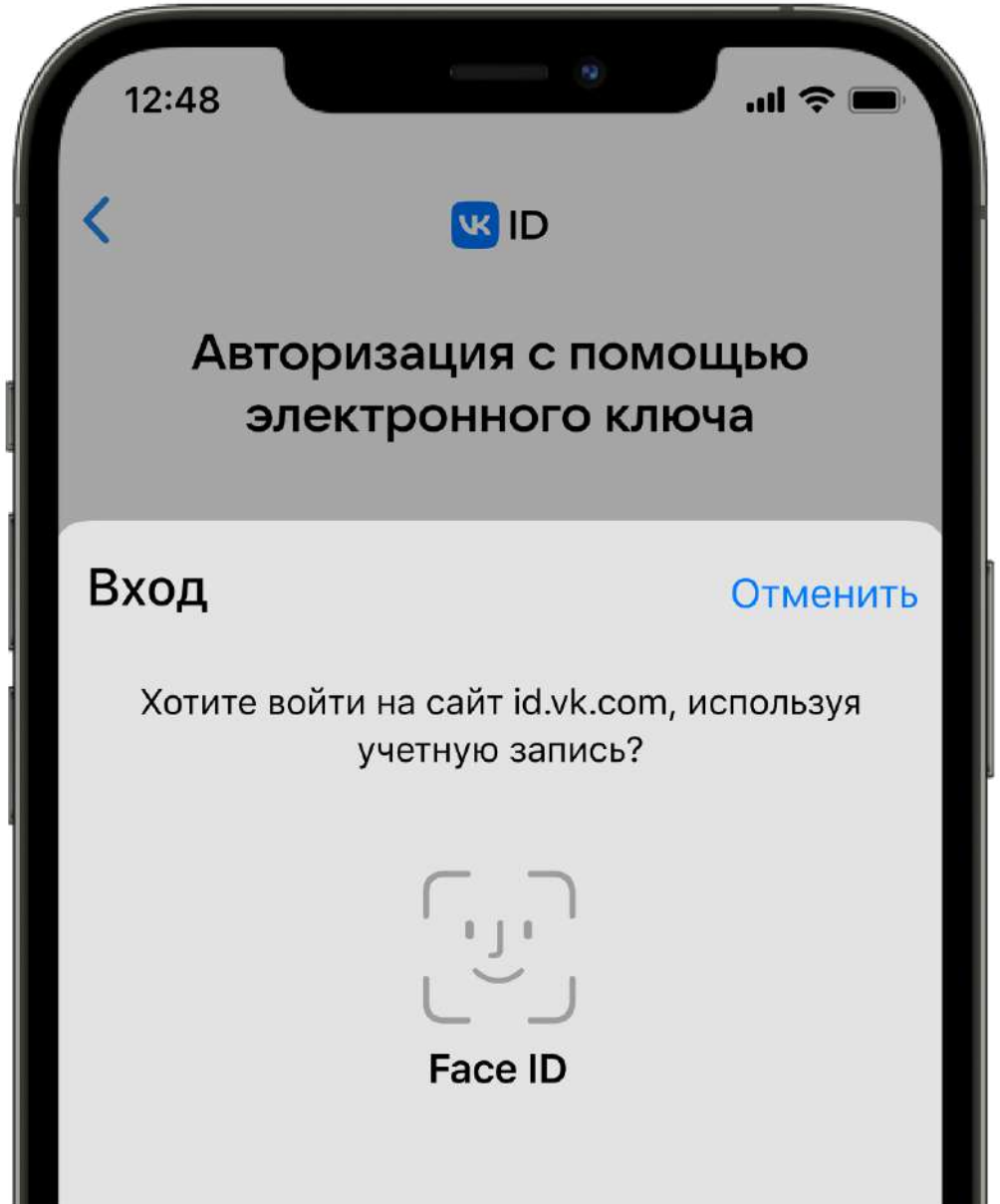
Топ самых распространённых паролей в России

password	12345678	наташа
123456	123456789	марина
111111	12345	максим
1q2w3e	qwerty123	кристина
qwerty	123123	андрей
йцукен	пароль	люблю
любовь	привет	

*По данным NordPass, 2022

Безопасный вход — беспарольный вход

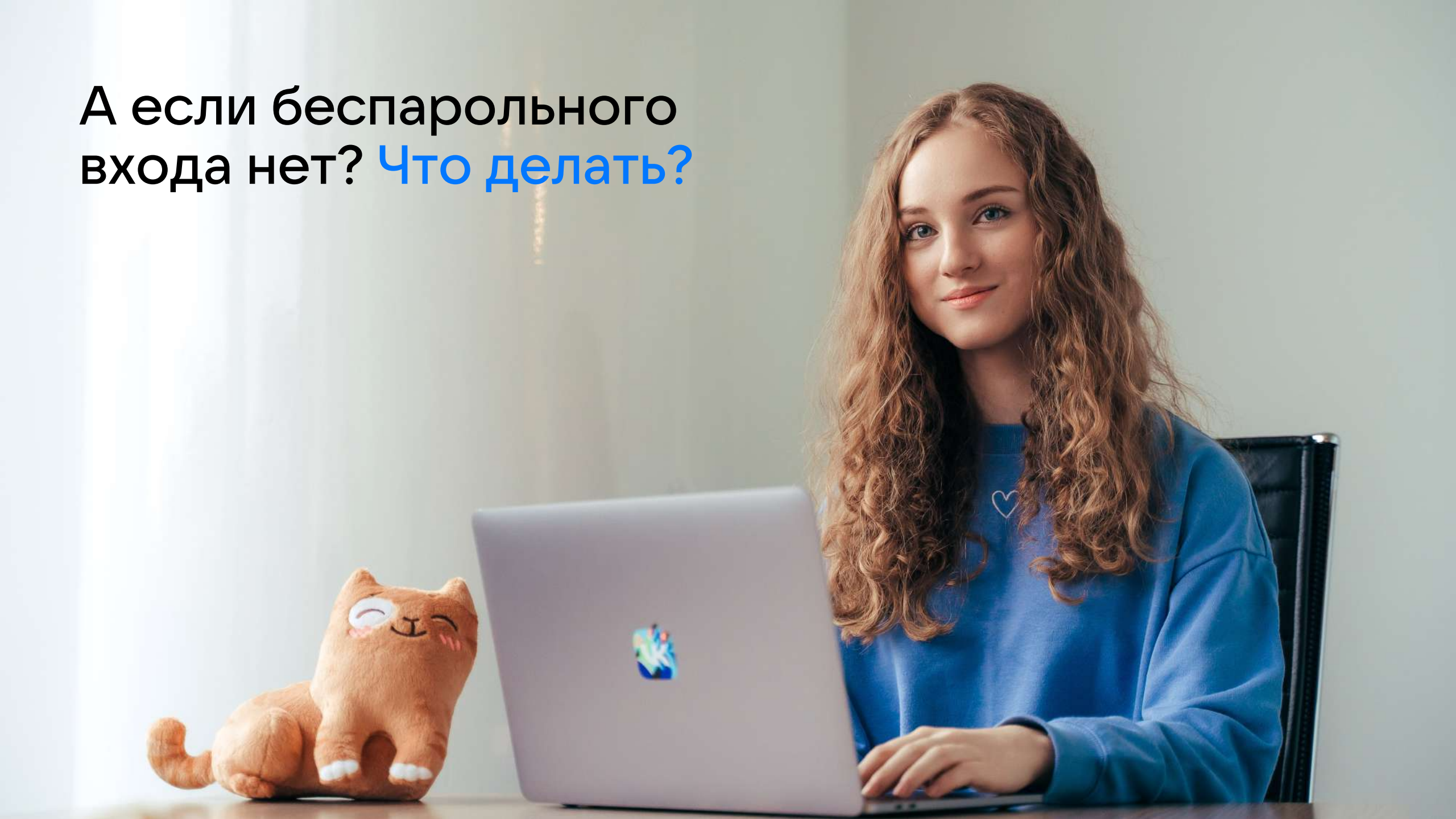
- по лицу
- SMS
- QR-коду
- push-уведомлению
- отпечатку пальца



Как настроить беспарольный вход

Если нет, включите
двухфакторную аутентификацию.

А если беспарольного входа нет? Что делать?



Сколько времени займёт у хакера взлом паролей методом перебора

Кол-во символов	Только числа	Буквы в нижнем регистре	Буквы в нижнем и верхнем регистре	Числа и буквы в нижнем и верхнем регистре	Числа и буквы в нижнем и верхнем регистре, символы
6	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
7	мгновенно	мгновенно	2 сек.	7 сек.	31 сек.
8	мгновенно	мгновенно	2 мин.	7 мин.	39 мин.
9	мгновенно	10 сек.	1 час	7 часов	2 дня
10	мгновенно	4 мин.	3 дня	3 недели	5 месяцев
11	мгновенно	2 часа	5 мес.	3 года	34 года
12	2 сек.	2 дня	24 года	200 лет	3 тыс. лет

Критерии надёжного пароля

1

Длина пароля — 10 символов и более

2

Не должен содержать обще-доступную информацию о вас (имя, фамилия, дата рождения)

3

В пароле нет простых последовательностей символов вроде 12345, 987, qwerty или password

4

В пароле есть и прописные, и строчные буквы

5

Пароль используется только для одного аккаунта

6

В пароле присутствуют специальные символы: (пробел) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ { | } ~

Как придумать сложный пароль?

Правило

- Взять за основу стихотворение, фразу или событие из вашей жизни + добавить цифры.
- Заменить пару букв на спецзнаки.

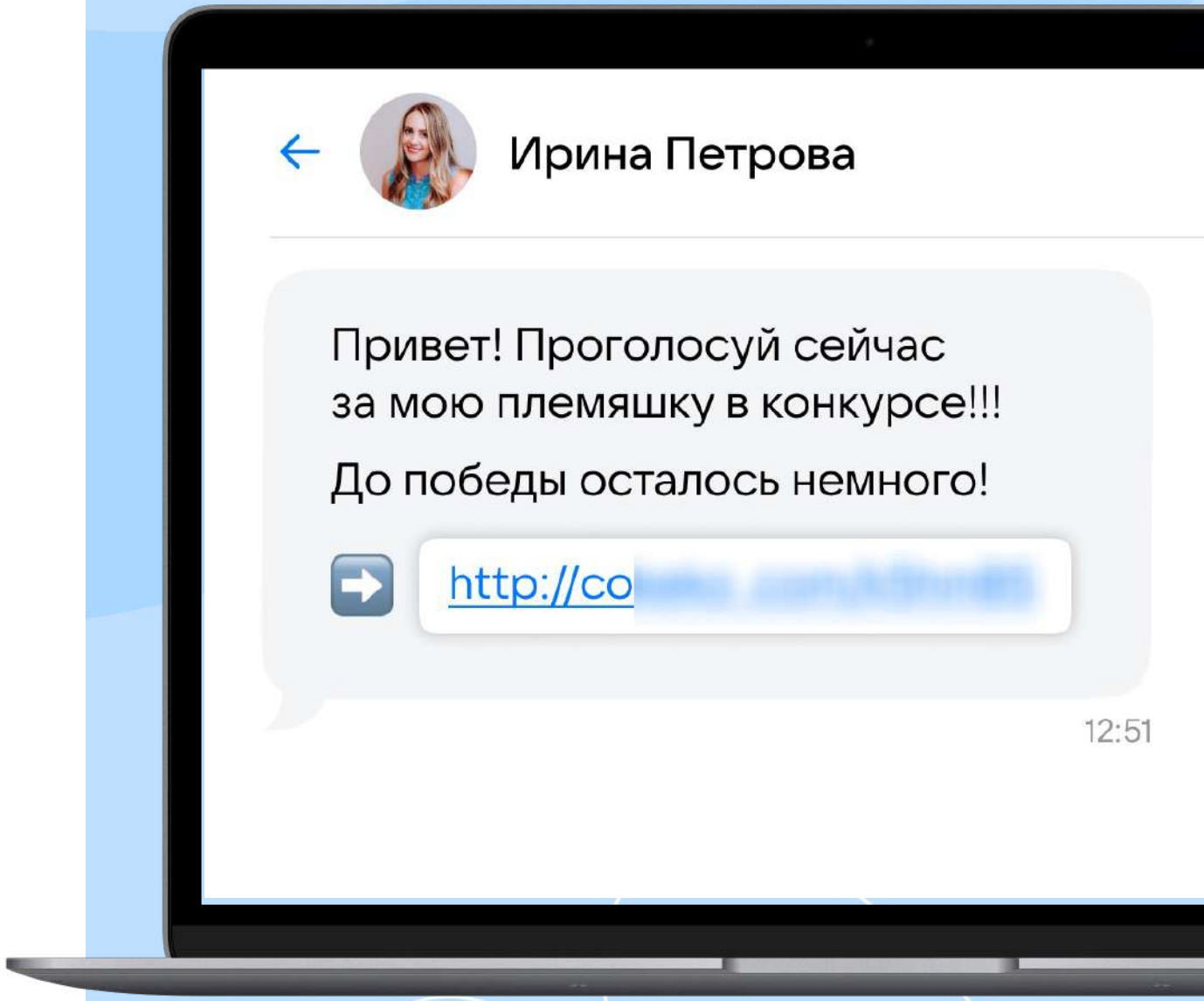
Двухфакторная аутентификация

Это дополнительная защита ваших данных, основанная на двух факторах:

- одним вы подтверждаете владение устройством, через которое происходит вход в аккаунт (телефон, на который приходит SMS с кодом, push, QR-код);
- другим подтверждаете «знание» (пароль), на основе которого входите в аккаунт.

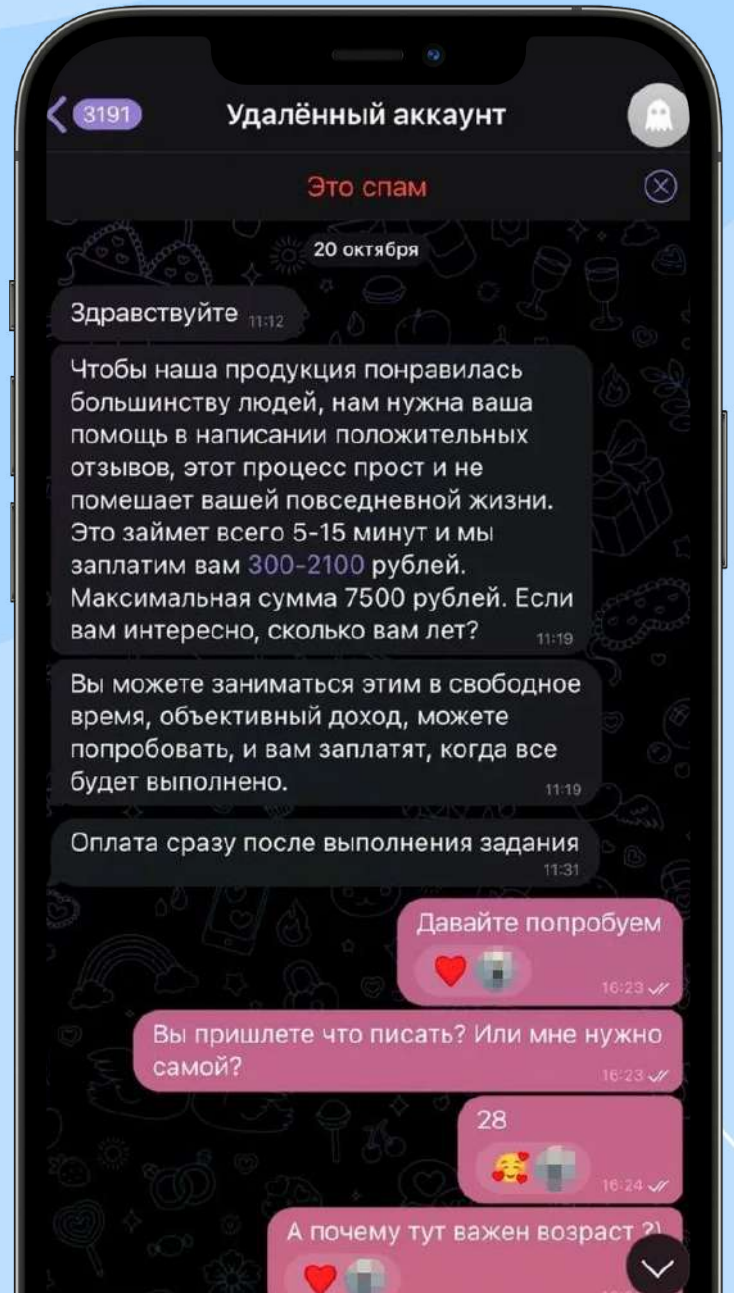
Что не так
с этим письмом?

Если перейти по ссылке
и ввести данные, аккаунт
попадёт к мошенникам.



Маркетплейсы — под прицелом мошенников

За 2023 год заблокировано 11 500 фишинговых ресурсов, которые использовали бренд популярного онлайн-магазина для обмана покупателей и продавцов.



Блог компании F.A.C.C.T. Информационная безопасность*

Социальная инженерия

Вид интернет-мошенничества с использованием умения убеждать и манипулировать людьми для достижения своих целей (получение доступа к конфиденциальным данным пользователей). Это обычно происходит путём обмана людей или манипуляции их чувствами.

Мошенник очень:

- хорошо разбирается в видах психологического воздействия;
- хорошо умеет манипулировать;
- подготовлен;
- хочет получить данные и заработать.

Психологические векторы атак

- Невнимательность
- Любопытство
- Страх
- Жадность
- Раздражение
- Желание помочь
- Авторитет
- Срочность

Способы защиты от кибер-мошенников

1. Беспарольный вход
2. Надёжный пароль
3. Двухфакторная аутентификация
4. Критический подход к любой входящей информации
5. Давать себе время на осмысление
6. Задавать вопросы

КВИЗ

Информационная безопасность

раунд 1

Разминка

- 4 вопросов
- 1 минута
- 4 варианта ответа

Вопросы на абсолютно разные темы — на эрудицию, логику и удачу.

Вопросы не повторяются.

За правильный ответ — 1 балл.

вопрос 1

Когда говорят «ресурс недоступен», иногда это значит, что на него была совершена атака.

О каком типе атак идёт речь?

ответ

1 Брутфорс

2 DDos

3 Фишинг

4 Вредоносное ПО

вопрос 2

Иконка какого приложения тут изображена?

ответ

1. VK Звонки
2. VK Почта
3. VK Мессенджер
4. VK Музыка

вопрос 3

Как называется новый способ входа ВКонтакте без пароля?

ответ

1. Алохомора
2. OnePass
3. Безбарьерный вход
4. Двухфакторная аутентификация

вопрос 4

Какой пароль является наиболее надёжным?

ответ

1. Love_1
2. Nataliya_2000
3. ~#0+_aD<Q3%A
4. 87654321234567

раунд 1

Ответы

вопрос 1

Когда говорят «ресурс недоступен», иногда это значит, что на него была совершена атака.

О каком типе атак идёт речь?

ответ

1 Брутфорс

2 DDos

3 Фишинг

4 Вредоносное ПО

вопрос 2

Иконка какого приложения тут изображена?

ответ

1 VK Звонки

2 VK Почта

3 VK Мессенджер

4 VK Музыка

вопрос 3

Как называется новый способ входа ВКонтакте без пароля?

ответ

1 Алохомора

2 OnePass

3 Безбарьерный вход

4 Двухфакторная аутентификация

вопрос 4

Какой пароль является наиболее надёжным?

ответ

1 Love_1

2 Nataliya_2000

3 ~#0+_aD<Q3%A

4 8765432123456

раунд 2

Фишинг — это не рыбалка

- 5 вопросов
- 1 минута
- 4 варианта ответа

За правильный ответ — 1 балл.

Вопросы на тему мошенничества в интернете.

Вопросы не повторяются.

вопрос 1

Мошенники — отличные психологи, они давят на эмоции жертв, чтобы поймать тех на крючок.

Соотнесите тему сообщения и эмоцию.

ответ

А. Страх	1. Смотри, как ты отжигаешь на видео
Б. Желание помочь	2. Ваш компьютер заражён и заблокирован
В. Раздражение	3. Чтобы отписаться, перейдите по ссылке
Г. Любопытство	4. Ваш коллега потерял свои вещи

вопрос 2

Справа перечислены разные типы фишинговых атак. Одно название из списка — выдуманное. Какое?

ответ

1. Вишинг

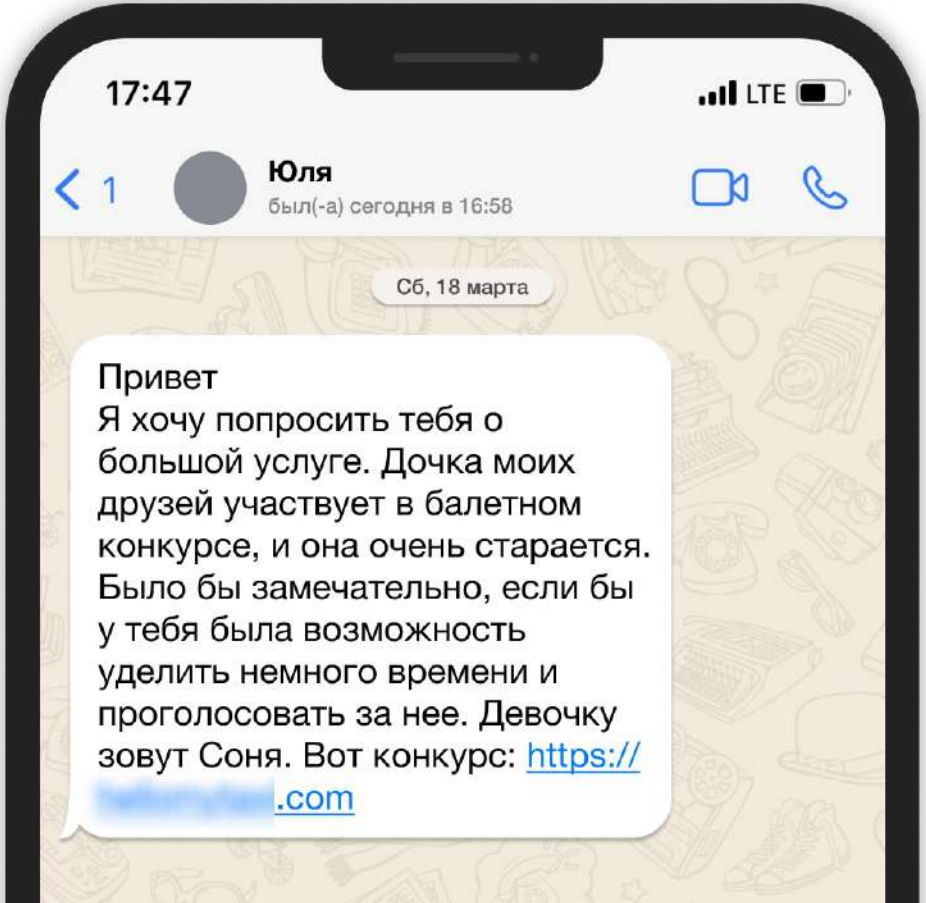
2. Уэйлинг

3. Емейлинг

4. Смишинг

вопрос 3

На какую эмоцию давят мошенники в этом сообщении?



ответ

1. Страх

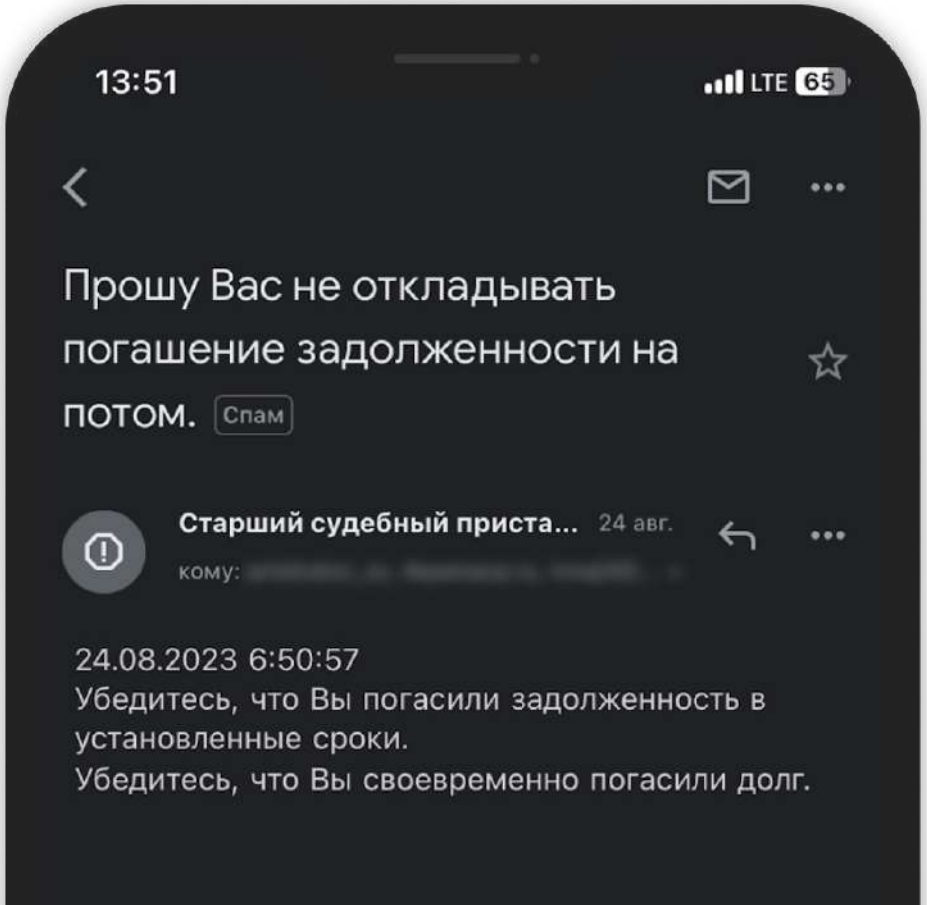
2. Желание помочь

3. Жадность

4. Любопытство

вопрос 4

На какую эмоцию давят мошенники в этом сообщении?



ответ

1. Страх

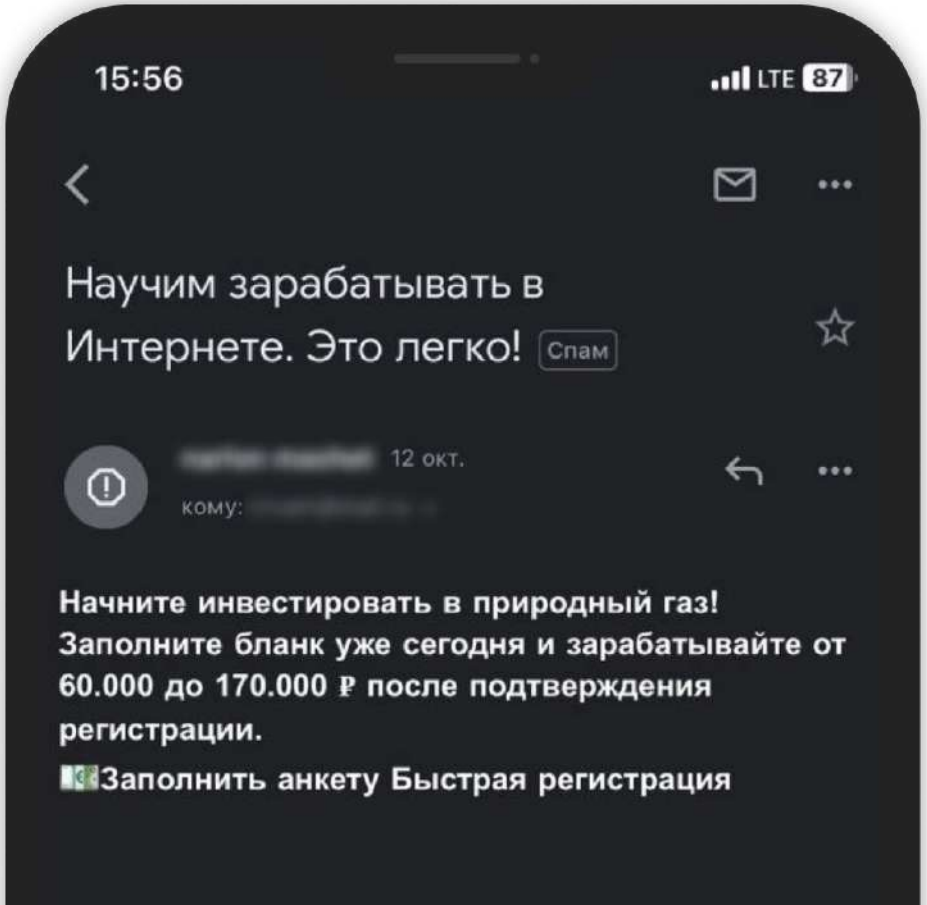
2. Желание помочь

3. Жадность

4. Любопытство

вопрос 5

На какую эмоцию давят мошенники в этом сообщении?



ответ

1. Страх

2. Желание помочь

3. Жадность

4. Любопытство

раунд 2

Ответы

вопрос 1

Мошенники — отличные психологи, они давят на эмоции жертв, чтобы поймать тех на крючок.

Соотнесите тему сообщения и эмоцию.

ответ

А. Страх	→	2. Ваш компьютер заражён и заблокирован
Б. Желание помочь	→	4. Ваш коллега потерял свои вещи
В. Раздражение	→	3. Чтобы отписаться, перейдите по ссылке
Г. Любопытство	→	1. Смотри, как ты отжигаешь на видео

вопрос 2

Справа перечислены разные типы фишинговых атак. Одно название из списка — выдуманное. Какое?

ответ

1. Вишинг

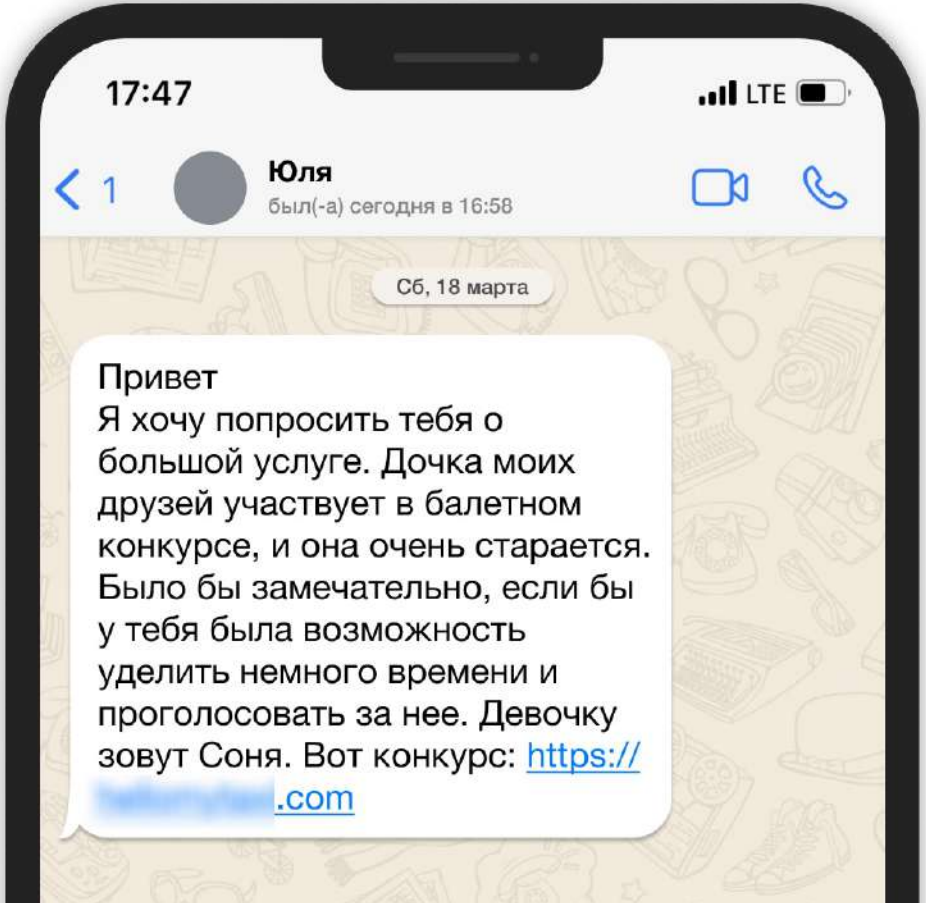
2. Уэйлинг

3. Емейлинг

4. Смишинг

вопрос 3

На какую эмоцию давят мошенники в этом сообщении?



ответ

1. Страх

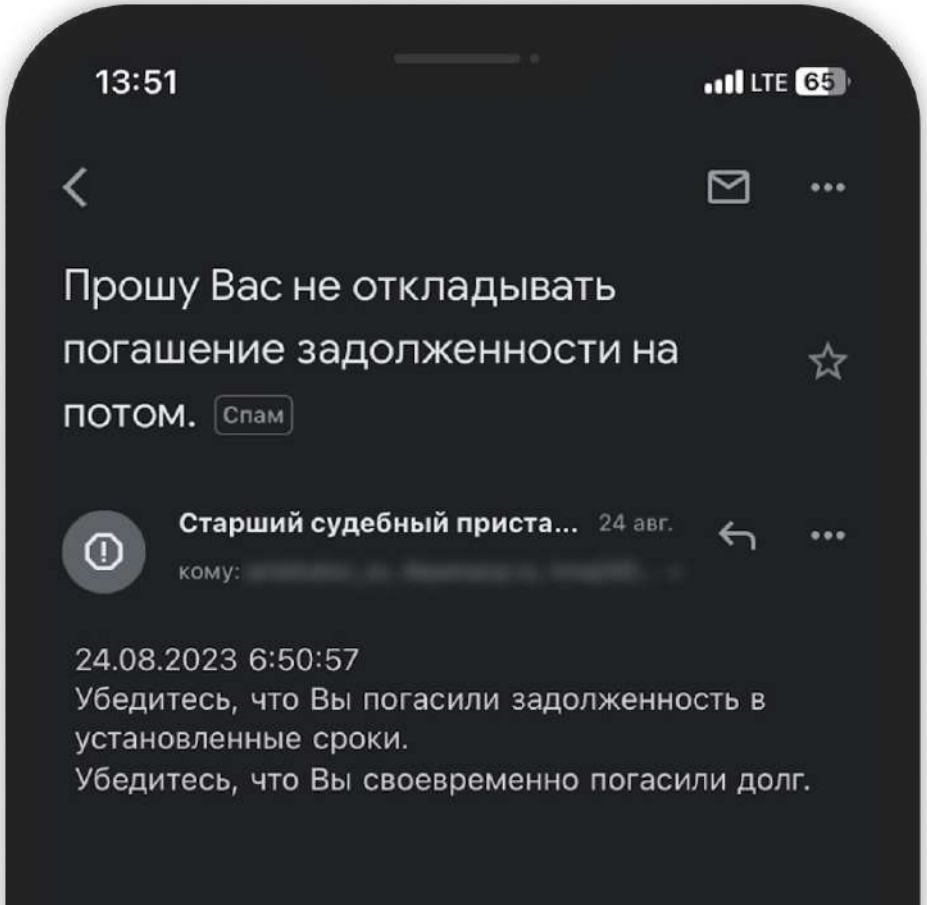
2. Желание помочь

3. Жадность

4. Любопытство

вопрос 4

На какую эмоцию давят мошенники в этом сообщении?



ответ

1. Страх

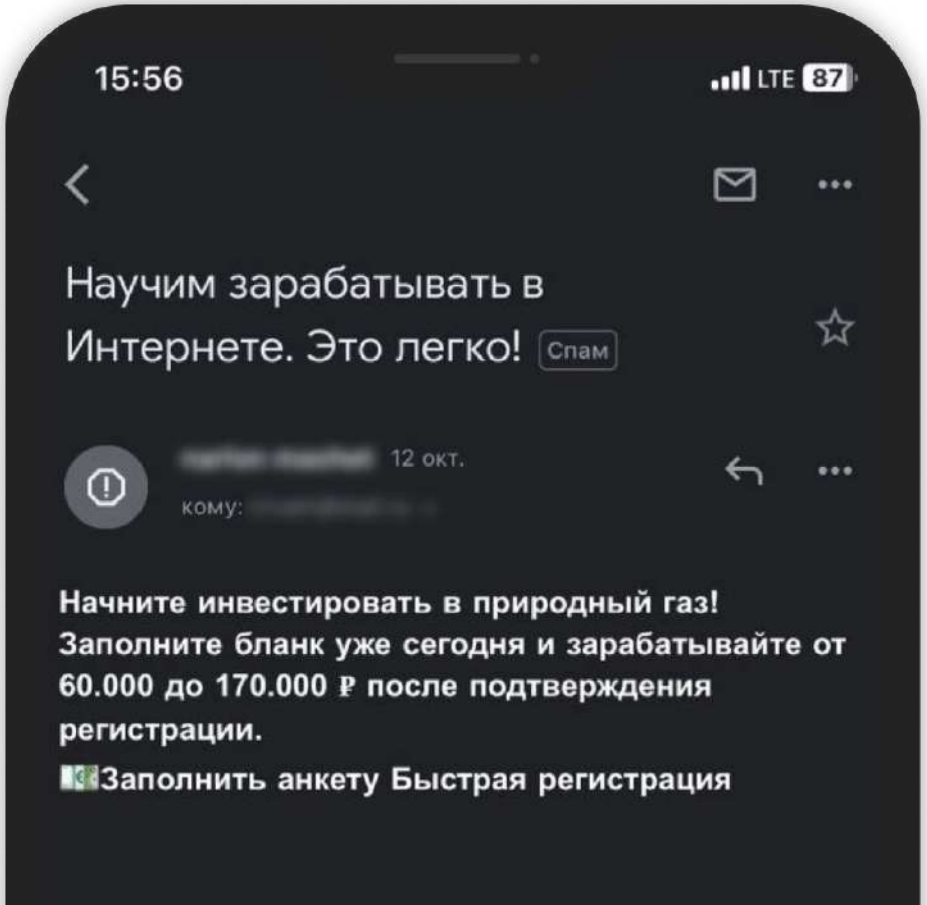
2. Желание помочь

3. Жадность

4. Любопытство

вопрос 5

На какую эмоцию давят мошенники в этом сообщении?



ответ

1. Страх

2. Желание помочь

3. Жадность

4. Любопытство

Игра «КиберЗащитник»

Цель: придумать как можно больше различных ситуаций, связанных с кибер-мошенничеством, и обосновать, почему эти ситуации опасны.

Правила:

1. Делимся на команды.
2. Придумываем как можно больше ситуаций с кибермошенничеством.
3. По очереди каждая команда читает ситуацию.
4. Повторы вычёркиваем.

Победит тот, кто прочитает последнюю ситуацию.

Игра «Проверь себя»

Правила:

1. Составьте 10 вопросов и напишите ответы (5 мин).
2. Передайте вопросы другой команде для ответов (5 мин).
3. Проверьте свои ответы.

Что мы узнали сегодня на уроке?

1. Кибермошенничество.
2. Фишинг.
3. Брутфорс.
4. Каким должен быть пароль.
5. Беспарольный вход (OnePass):
   - по лицу;
   - отпечатку пальца;
   - QR-коду;
   - SMS;
   - push-уведомлению.
6. Двухфакторная авторизация.
7. Социальная инженерия.

До новых встреч в следующем сезоне проекта!

ЦИФРОВОЙ ЛИКБЕЗ

ЦИФРОВАЯ ЭКОНОМИКА
D-ECONOMY.RU