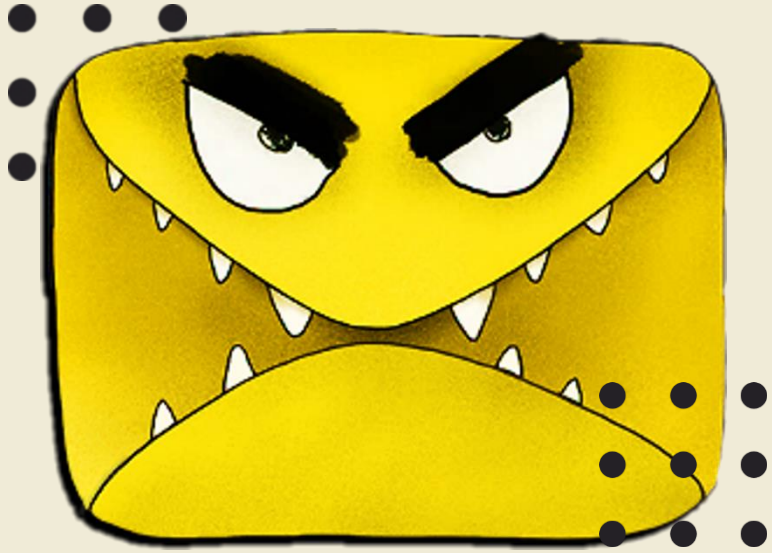
СБЕР

ВСЕРОССИЙСКАЯ ПРОГРАММА ДНИ ФИНАНСОВОЙ ГРАМОТНОСТИ В УЧЕБНЫХ ЗАВЕДЕНИЯХ

DPO DATA PROTECTION OFFICE

Вебинар на тему:

Гуру антифишинговых наук



Вперед!

СПИКЕРЫ

Андрей Никифоров

Эксперт по защите персональных данных
ПАО СберБанк

Илья Бичаров

Эксперт по защите персональных данных
ПАО СберБанк

Гуру должен знать:

01 Что такое фишинговые рассылки

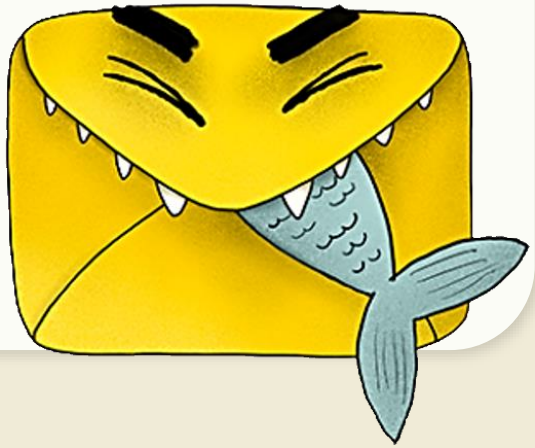
02 Что такое фишинг по электронной почте

03 Что такое фишинг по СМС

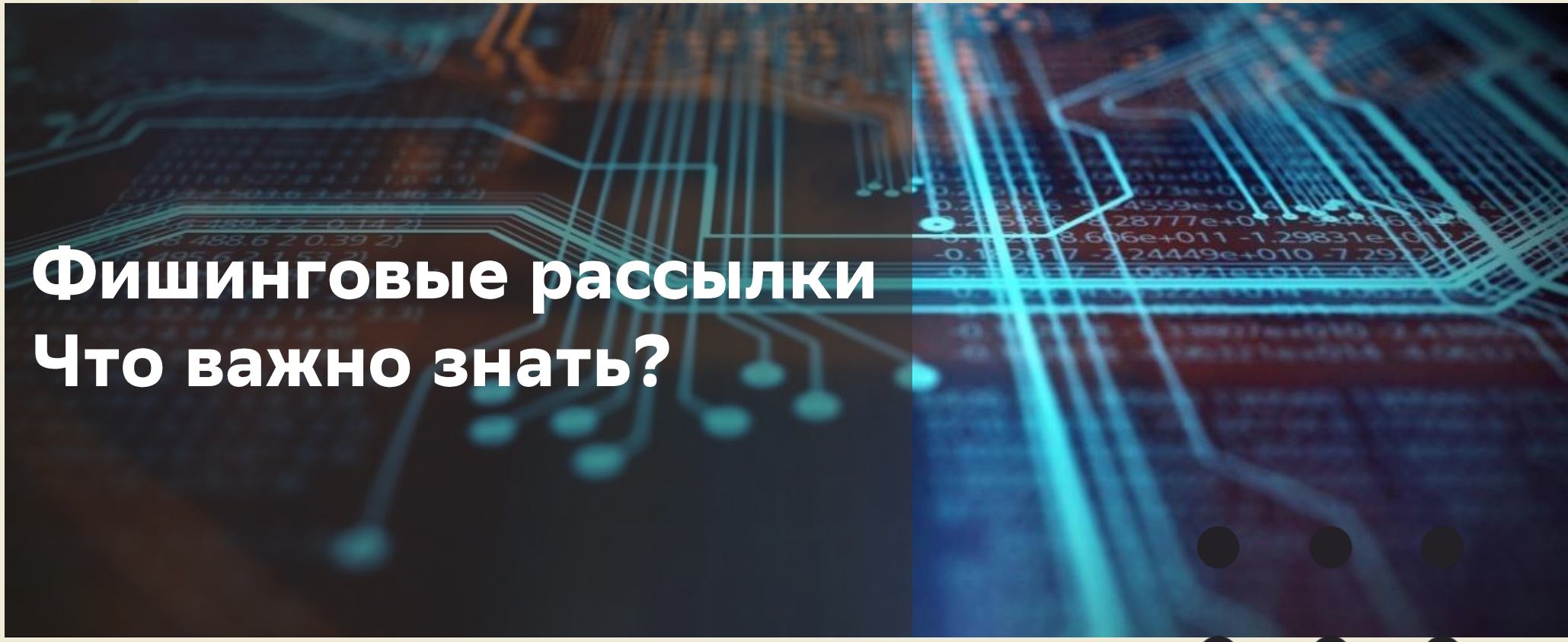
04 Что такое фишинг в мессенджерах и соцсетях

05 Какие новые схемы фишинга существуют

06 Общие правила безопасности



01



Фишинговые рассылки
Что важно знать?

Почему же мы попадаемся?

Мошенники используют триггеры, использующие **наши состояния:**

Восторга

Страха

Невнимательности

Любопытства

ВАЖНО помнить: на фишинговых сайтах всегда есть вредоносная ссылка – иногда она указана напрямую, либо интегрирована в баннер или картинку, в определенные слова (например, «ссылка»).

Фишинговые рассылки

Фишинг – один из самых распространенных видов мошенничества

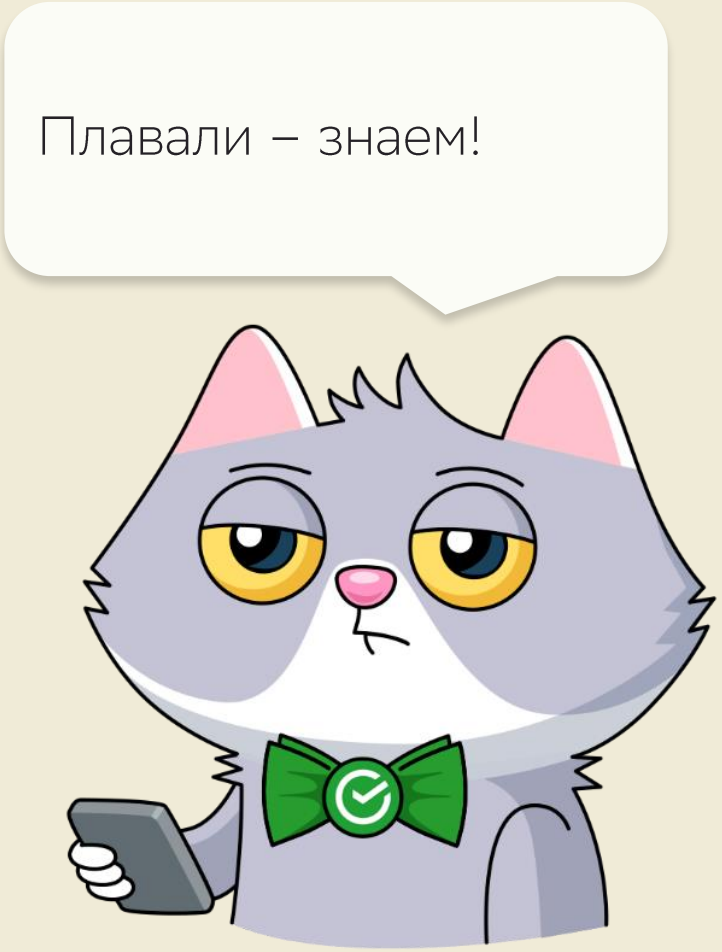
Фишинг (англ. phishing от fishing «рыбная ловля, выуживание»)

Фишинг – инструмент социальной инженерии

Социальная инженерия – метод манипуляции мыслями и поступками людей, который базируется на психологических особенностях личности и закономерностях человеческого мышления.

Рассылки - один из основных способов фишинга

Фишинговая рассылка – вид интернет-мошенничества, при котором обманным путем заставляют получателей нажать на вредоносную ссылку или скачать вложение, чтобы украсть их личную информацию и деньги.



Примеры вредоносных ссылок

Ссылка в виде цифр:

http://148.258.287.27

Ссылка с символом «@»:

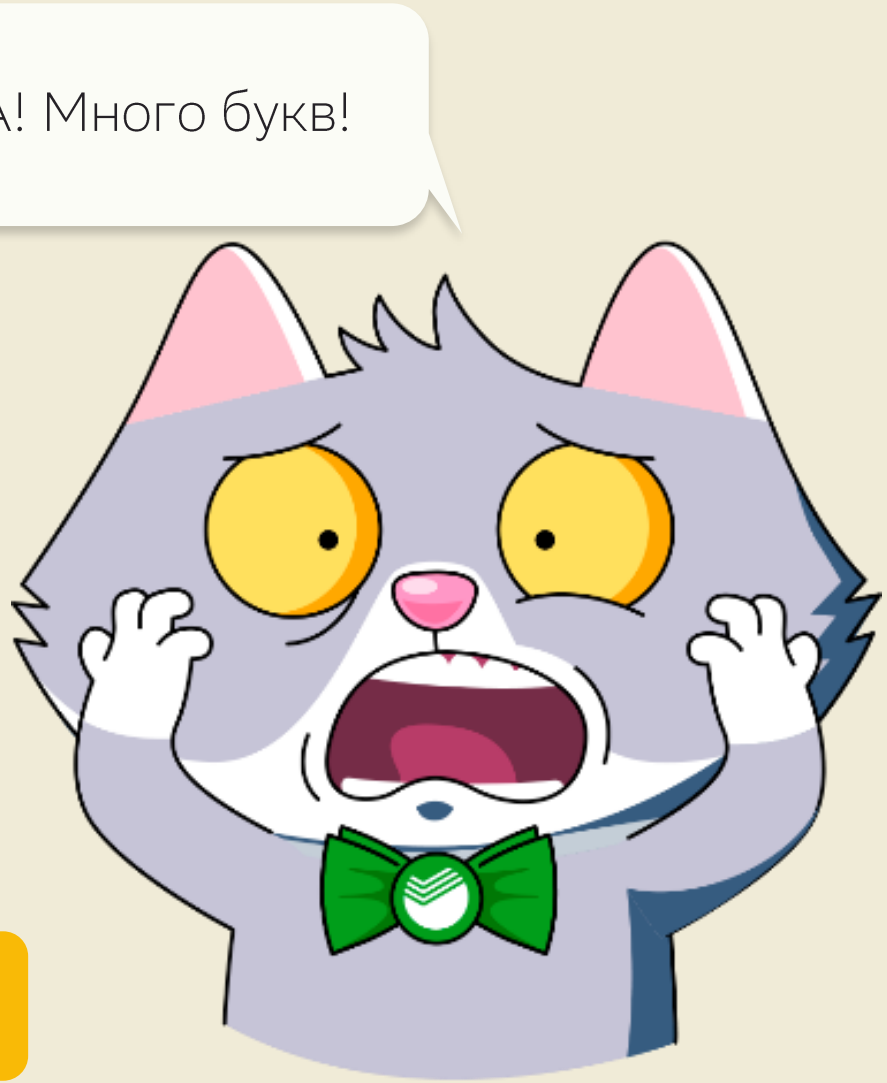
http://bank.ru@fake.ru

Ссылки с поддоменами:

https://sberbank.prizy.ru

Ссылки с двумя и более адресами:

https://bank.ru/rd.php?go=https://fake.ru



Как распознать вредоносные ссылки

- При наведении курсора на ссылку она выглядит иначе:

  написано tele2.ru, а при наведении мыши отображается

  teie2@167.xx.123.ru

- Ссылка некликабельна:

  указана ссылка gosuslugi.ru, при копировании оказывается, что это

  gosyslugi.ru

- Замена букв в названии адреса (вместо online.bank.ru)

  Заменены буквы «b» на «d», «l» на «I», «o» на «0»

  0nline.dank.ru

ВАЖНО помнить:
вы всегда можете проверить ссылку на официальном сайте СБЕРа

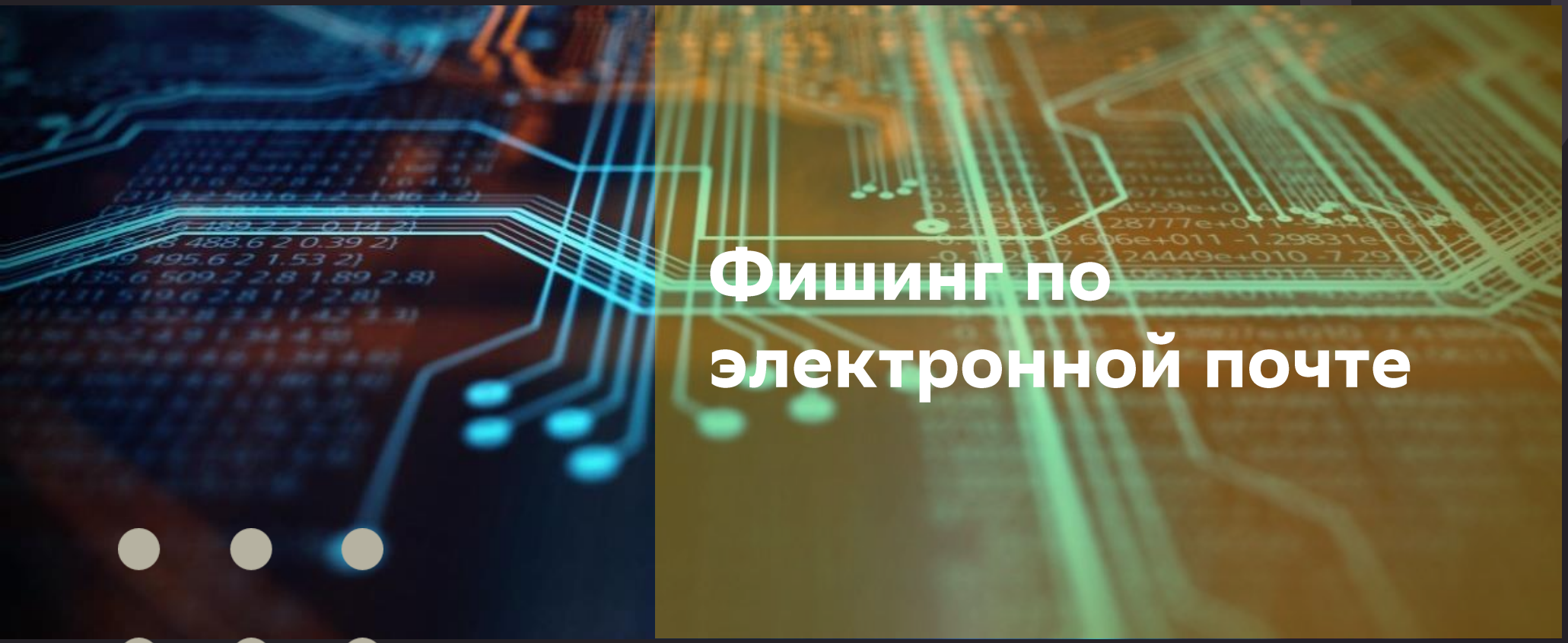
Фишинговая рассылка осуществляется через следующие каналы

электронная почта

SMS

популярные мессенджеры

социальные сети



Фишинг по электронной почте

Самые распространенные мошеннические схемы с использованием электронной почты

1. Без голоса: как мошенники выдают себя за сотрудников банка в переписках
2. «Отписка от спама»: новый способ мошенничества с электронной почтой
3. Обман с помощью популярных форм опросов
4. Сказочно большие скидки
5. Игра на нашем азарте

Как распознать фишинговое письмо?

1. Обезличенное обращение
2. Адрес отправителя
3. Домен отправителя
4. Ошибки в словах и названиях брендов
5. Предложение перейти по сомнительной ссылке
6. Просьба ввести логин и пароль при переходе по ссылке
7. Тревожная тональность сообщения
8. Супервыгодное предложение
9. Только картинки, кнопки, QR-коды

Как защититься от фишинговых писем

1. Не спешите с действиями и проверьте письмо на признаки фишингового письма
2. Проверяйте любую информацию на официальных сайтах, в группах и аккаунтах
3. Обращайте внимание на ссылки
4. Блокируйте нежелательных отправителей
5. Настройте СПАМ-фильтр

Все потому, что настроил спам-фильтры!

Фишинг по СМС

СМС-фишинг (смишинг)

Смишинг – вид фишинга, направленный на то, чтобы пользователь, получив СМС-сообщение от якобы надежного отправителя, выдал данные своей банковской карты, пароли или другую персональную информацию.

После перехода по ссылке из сообщения для ввода данных пользователь попадает на поддельный сайт с виду похожий на оригинальный или сайт, зараженный вирусом.
Итог – потеря данных и денег...

Самые распространенные мошеннические схемы с использованием смишинга

Мошенническая СМС-бомбежка

Отмена экспорта данных

Ошибочный перевод

СМС от доски объявлений

СМС-опросы

Основные правила безопасности

1 **Будьте осторожны с сообщениями от мобильного оператора**

2 **Не перезванивайте по подозрительным номерам**

3 **Не поддавайтесь на манипуляции мошенников**

4 **Остерегайтесь заманчивых предложений**

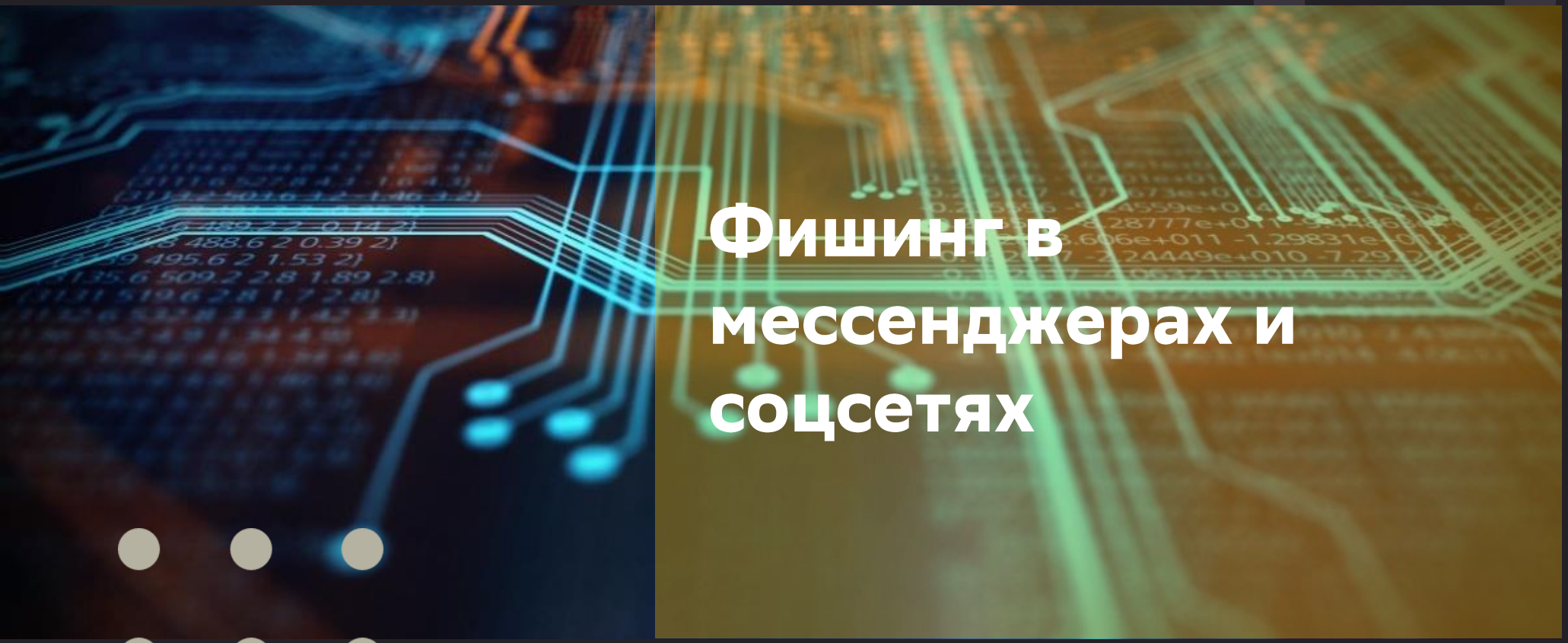
Основные правила безопасности

5 **Настороженно относитесь к ссылкам в сообщениях от незнакомых людей**

6 **Проверяйте полученные подозрительные СМС-сообщения от банка**

7 **Не доверяйте СМС-сообщениям о заражении телефона**

8 **Защищайте смартфон с помощью надежных антивирусных программ**



Фишинг в мессенджерах и соцсетях

Как мошенники используют мессенджеры

Ссылка с переходом на фишинговые сайты

1

Звонок от имени известной организации

2

Якобы выгодные акции, розыгрыши призов

3

Ничеси!

Фейковые ссылки на покупки товаров

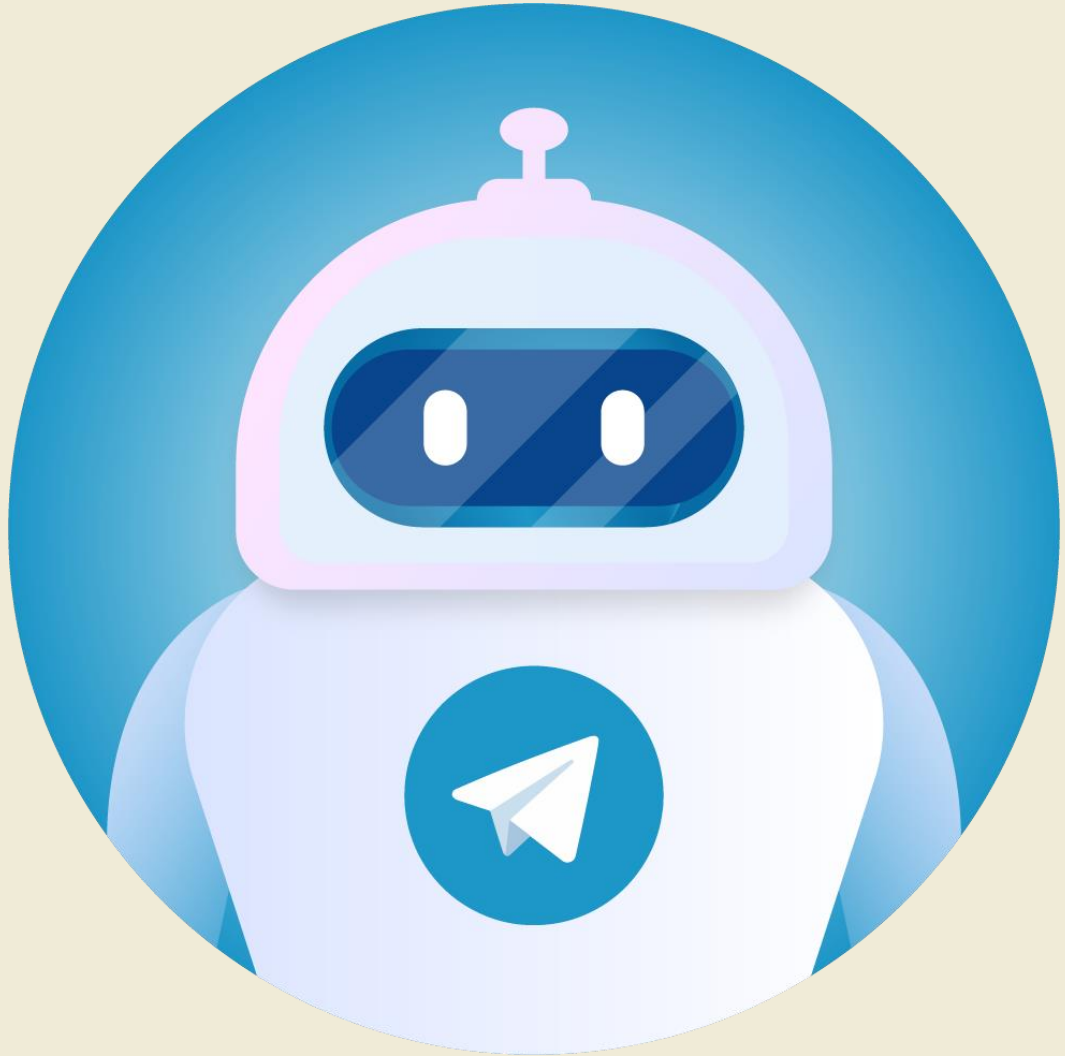
4

Боты в мошеннических схемах (особенно в Telegram)

5

Что важно знать о Telegram-ботах

Мессенджер Telegram – это технологичная платформа с огромным количеством полезных ботов, но, к сожалению, даже самые полезные боты могут использоваться в мошеннических схемах.



Как мошенники с помощью Telegram-ботов похищают деньги?

Боты позволяют создавать по заданным параметрам страницы-клоны популярных онлайн-сервисов с формой оплаты товара.

Средний чек одной кражи составляет 500-1500 рублей!

В случаях с покупками товара ущерб больше – он оценивается в десятки тысяч рублей.

Как себя обезопасить?

- Никогда не соглашайтесь на предоплату услуг и всегда проверяйте отзывы на продавцов, которые ведут свою деятельность в мессенджерах.
- Если прошли по ссылке в мессенджере – внимательно изучите адрес сайта, на который вы попали.
- Никогда не отправляйте чат-боту личную информацию по запросу, например, ваши ФИО, адрес, паспортные данные, логины и пароли от какого-либо аккаунта или номер карты.

Схемы фишинга в соцсетях

Посты с призывом о помощи

01

Просьба друга

02

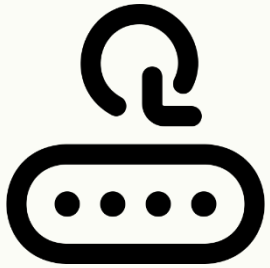
Ого, это правда!?

03

Узнай кто смотрел твой профиль?

04

Как защититься от фишинга в соцсетях



Меняйте пароли раз в три месяца

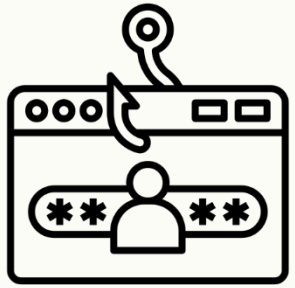
1

Не используйте одинаковые пароли

2

Подключите двухфакторную аутентификацию

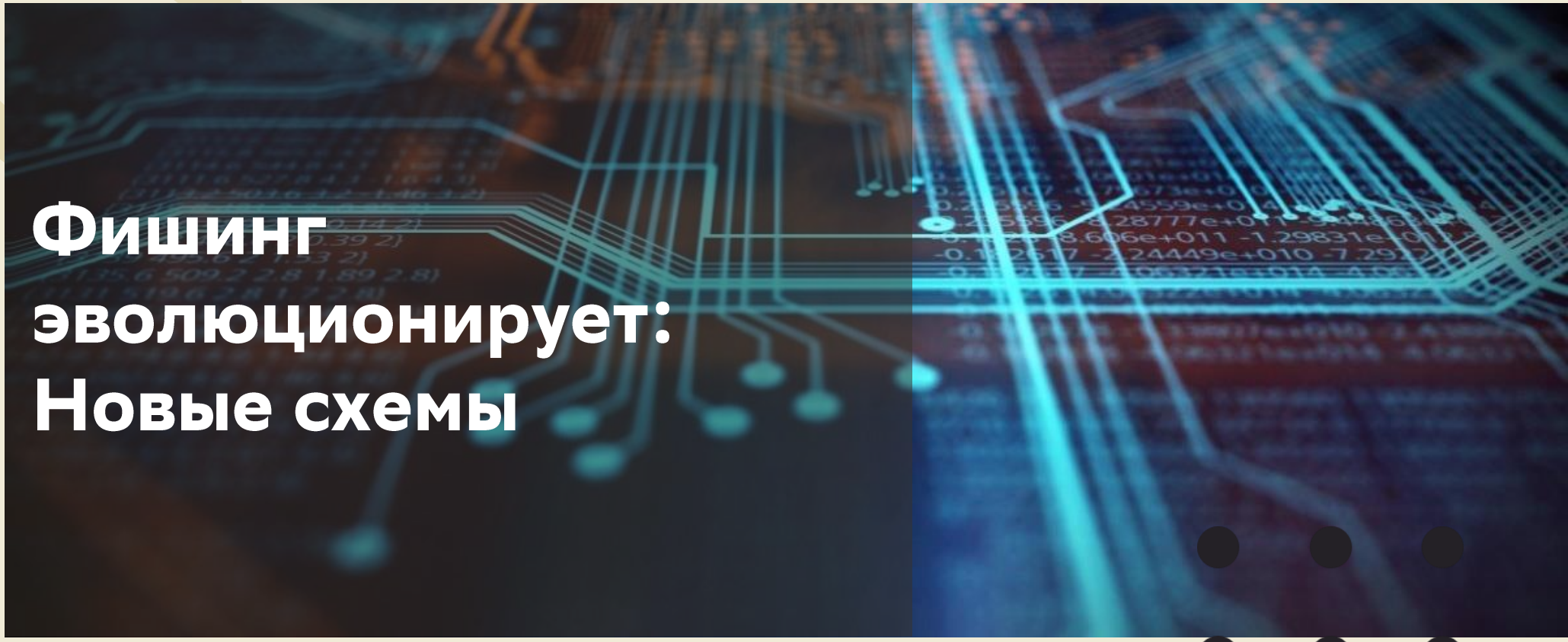
3



Не доверяйте сомнительным предложениям

4

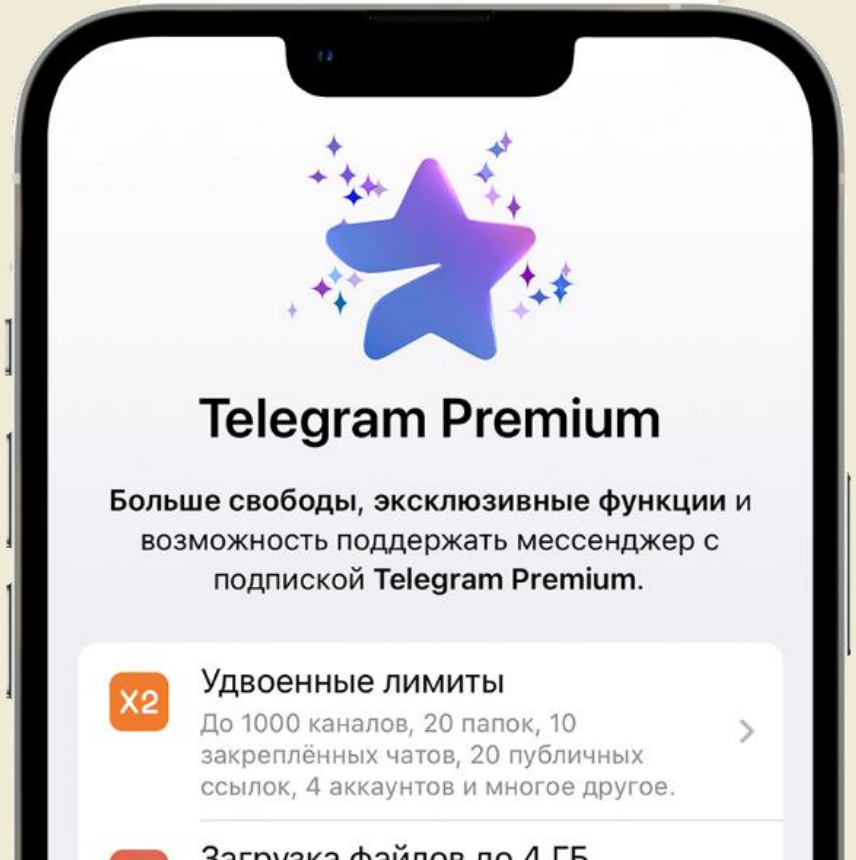
05



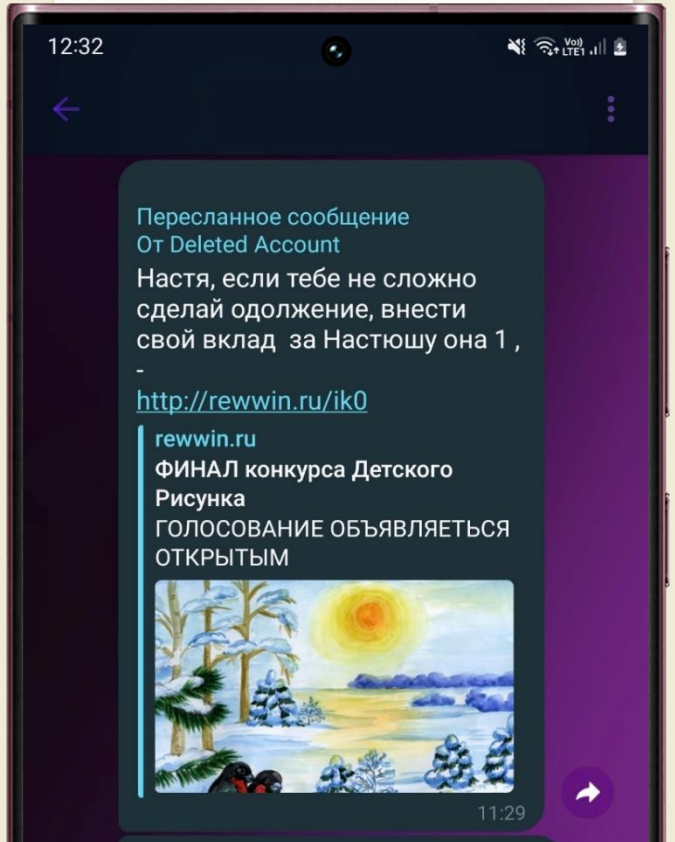
Фишинг эволюционирует: Новые схемы

Как угоняют аккаунты в «Телеграме»

Бесплатный премиум



Проголосуй, пожалуйста!



Как защитить свой аккаунт

1

Проверьте активные сеансы

Зайдите в «Настройки», выберите «Устройства», а затем «Активные сеансы». Если заметите неизвестные устройства и локации, с которых был выполнен вход, завершите на них сеансы.

2

Свяжитесь с отправителем

Не реагируйте на неожиданные просьбы прислать денег или проголосовать в конкурсе. Свяжитесь с отправителем подозрительного сообщения (по телефону или СМС) и уточните, не взломали ли его аккаунт.

3

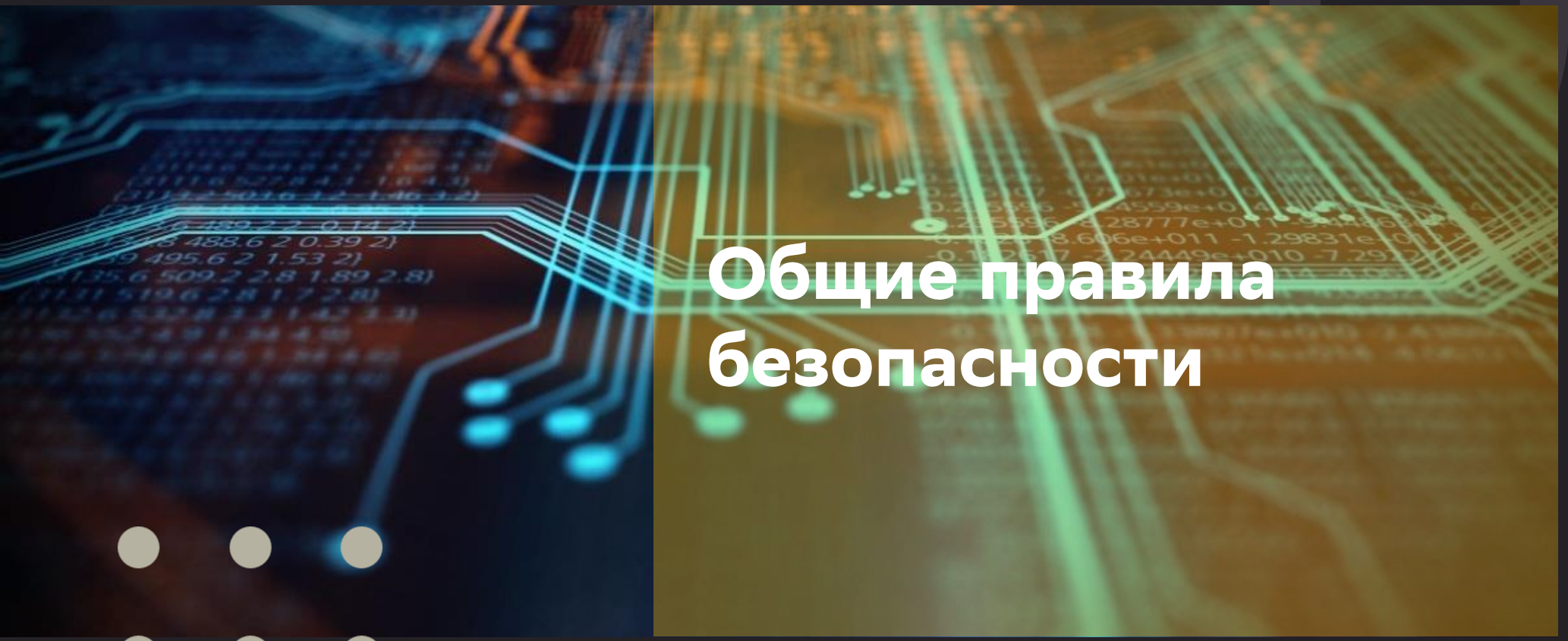
Не переходите по ссылкам

Не переходите по ссылкам, в надёжности которых не уверены, и не вводите номер телефона и одноразовый пароль для авторизации в «Телеграме» ни на каких сторонних страницах.

4

Установите двухэтапную аутентификацию

Зайдите в «Настройки», выберите «Конфиденциальность», а после — «Двухэтапная аутентификация». В этом пункте вам нужно будет задать «Облачный пароль». Он будет использоваться как дополнительный этап проверки при подключении к новому устройству.



Общие правила безопасности

Общие правила безопасности

1 **Остерегайтесь заманчивых предложений**

2 **Учитесь мыслить критически!**

3 **Не торопитесь!**

4 **Будьте бдительны! Не поддавайтесь на манипуляции мошенников**

5 **Скройте себя в мессенджерах с помощью настроек конфиденциальности**

ВАЖНО: при использовании мессенджеров есть ещё одна угроза – аккаунт могут взломать, чтобы украсть персональную информацию или рассылать сообщения от вашего имени. Чтобы этого не произошло, **установите в мессенджерах двухфакторную аутентификацию** – эта функция не позволит мошенникам взломать ваш профиль.

Что еще важно помнить

1

Никогда не принимайте поспешных решений

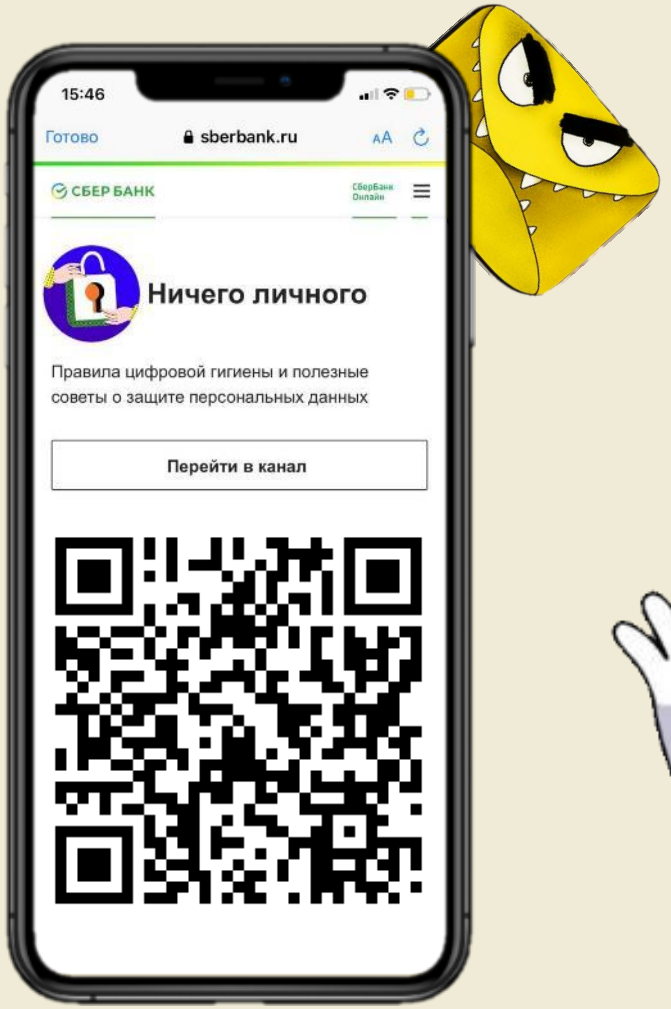
2

Всегда держите руку на пульсе

3

Проявляйте социальную ответственность

Держать руку на пульсе удобно с **каналом «Ничего личного»!**



СБЕР

ВСЕРОССИЙСКАЯ ПРОГРАММА
ДНИ ФИНАНСОВОЙ ГРАМОТНОСТИ
В УЧЕБНЫХ ЗАВЕДЕНИЯХ

DPO DATA PROTECTION OFFICE

Спасибо!