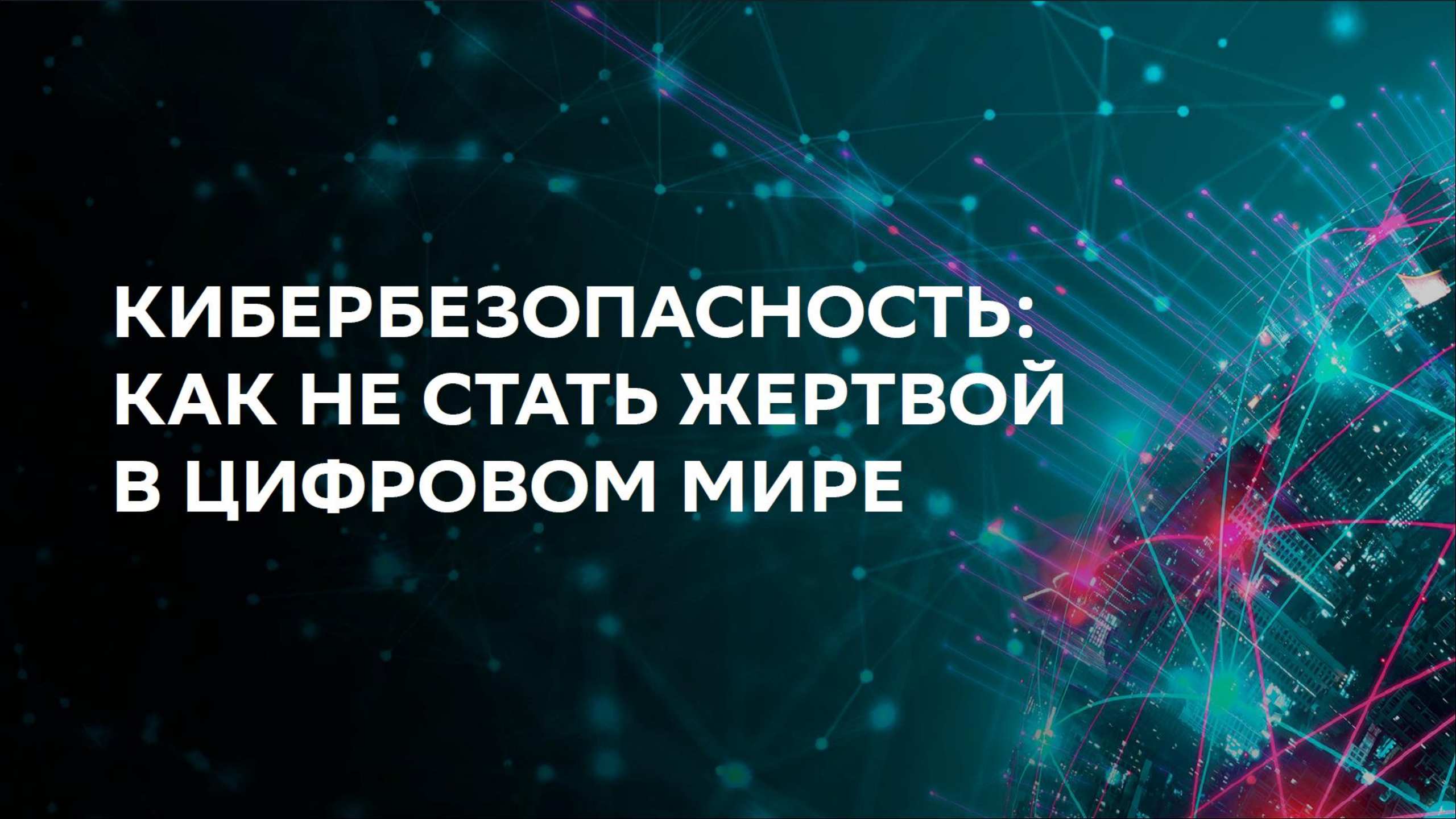
КИБЕРБЕЗОПАСНОСТЬ: КАК НЕ СТАТЬ ЖЕРТВОЙ В ЦИФРОВОМ МИРЕ



Киберпреступность сегодня

SCS SBER CYBER SECURITY

>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 кибермошенничеством[1]

5,2 тыс.

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

[1]Источник: ЦБ РФ
[2]Источник: АНО «Координационный центр доменов»

Что нужно киберпреступникам

Free photo Crime Cyber Internet Criminal Security Cyberspace - Max Pixel

Ваши данные

Ваши деньги

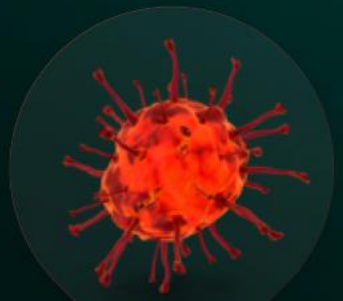
Социальная инженерия – это...

...**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

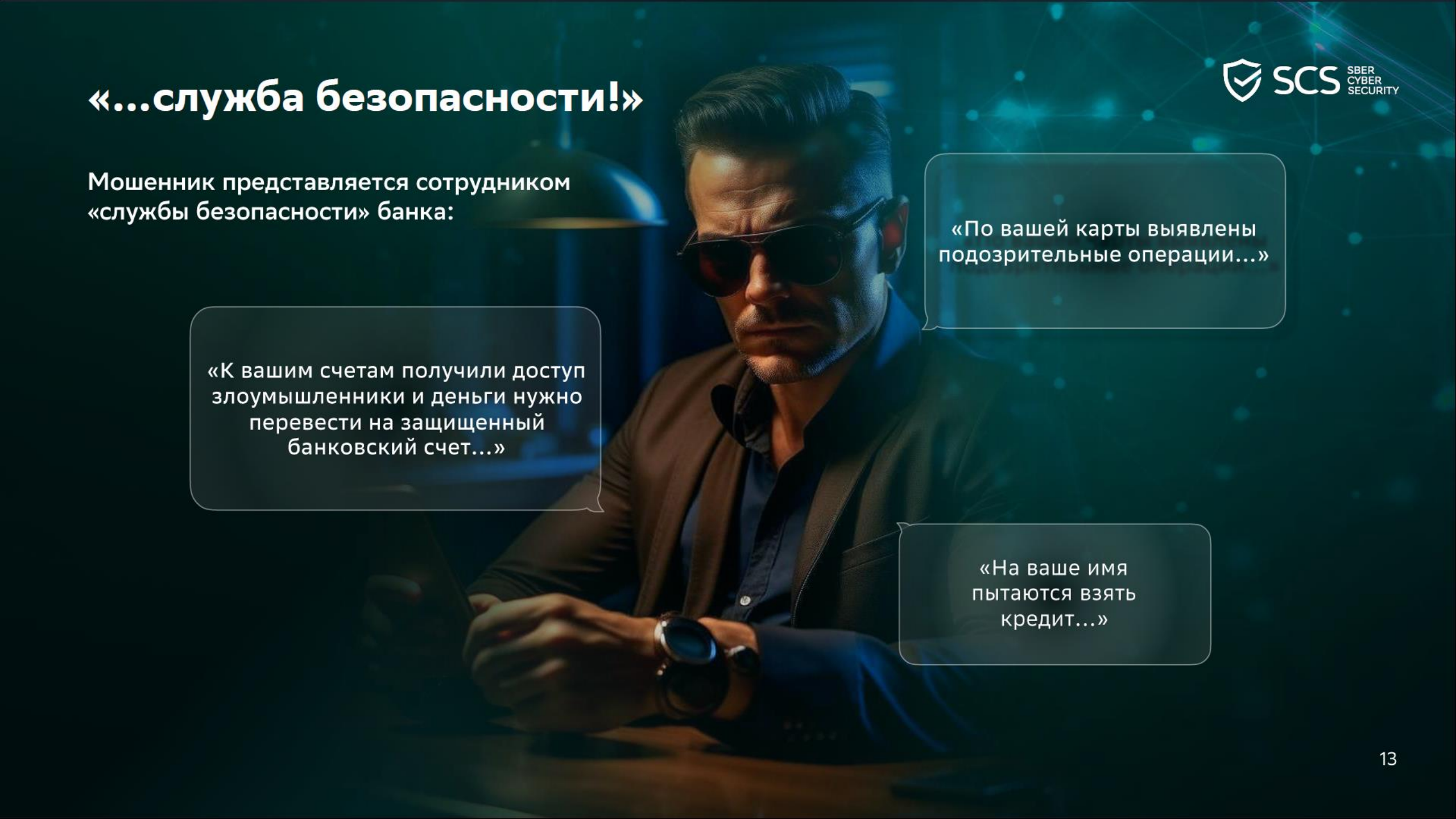
2024-...

- Выборы
- ЧЕ 2024

Злоумышленники всегда эксплуатируют наиболее «горячие» темы

«...служба безопасности!»

Мошенник представляется сотрудником «службы безопасности» банка:



«По вашей карты выявлены подозрительные операции...»

«К вашим счетам получили доступ злоумышленники и деньги нужно перевести на защищенный банковский счет...»

«На ваше имя пытаются взять кредит...»

Когда звонит «тащмайор»

Мошенник представляется сотрудником МВД / СК / ФСБ:

- Злоумышленник предлагает решить проблему:
  - Вывести все деньги с банковских карт жертвы и перевести их на «безопасный» счет.
  - Исчерпать лимит кредитов по карте и перевести их на «безопасный» счет.
- Часто в схеме участвует не один человек

«По вашим поддельным документам кто-то пытается взять кредит на крупную сумму...»

«Родственник попал в беду или вы?»

Мошенник представляется сыном / внучкой / родственником:

- Все это говорится быстро и с максимально достоверной актерской игрой, чтобы ввести потенциальную жертву в стресс и не дать мыслить рационально
- Злоумышленники отправляют курьера по адресу жертвы, чтобы забрать «деньги», после чего исчезают

«Я сбил
на машине ребенка,
но уже договорился
о взятке, срочно нужны
деньги»

Что делать, если звонят мошенники

Внимательно проверяйте входящий номер

Не совершайте никаких операций по инструкциям звонящего

Сразу заканчивайте разговор при любых сомнениях

Проверьте, не было ли сомнительных операций за время разговора

Сотрудники правоохранительных органов **не могут допрашивать по телефону**

ЦБ РФ никогда не звонит физическим лицам

Поставьте приложение для фильтрации входящих вызовов

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

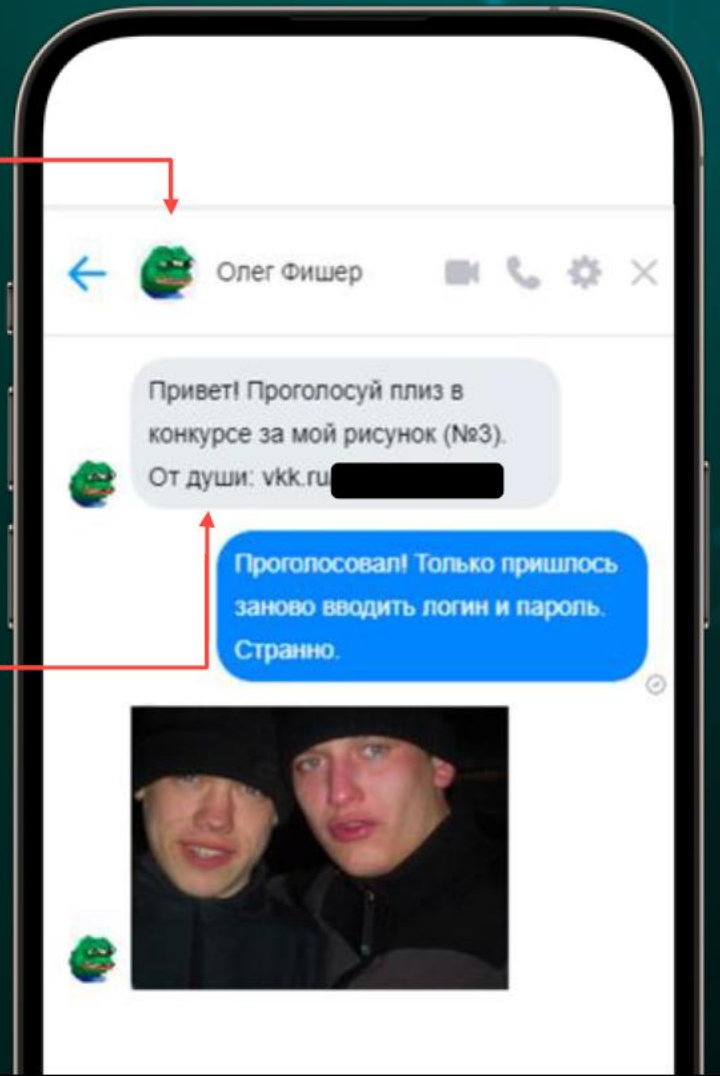
С английского «phishing» – созвучно с «fishing» (рыбалка)

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

«Голосуй или проиграешь!»

Неизвестный контакт или ваш знакомый (которого взломали)

Просьба совершить деиствие и ссылка на внешний ресурс



Что делать, если есть подозрение на фишинг

Обращайте внимание
на домен

Обращайте внимание
на обращение и подпись

Внимание: побуждение
к немедленному действию

Не переходите по ссылкам,
не кликайте на подозрительные
объекты.

Будьте осторожны
с вложениями

Не вводите свои данные
и не отвечайте
на подозрительные письма

Угрозы конфиденциальности

Любое действие в сети оставляет цифровой след

Цифровой след

- Регистрация на сайтах
- Лайки в соцсетях
- Посты и репосты
- Комментарии к постам
- Фото и видео

Цифровой портрет

Кнопки Delete в Интернете нет

Базовые правила кибербезопасности

SCS SBER CYBER SECURITY

- Обновляйте операционную систему и приложения
- Используйте защитное программное обеспечение на компьютерах и смартфонах
- Создавайте надежные и уникальные пароли для всех ресурсов
- Настройте двухфакторную аутентификацию везде, где это возможно
- Создавайте резервные копии важной информации
- Устанавливайте только лицензионное программное обеспечение и приложения из надежных источников
- Не оставляйте личные устройства без присмотра
- Не переходите по подозрительным ссылкам
- Сомневайтесь и будьте скептиком

Надежный пароль

SCS SBER CYBER SECURITY

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

Сервисы кибербезопасности в «СберБанк Онлайн»

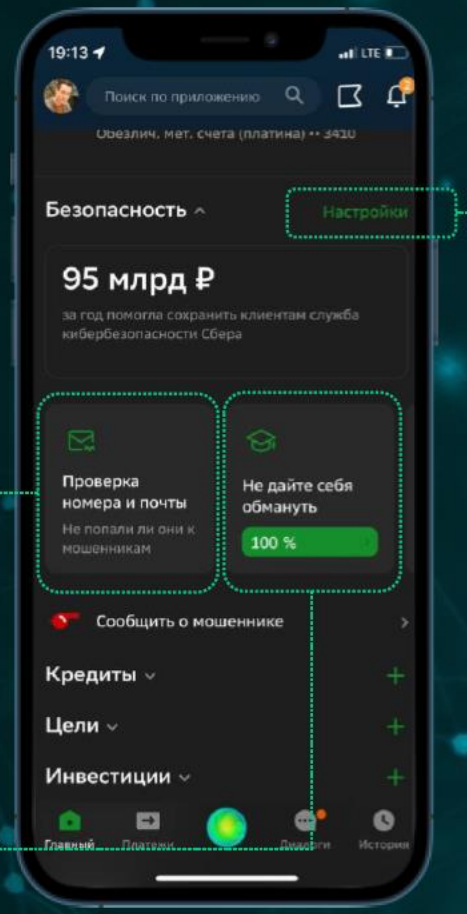
65 млн
пользователей

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

Информационные каналы в Сбербанк Онлайн

SCS SBER CYBER SECURITY

2 новых поста каждую неделю

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

В канале **«Ничего личного»** рассказываем о том, как использовать, хранить и передавать личную информацию