КИБЕРБЕЗОПАСНОСТЬ: КАК НЕ СТАТЬ ЖЕРТВОЙ В ЦИФРОВОМ МИРЕ

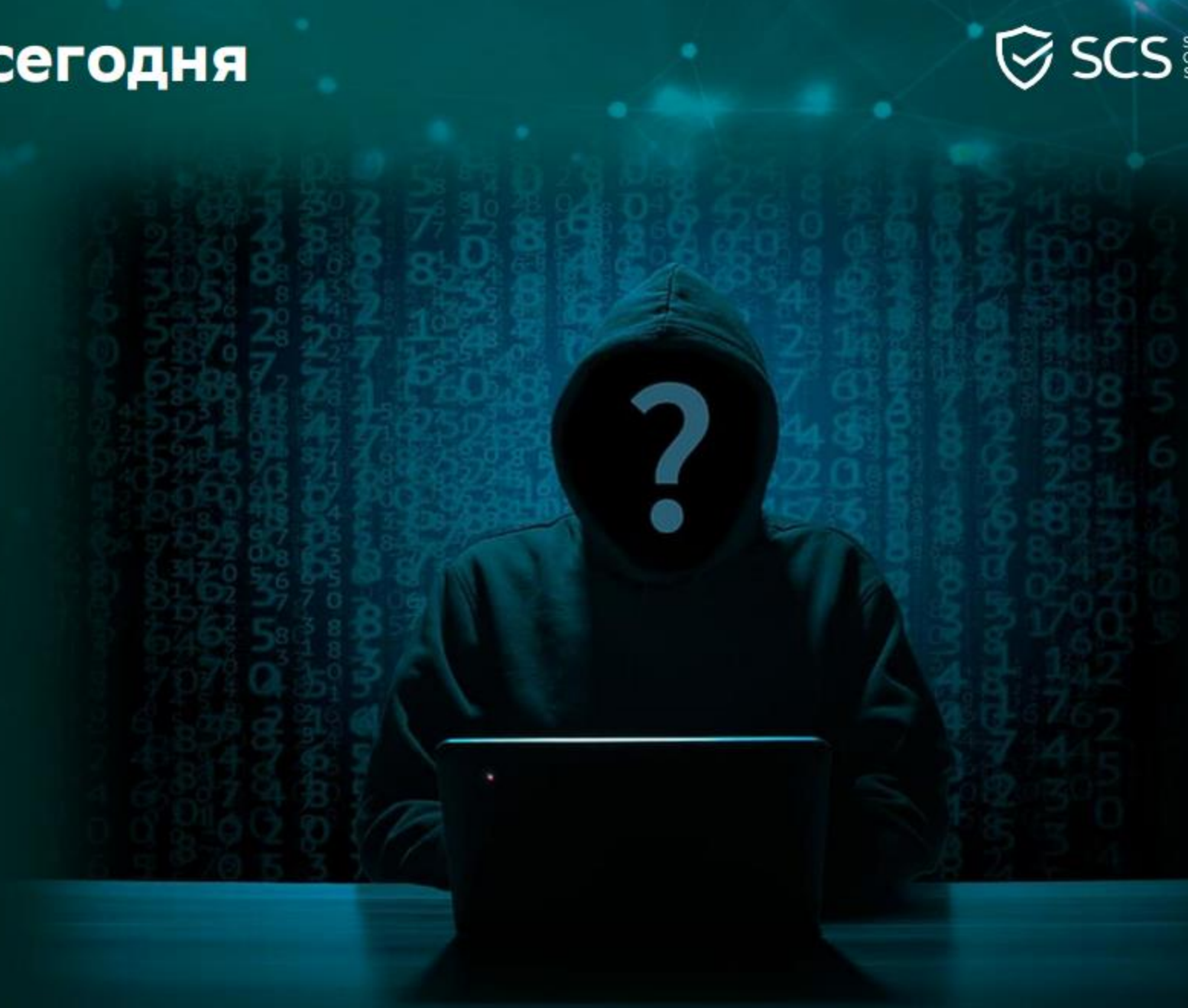
Киберпреступность сегодня

>510 тыс.

преступлений в сфере ИТ в 2022 г.*

1/4

доля преступлений в ИТ от общего числа преступлений в 2022 г.*



*Источник: МВД

Киберпреступность сегодня

83%

граждан России хотя бы раз сталкивались с кибермошенничество

5,2 тыс.

фишинговых сайтов выявлено в первом квартале 2023 г.[2]

[1]Источник: ЦБ РФ

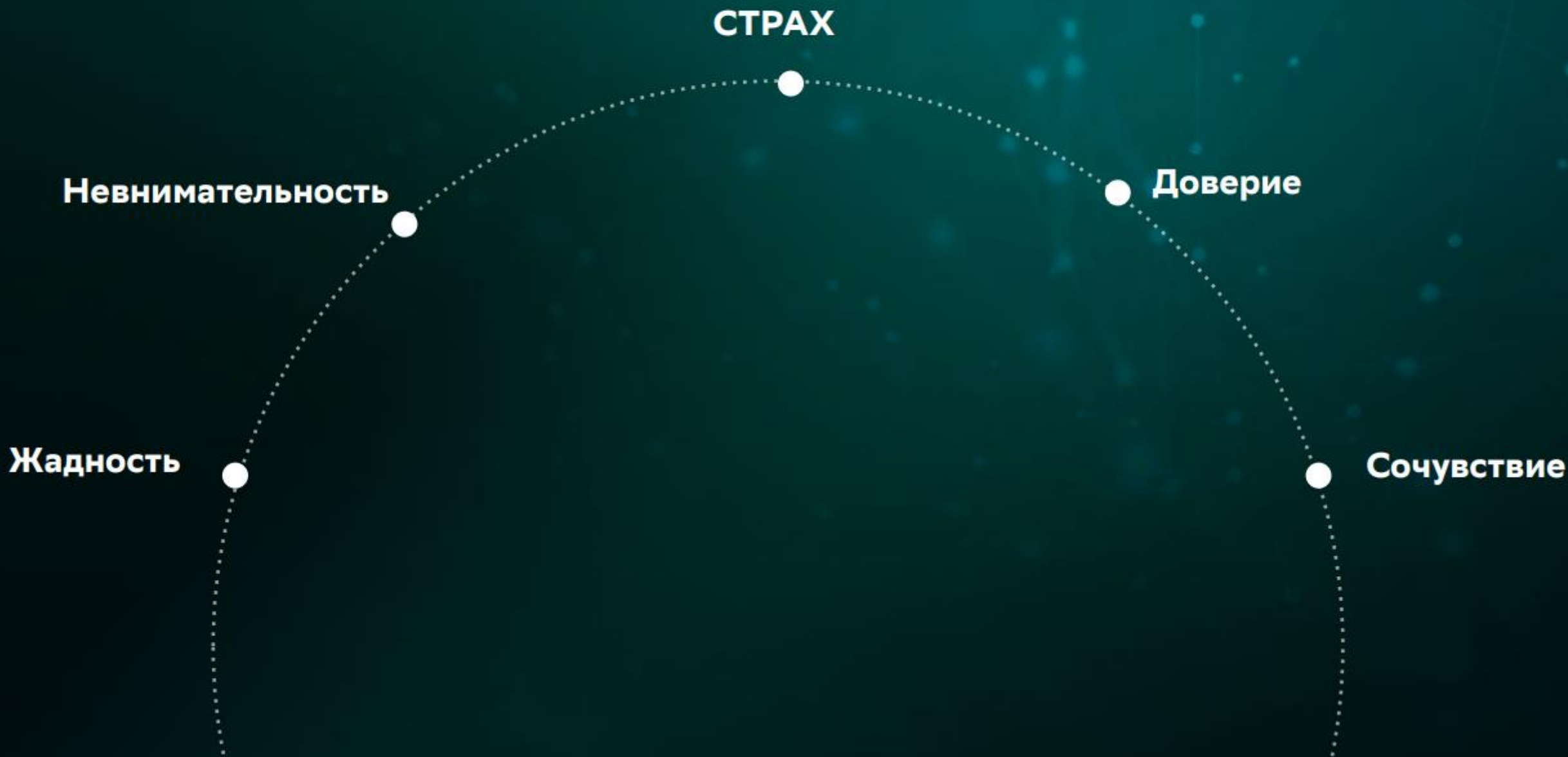
«Взломай» человека – взломаешь все остальное

Социальная инженерия – это...

...**психологическое манипулирование людьми** с целью совершения определенных действий или разглашения конфиденциальной информации. Социальная инженерия лежит в основе всех методов и видов кибермошенничества

Человек был и остается самым слабым местом в любой системе защиты: начиная от домашней сети и заканчивая эшелонированными системами безопасности крупной корпорации. **«Взломай» человека – взломаешь все остальное**

Злоумышленники используют чувства и эмоции



Использование новостной повестки

2020-2021

- COVID-19
- Вакцинация

2022-2023

- СВО
- Мобилизация

2024-...

- Выборы
- ЧЕ 2024

Злоумышленники всегда эксплуатируют наиболее «горячие» темы

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

2022 год:

14 млрд.руб.
украдено
злоумышленниками

15 млн. раз
позвонили
мошенники
россиянам

«У меня зазвонил телефон. Кто говорит?..»

Служба безопасности

Сотрудник ЦБ

Майор ФСБ

Капитан полиции

Старший следователь СК

Мама, это я

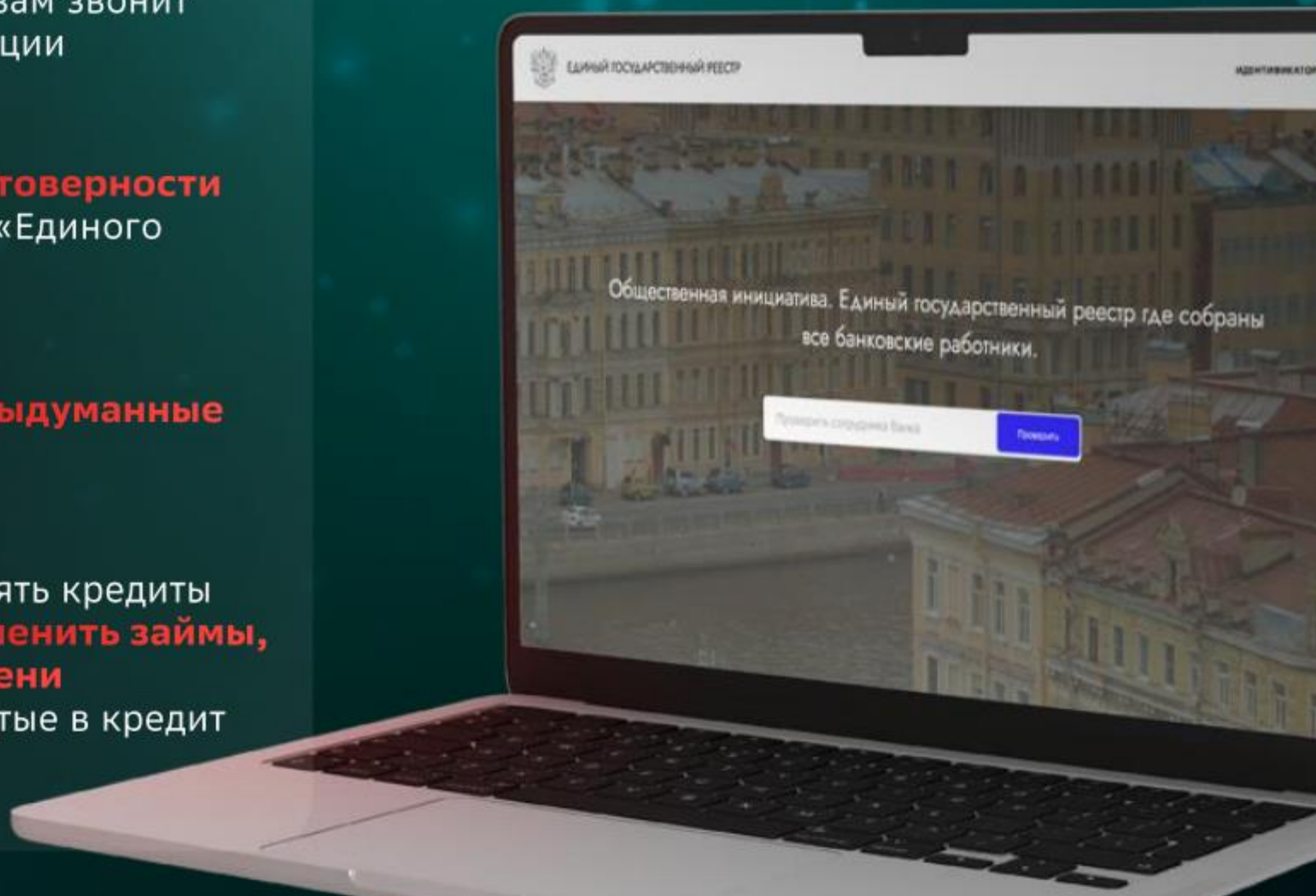
Поддельный реестр сотрудников

Мошенники создают сайты, на которых якобы можно проверить, действительно ли вам звонит настоящий сотрудник банка или полиции

Жертве предлагают **убедиться в достоверности** сообщаемой информации через сайт «Единого государственного реестра»

После ввода номера **жертва видит выдуманные характеристики «работника»**

Мошенник убеждает клиента оформлять кредиты в разных банках для того, чтобы **«отменить займы, которые пытаются взять от его имени злоумышленники»,** и перевести взятые в кредит деньги на «безопасный счёт»



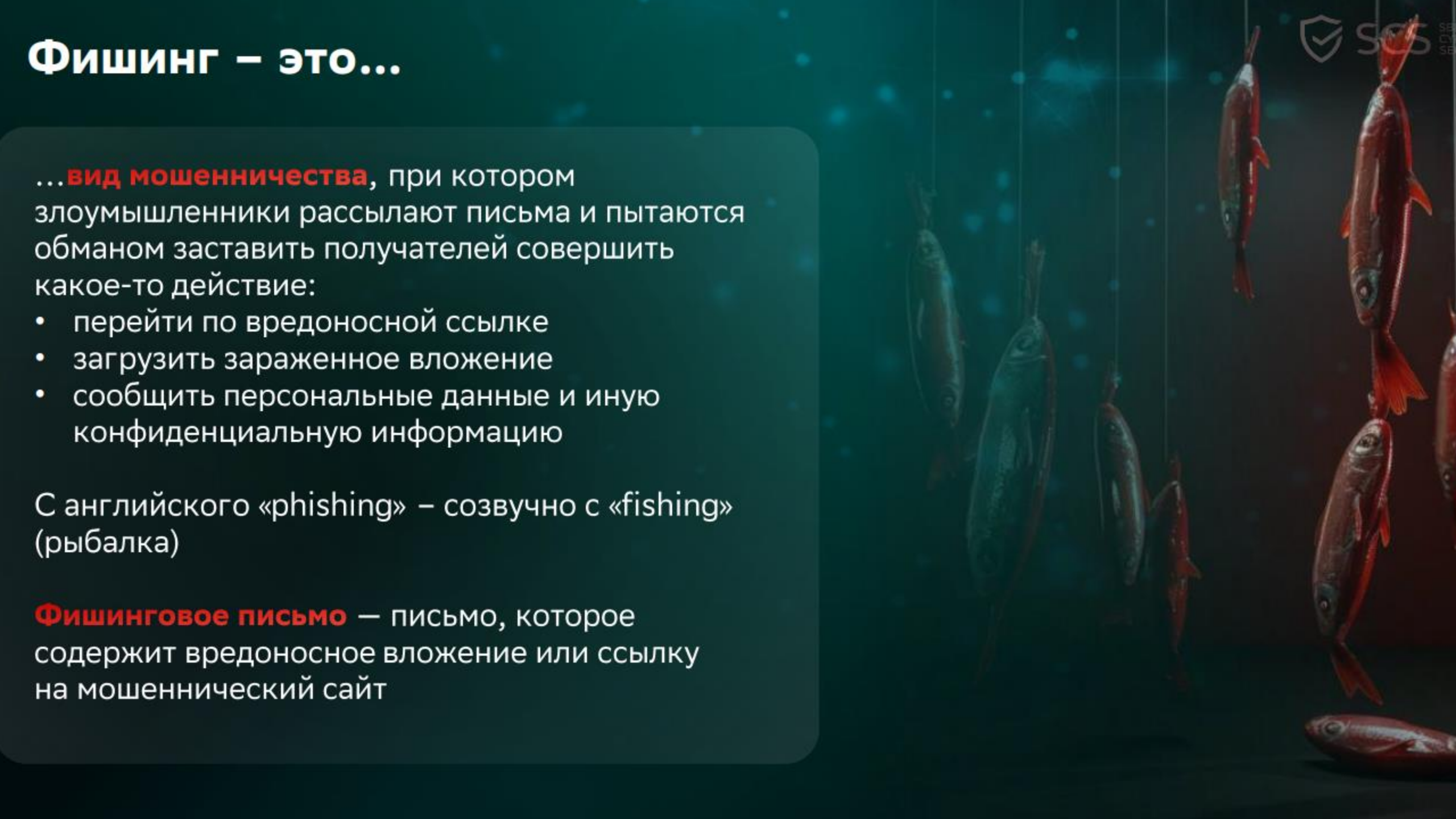
Фишинг – это...

...**вид мошенничества**, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей совершить какое-то действие:

- перейти по вредоносной ссылке
- загрузить зараженное вложение
- сообщить персональные данные и иную конфиденциальную информацию

С английского «phishing» – созвучно с «fishing» (рыбалка)

Фишинговое письмо — письмо, которое содержит вредоносное вложение или ссылку на мошеннический сайт



Какие уловки используют мошенники в письмах

Службы доставки

Маркетплейсы

Криптовалюта

Горячие новости

Лотерии

Дополнительный заработок и инвестиции

Туроператоры и отдых

Билеты на мероприятия

Подписки и онлайн-сервисы

Мошенничество в социальных сетях

Инфоцыгане

Голосования

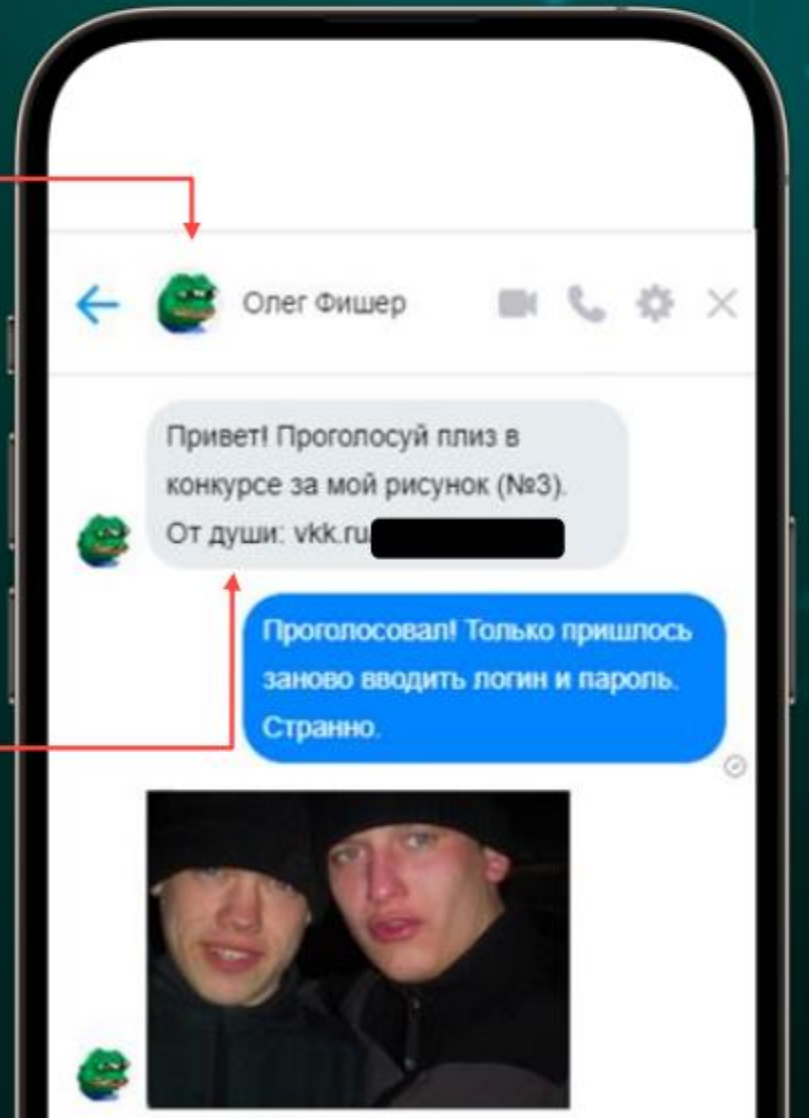
Взлом аккаунтов

Цифровое клонирование

«Голосуй или проиграешь!»

Неизвестный контакт или ваш знакомый (которого взломали)

Просьба совершить деиствие и ссылка на внешний ресурс



Успешный успех

Инфоцыгане в социальных сетях — это особая категория коучей и бизнес-тренеров, которые обещают научить вас всем своим секретам, благодаря которым вы тут же разбогатеете. Такие курсы, разумеется, платные.

- Вам гарантируют результат
- Человек является супер-экспертом во всех областях сразу
- Основной фокус в рекламе сосредоточен на эмоциях, а не на конкретных знаниях
- Возраст бизнес-тренера
- Навязчивая и «кричащая» реклама курсов и тренингов
- Инфоцыгане не любят заключать договор об обучении

Как ~~заработать~~ потерять более 15 000₽ за день

1. Злоумышленники создают группу в мессенджерах или отправляют сообщения, в которых предлагают оценивать сервис бронирования отелей / выкупать товары.

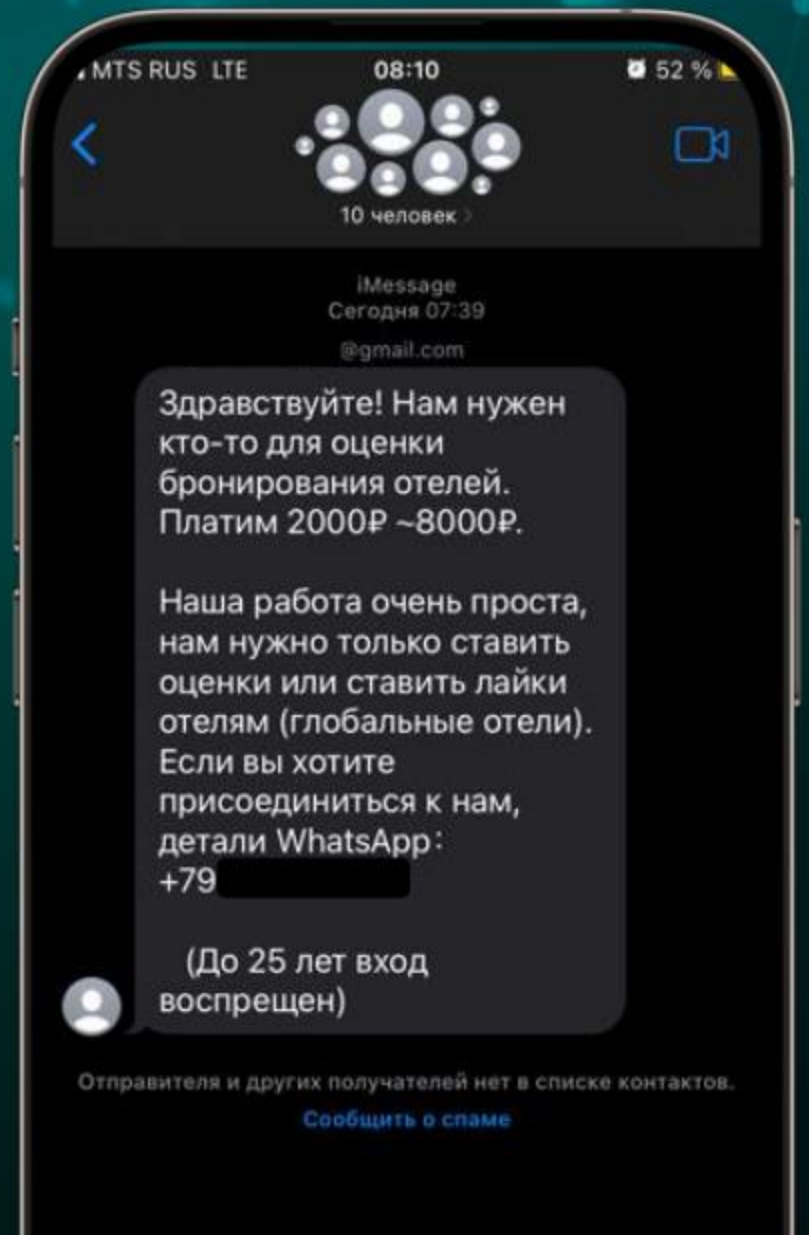
2. Пользователю предлагается связаться с персональным «менеджером» для обсуждения «сотрудничества».

3. Злоумышленники отправляют клиенту ссылку на мошеннический сайт, где нужно пройти регистрацию.

4. После регистрации клиенту необходимо внести определённую сумму на указанный счет, чтобы начать выполнять задания по оценке различных отелей или выкупе товаров за низкую цену.

5. В конце каждого «рабочего» дня на счете клиента первоначально «инвестированная» сумма увеличивается.

6. Вывести «заработанные» деньги не получится, а попытки связаться с «менеджером» ни к чему не приведут.



Псевдоброкеры – это...

...**мошенники, которые выдают себя за профессиональных участников фондового рынка.** Они регулярно предлагают клиентам брокерские или дилерские услуги, с помощью которых якобы можно преумножить свой капитал.

«Взломать» могут каждого

Завышенная самооценка

Со мной это никогда не случится…

БАНК должен…

КАК ЗАЩИТИТЬ СЕБЯ

Надежный пароль

Сколько времени нужно, чтобы взломать пароль

Кол-во знаков	Только цифры	Строчные буквы	Прописные и строчные буквы	Цифры, прописные и строчные буквы	Цифры, прописные и строчные буквы и символы
8	мгновенно	5 сек.	22 мин.	1 час	8 часов
9	мгновенно	2 мин.	19 ч.	3 дня	3 недели
10	мгновенно	58 мин.	1 месяц	7 мес.	5 лет
11	2 сек.	1 день	5 лет	41 год	400 лет
12	25 сек.	3 недели	300 лет	2 тыс. лет	34 тыс. лет

Как можно создать надежный пароль

SCS SBER CYBER SECURITY

Возьмите фразу или цитату, например, «Терпение и труд всё перетрут», соедините первые буквы слов или слоги	Придумайте одно или два числа, которые легко запомнить – число/месяц рождения, счастливое число, текущий год	Выберите любой спецсимвол (а лучше 2), который вам нравится	Создайте пароль, соединив три части в произвольном порядке
TiTrVsPere	**22 и 7**	**% и !**	**T22iTr%Vs7Pere!**

СЕРВИСЫ СБЕРБАНКА

Сервисы кибербезопасности в «СберБанк Онлайн»

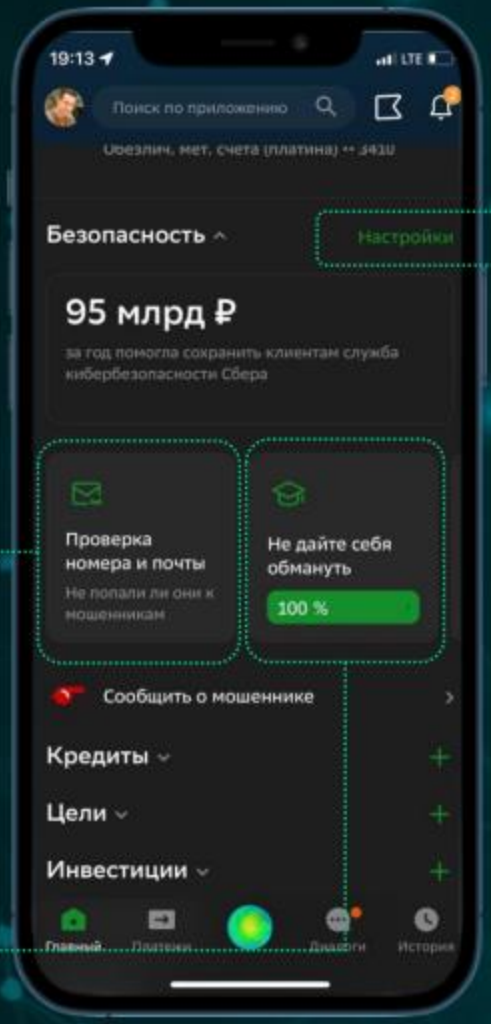
65 млн
пользователей

Сервисы кибербезопасности

- Проверка входящих звонков
- Проверка номера и почты на утечки
- Закрытие доступа к картам и вкладам
- Передача информации о мошеннике в Банк

Повышение киберграмотности клиентов

- Комиксы-статьи и видеоролики об актуальных схемах мошенничества
- Тестирование клиентов на уровень киберграмотности



Продукт на главном экране!

Настройки кибербезопасности

- Управление доступностью продуктов
- Настройка ограничения оплаты в интернете
- Управление доверенными устройствами
- Установка лимитов на снятие наличных
- Изменение суточного лимита
- Настройка способа входа в личный кабинет СБОЛ
- Проверка операций близкого

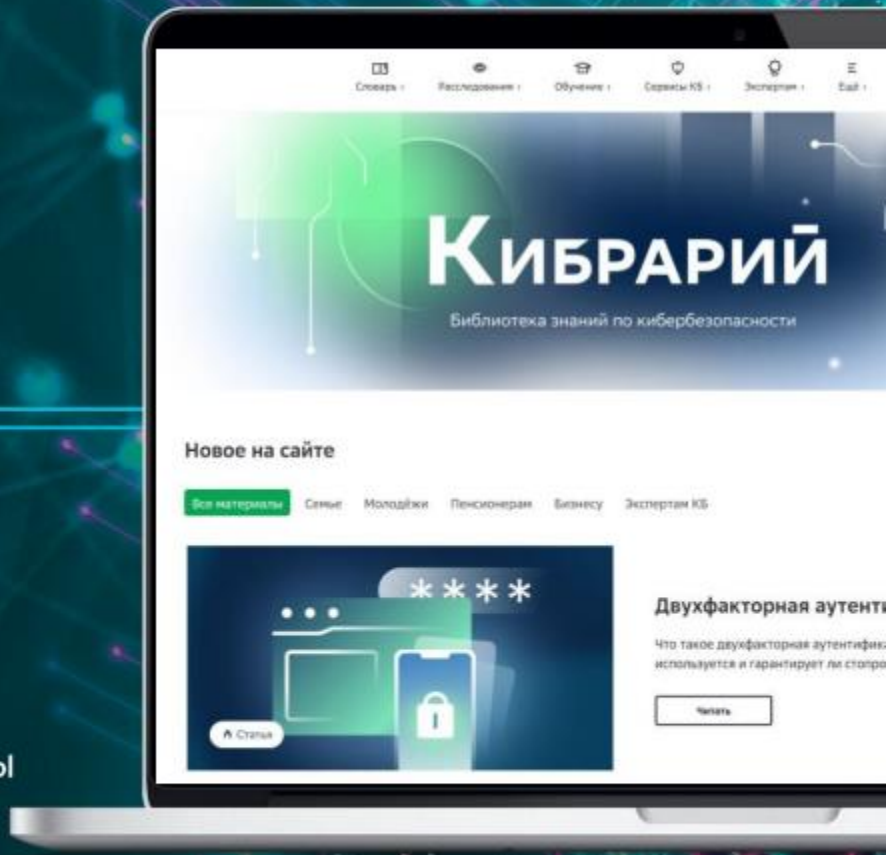
«Кибрарий» – библиотека знаний по кибербезопасности

>100
терминов и определений

>15
видеоматериалов по схемам мошенничества

sberbank.ru/kibrary

«Кибрарий» – общедоступный портал знаний для развития киберграмотности населения



Более 200

полезных материалов для повышения киберграмотности
(памятки, статьи, тесты, советы, курсы и рекомендации экспертов СберБанка)

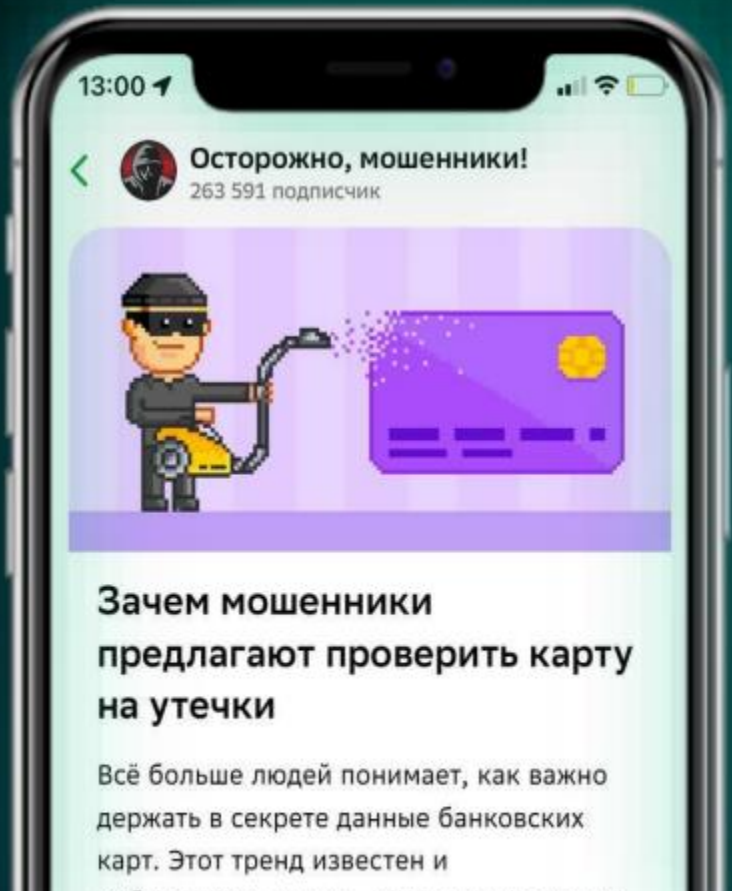
Расследования
Полезная информация

Советы и рекомендации
Обучающие курсы

Информационные каналы в Сбербанк Онлайн

2 новых поста
каждую неделю

В канале
«Осторожно, мошенники!»
регулярно публикуются
самые актуальные
мошеннические схемы
и способы защиты от них



В кан
«Ничего лично
рассказываем о том,
использовать, храни
передавать лич
информа

СберСова – платформа развития финансовой грамотности Сбера