МОШЕННИКИ В ЦИФРОВОМ МИРЕ

КАК СБЕРЕЧЬ СВОИ ДЕНЬГИ?

Светлана Толкачева

Авторский курс

Толкачева Светлана

Топ-менеджер банка / Группа ВТБ
Автор учебника «Финансовая грамотность. Цифровой мир»/ (издательство «Просвещение»)
Автор YouTube и Rutube-каналов «Финансовая грамотность со Светланой Толкачевой»

ХОЧУ ЗНАТЬ БОЛЬШЕ

www.youtube.com/c/SvetlanaTolkacheva

https://rutube.ru/channel/24115490/

https://vk.com/tolkacheva_sv

ОБЩЕСТВЕННАЯ ДЕЯТЕЛЬНОСТЬ

- С 2015 года — мастер-классы по социализации и адаптации детей из интернатных учреждений по теме «Финансовая грамотность», автор и ведущая
- Член экспертного совета при Центральном банке Российской Федерации, руководитель рабочей группы по взаимодействию с образовательными организациями
- Член Наблюдательного совета Ассоциации развития финансовой грамотности
- Член Общественного совета при Департаменте образования и науки города Москвы

ОБРАЗОВАНИЕ

- 2007-2009 гг. — Бизнес-школа Университета Антверпена (UAMS) совместно с ИБДА АНХ при Правительстве РФ (Бельгия, Антверпен), executive MBA
- 2005 г. — Московский университет МВД России, кандидат юридических наук
- 2002-2003 гг. — Международная академия предпринимательства, консультант по налогам и сборам
- 1997-2002 гг. — Московский государственный социальный университет, юриспруденция
- 1995-2000 гг. — Российская экономическая академия им Г. В. Плеханова, экономика и управление на предприятии

ПРОФЕССИОНАЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

Более 19 лет работы в финансовых компаниях, включая 15 лет в банковской сфере

СОДЕРЖАНИЕ

ПРЕДПОСЫЛКИ УВЕЛИЧЕНИЯ ЧИСЛА МОШЕННИЧЕСТВ

ПРЕДПОСЫЛКИ УВЕЛИЧЕНИЯ ЧИСЛА МОШЕННИЧЕСТВ

УВЕЛИЧЕНИЕ объема финансовых транзакций

ИЗБЫТОК противоречивой информации и **РАЗНООБРАЗИЕ** видов финансовых инструментов

ВОЗМОЖНОСТИ удаленной идентификации и аутентификации

УСКОРЕНИЕ технологических процессов и **ПЕРЕХОД** сделок и операций в цифровую среду

РАЗРЫВ между знаниями о финансовых инструментах и поведением граждан, в том числе в цифровой среде

Возраст ребенка, в котором большинство родителей инициирует пользование электронными устройствами, — 3 года*

(почти половина взрослых начинает давать ребенку телефон или планшет в автомобиле)

К 4-6 годам у 54% детей есть планшет или смартфон

К 11-14 годам — уже у 97%

Банк России по итогам 2023 года ожидает роста доли безналичных операций в розничной торговле до 78-80% (77,7% по итогам сентября 2022 года)

*уточненные показатели Стратегии развития национальной платежной системы на 2021-2023 годы***

Пять лет назад на безналичные платежи приходилось всего 30%, и никто не верил, что ситуация изменится

Из выступлений председателя ЦБ РФ Э.Набиуллиной на пресс-конференции, февраль 2021

ФИНАНСОВАЯ ГРАМОТНОСТЬ БЕЗ ЗНАНИЙ О ЦИФРОВОЙ СРЕДЕ

не позволяет эффективно решать повседневные задачи

* По данным исследования «Лаборатория Касперского», представленного в марте 2019 - «Взрослые и дети в цифровом мире»

** https://cbr.ru/Content/Document/File/142336/nps_key_25112022.pdf

СТАТИСТИКА КИБЕРПРЕСТУПЛЕНИЙ

ПО ДАННЫМ СТАТИСТИКИ МВД РФ за январь-ноябрь 2022*

ОБЩИЕ СВЕДЕНИЯ О СОСТОЯНИИ ПРЕСТУПНОСТИ

	ЗАРЕГИСТРИРОВАНО (в отчетном периоде)		Из числа преступлений, дела и материалы о которых находились в производстве в отчетном периоде:	
	ВСЕГО	+,- в %	РАСКРЫТО* ВСЕГО	+,- в %
ВСЕГО ПРЕСТУПЛЕНИЙ	1823348	-1,6	953244	0,5
совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации**	470143	-4,9	128417	6,5

26 % - доля киберпреступлений

27 % - раскрыто от зарегистрированных

СТРУКТУРА

КАЖДОЕ ЧЕТВЕРТОЕ преступление – это киберпреступление

Из них:

- **БОЛЕЕ ПОЛОВИНЫ (53%) относится к категориям ТЯЖКИХ И ОСОБО ТЯЖКИХ (248 тыс.)**
- **73 % совершено с использованием СЕТИ ИНТЕРНЕТ (342 тыс.)**
- **СВЫШЕ 40 % - с помощью средств МОБИЛЬНОЙ СВЯЗИ (190 тыс.)**
- **25 % - с использованием пластиковых карт (116 тыс.)**

САМЫЕ ПОПУЛЯРНЫЕ КБ

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ)
- распространение вредоносных компьютерных программ (ст. 273 УК)
- мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК)

В феврале 2020 МВД России в структуре ведомства появились **подразделения по борьбе с киберпреступлениями**. Ранее такие подразделения создали в СК РФ

ДИНАМИКА

КОЛИЧЕСТВО КИБЕПРЕСТУПЛЕНИЙ В РОССИИ ЗА 8 ЛЕТ ВЫРОСЛО В 47 РАЗ!

2013 – 11 тыс.	2019 – 294 тыс.
2014 – 44 тыс.	2020 – 510 тыс.
2016 – 66 тыс.	2021 – 518 тыс.

* Из Отчета МВД РФ за январь-ноябрь 2022 года «Состояние преступности в России»

МОШЕННИЧЕСТВО В ЦИФРАХ

По данным ЦБ РФ *

Что лидирует. Основным инструментом злоумышленников для хищения средств остается использование приемов и методов социальной инженерии. Доля таких операций по итогам на ноябрь 2022 выросла по сравнению с аналогичным периодом прошлого года с 41 до 54%

Возраст жертв. Средний возраст жертв по мошенничеству через интернет и телефонные звонки - от 30 до 45 лет

«Средний чек» мошенника. Средняя сумма хищения, совершенного с использованием приемов и методов социальной инженерии, у граждан в 2021 году составила 11,8 тыс. руб.

Возврат похищенного. По итогам III кв. 2022 года операции без согласия клиентов составили 3,97 млрд руб. При этом кредитные организации вернули всего лишь 3,4% (за аналогичный период 2021 года – 7,7 %)

По данным МВД РФ **

Каждый седьмой россиянин в 2021 году подвергался попытке хищения денег со стороны телефонных мошенников

50% потерпевших добровольно передавали свои данные, в том числе пароли и секретные коды

* https://www.cbr.ru/analytics/ib/review_3q_2022/; https://www.cbr.ru/analytics/ib/operations_survey_2021/; https://ria.ru/20200723/1574790201.html

** https://n.tass.ru/obschestvo/13194049

СТАТИСТИКА УТЕЧЕК

• **Пресс-служба Роскомнадзора 16.12.22*:**

«С начала военной операции резко увеличилось количество утечек персональных данных - более 140 случаев, в сеть попали около 600 млн записей о гражданах. Нарушена конфиденциальность медицинских персональных данных, подлежащих особой защите. Основной источник сливов - иностранные ресурсы»

• **«Лаборатория Касперского» (декабрь, 2022)**:**

объем персональных данных россиян, попавших в сеть вследствие 10 самых крупных утечек 2022 года - более 1,5 млрд записей

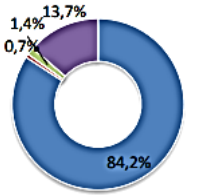
• **Экспертно-аналитический центр ГК InfoWatch (отчет за I полугодие 2022)***:**

рост утечек в России в 1,5 раза по сравнению с 1-м полугодием 2021 года – 305 инцидентов

РАСПРЕДЕЛЕНИЕ УТЕЧЕК В РФ***

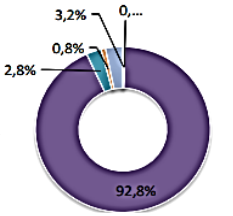
По типу данных:

- Персональные данные – 84,2 %
- Платежная информация – 0,7 %
- Государственная тайна – 1,4 %
- Коммерческая тайна, ноу-хау – 13,7 %



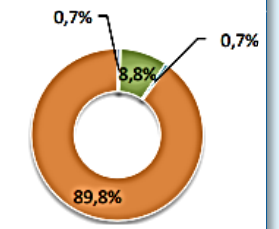
По каналам утечек:

- Сеть (браузер, Cloud) – 92,8 %
- IM (Instant messaging) - службы мгновенных сообщений: текст, голос, видео) – 3,2 %
- Электронная почта – 2,8 %
- Прочее (моб.устройства, съемные носители) – 1,2%



По виновникам:

- 89,8% - хакеры
- 8,8 % - непривилегированные сотрудники



• **Громкие утечки персональных данных в России в 2022 году:**

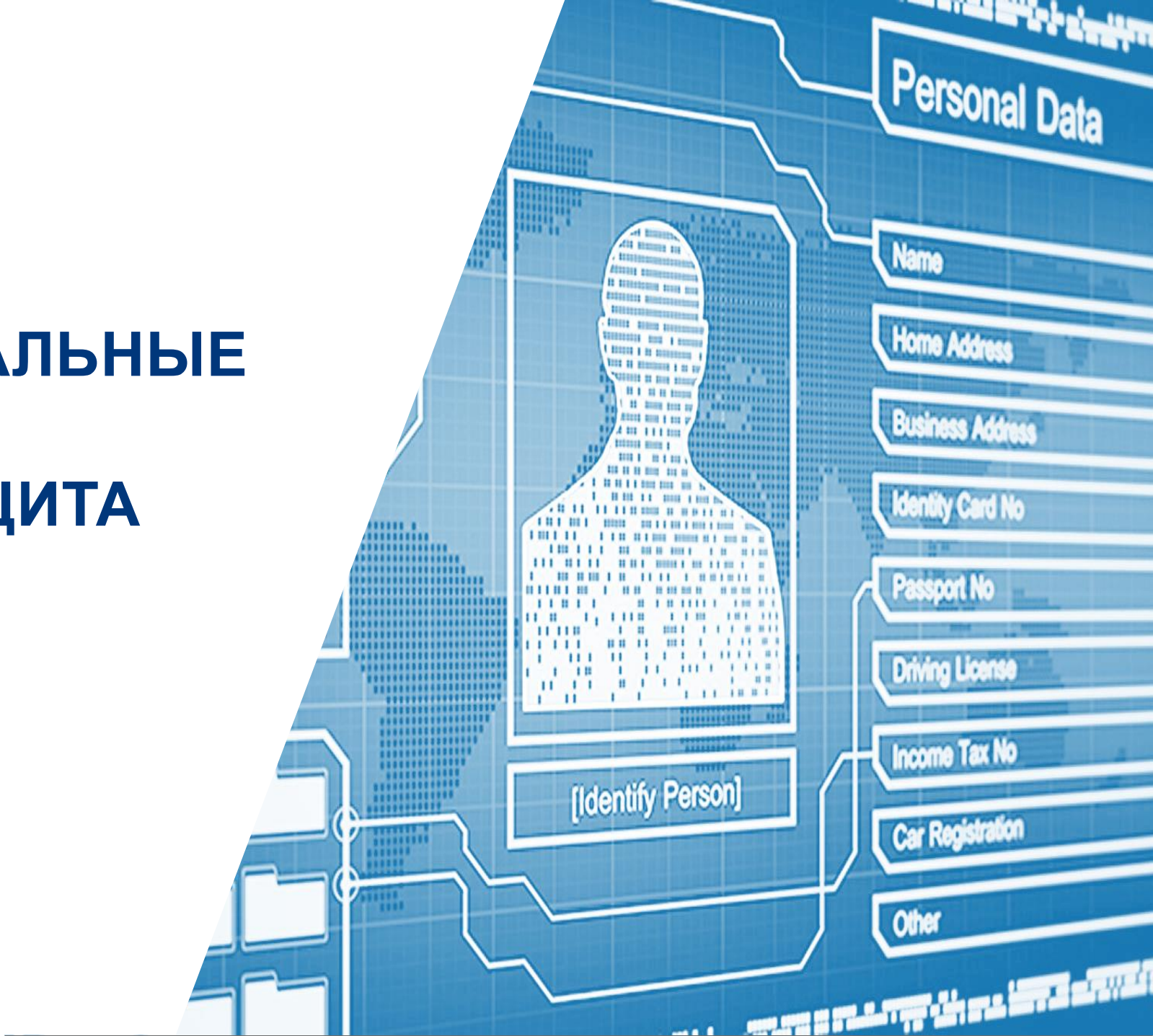
перевозчики («Победа», Utair, AzurAir, Мосгортранс, РЖД); сервисы продажи билетов (OneTwoTrip, tutu.ru); операторы связи (Ростелеком, Билайн,Tele2, Дом.ру); банки (Сбер, Совкомбанк); онлайн-магазины и службы доставки (Wildberries, Спортмастер, Яндекс.Еда, DNS, Ozon, СДЭК, Почта России); онлайн-кинотеатры и видеохостинги (START, Yappi); служба заказа такси «Ситимобил»; медицинские центры («Гемотест», клиника «Здоровье») и др.

* https://tass.ru/obschestvo/16611425

** https://csn-tv.ru/posts/id141248-v-laboratorii-kasperskogo-ocenili-masshtab-utechek-personalnykh-dannykh-rossiyan-za-2022-god

*** Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года. Экспертно-аналитический центр InfoWatch. 2022 г. https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf

ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ИХ ЗАЩИТА



ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПДн)

Защита информации о личности граждан обеспечивается Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»

- **Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физлицу - **субъекту ПДн**.

- **Закон не содержит конкретного перечня.** Это набор данных, неразрывно связанный с личностью и позволяющий ее идентифицировать.

- **Оператор ПДн** – лицо*, обрабатывающее ПДн, предварительно определив их состав, цели и действия с ними (реестр операторов на сайте Роскомнадзора).

КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

- **ОБЩЕДОСТУПНЫЕ***** (ФИО, год и место рождения, адрес, абонентский номер, профессия, образование…)
- **СПЕЦИАЛЬНЫЕ** (раса, национальность, политические взгляды, религиозные убеждения, состояние здоровья, интимная жизнь, судимость)
- **БИОМЕТРИЧЕСКИЕ** (сведения о физиологических и биологических особенностях человека именно с целью его идентификации (не анализ крови)
- **ИНЫЕ** (не входят в др. категории - корпоративные данные, геолокация…)

ОПЕРАТОР ОБЯЗАН ОБЕСПЕЧИВАТЬ СТЕПЕНЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО КАТЕГОРЯМ

* Государственный, муниципальный орган, юридическое или физическое лицо. Оператор имеет право, с согласия гражданина, поручить обработку др.лицу - обработчику

** При обработке ПДн в информационных системах - 4 уровня защищенности ПДн (в зависимости от категории ПДн, количества субъектов ПДн (менее или более 100 тыс.), формы отношений (работники или клиенты) и типа угроз для ПО).

*** Могут включатся в общедоступные источники (справочники, адресные книги) с согласия субъекта ПДн. Данные, которые можно найти в интернете общедоступными не являются (размещенные субъектом ПДн в открытых источниках обрабатывать, распространять без согласия нельзя).

ЗАКОНОДАТЕЛЬНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

КОНФИДЕНЦИАЛЬНОСТЬ ПДн (ст.7 № 152-ФЗ)

«Операторы ПДн обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн»*

Согласие можно отозвать

▲ **Согласие на обработку ПДн**

- Раскрытие определенному кругу лиц
- Обработка целевого ограниченного набора ПДн (с 01.09.22 цели должны быть предметны и однозначны) По достижении целей ПДн уничтожаются

▲ **Согласие на обработку ПДн для распространения**

- Оформляется отдельно с 2021 г.
- Раскрытие ПДн неопределенному кругу лиц
- Выбор ПДн по каждой категории
- Молчание субъекта ПДн не означает его согласие

Операторы персональных данных несут ответственность за их сохранность – законом предусмотрена административная, уголовная и другие виды ответственности**

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения

Я, Анастасия Васильевна Цветкова, даю свое согласие АО «Ромашка» на распространение моих персональных данных с целью размещения их на официальном сайте АО «Ромашка» согласно ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Перечень устанавливаемых условий и запретов	Дополнительные условия
Общие персональные данные	фамилия	да		
	имя	да		
	отчество	да		
	год рождения	да	ДА/НЕТ	
	месяц рождения	да		
	дата рождения	да		
	место рождения	нет		
	адрес	нет		только сотрудникам АО «Ромашка»
	семейное положение	нет		
	образование	нет		только сотрудникам отдела кадров
	профессия	да		
Специальные категории персональных данных	состояние здоровья	нет		только сотрудникам отдела кадров
Биометрические персональные данные	цветное цифровое фотографическое изображение лица	нет		
Перечень устанавливаемых условий и запретов				

Сведения об информационных ресурсах оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
https://www.romashka.ru	Предоставление сведений неограниченному кругу лиц

Срок действия согласия — с 01.10.2021 по 01.10.2025.

Оставляю за собой право потребовать прекратить распространять мои персональные данные в течение трех рабочих дней с момента получения требования.

1 октября 2021 года _____ А.В. Цветкова

Контур Школа

* Конкретной формы согласия нет, есть обязательные требования в приказе Роскомнадзора

** Обработка ПДн без согласия гражданина или с нарушением требований к составу сведений, включаемых в согласие, грозит штрафом в размере: для граждан – 6 000–10 000 руб.; для должностных лиц — 20 000–40 000 руб.; для юрлиц — 30 000–150 000 руб. При повторном нарушении: для граждан — 10 000–20 000 руб.; для должностных лиц — 40 000–100 000 руб.; для ИП — 100 000–300 000 руб.; для юрлиц — 300 000–500 000 руб. С 1 сентября 2022 устанавливается административная ответственность за отказ потребителю в заключении договора из-за непредоставления ПДн. Штраф за нарушение для ИП и юрлиц составит от 30 до 50 тыс. руб. (Федеральный закон от 28.05.2022 № 145-ФЗ).

ТОП-5 ВОПРОСОВ О ПЕРСОНАЛЬНЫХ ДАННЫХ

	ВОПРОС	ОТВЕТ
1	Что делать, если обнаружил в интернете незаконно размещенные ПДн о себе?	Направить собственнику ресурса требование удалить ПДн. При отсутствии реакции - обращение в суд с требованием защиты ваших прав как субъекта ПДн. После вступления решения суда в силу - обращение в Роскомнадзор для внесения данных в автоматизированный Реестр нарушителей прав субъектов ПДн, запускающий процедуру устранения нарушения вплоть до блокировки ресурса.
2	В какие сроки оператор должен прекратить обработку и распространение моих ПДн по направленному мной требованию?	В течение 10 рабочих дней с даты получения требования прекратить обработку, 3 рабочих дней - распространение. Также при отзыве согласия на обработку ПДн в срок не более 30 дней они должны быть уничтожены.
3	Как узнавать о компрометации моих ПДн, если компания не огласит факт утечки?	С 01.03.2023 г. операторы ПДн обязаны в течение 24 часов сообщить в Роскомнадзор об инцидентах с утечками ПДн и в течение 72 часов отчитаться о результатах внутреннего расследования. Но важно самому верифицировать текущую ситуацию с ПДн – регулярно запрашивать кредитную историю в БКИ, проверять информацию в ЛК ФНС и др. значимых ресурсах, включая браузеры на предмет подключения чужих устройств к аккаунту и пр.
4	Что делать, если продавец отказывает в необходимой мне услуге из-за моего нежелания предоставить ПДн?	С 01.09.2022 г. установлены штрафы за отказ потребителю в заключении договора из-за непредоставления ПДн, включая биометрические ПДн, кроме случаев, если ПДн обязательны по законодательным требованиям или непосредственно нужны для исполнения условий договора. При избыточных требованиях можно жаловаться на отказ в Роскомнадзор.
5	Зачем сайты предупреждают об использовании файлов cookie и запрашивают согласие пользователя?	Cookie – текстовые файлы на вашем устройстве со служебной информацией браузера (личные данные – имя, логин и пр.; поведение на сайте - корзина товаров, геолокация и пр.; индивидуальные настройки и др.). Отсутствие предупреждения не означает отключение cookie. Есть судебная практика, определяющая Cookie как ПДн.

НАДЕЖНЫЙ ПАРОЛЬ

Исследование компании-разработчика менеджера паролей NordPass*

Эксперты оценили базу данных паролей, попавших в открытый доступ в 2021 году (4 ТБ), в 50 странах.

Россия в 2021 году заняла 1-ое место в мире по числу утечек паролей на душу населения (разрыв со 2 местом в 3 раза): почти 20 утечек на человека, общее количество — 2,9 млрд.

Самый распространенный пароль в мире «123456» - его используют более 100 млн пользователей**

123456 – 103,1 млн использований
123456789 – 46 млн;
12345 – 33 млн;
qwerty – 22,3 млн;
password – 20,9 млн;
12345678 – 14,7 млн;
111111 – 13,3 млн;
123123 – 10,2 млн;
1234567890 – 9,6 млн;
1234567 – 9,3 млн.

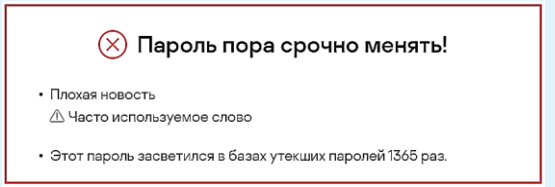
Первые 10 паролей из списка самых взламываемых использовались почти 300 млн раз

Время взлома для паролей «123456», «пароль» и «qwerty» - не более 1 секунды

Проверяем надежность пароля по мере его усложнения на сервисе или аналогичном

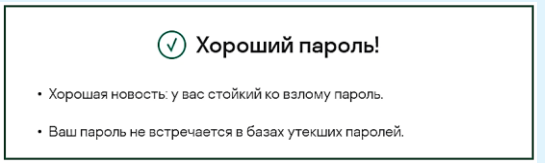
kaspersky password checker

sveta1988



SvetiK1988

$1v9e8t8iK_1988



- Очень важна длина пароля (12 символов, 8 – это минимум)
- Смена пароля – раз в 90 дней
- Для разных сервисов – разные пароли (можно добавлять к одному паролю отличительные для сервиса буквы и символы – Vk, Ok)
- Пароль аккаунта основной электронной почты должен принципиально отличаться - это «мастер-ключ» для остальных сервисов
- Сложный пароль тоже должен быть запоминаемым. В помощь - мнемотехники или своя система запоминания, например, усложнение на базе фраз, что-то для вас значащих
- Можно использовать менеджер паролей – выбирайте по надежности на основе рейтингов

Менеджер паролей – программа-сейф для хранения (дополнительно – для генерации) паролей и логинов от учетных записей для безопасной авторизации в Интернете. Необходимо запомнить только один сложный «Мастер-пароль».

Важно, где МП хранит пароли – на ваших устройствах или на веб-сайтах провайдеров. Второй вариант имеет плюсы – мобильность и низкий риск потери путем кражи и повреждения устройства, но нужно доверие к хостингу сайта.

* https://nordpass.com/most-common-passwords-list/

** самые популярные пароли-2021 у россиян - qwerty123, qwerty1, 123456, кириллические - «йцукен», «пароль», «любовь», «привет» (https://dlbi.ru/five-billion-password-2021/)

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Двухфакторная аутентификация (2FA) или «Подтверждение входа» - способ идентификации пользователя для входа в сервис, при котором нужно двумя разными способами подтвердить, что вы владелец аккаунта - система двух ключей.

Требуется иметь два не связанных между собой типа идентификационных данных из трех возможных:

1 фактор

То, что вы знаете

Логин и пароль

Риск – надежный пароль спасает при хакинге, но есть другие риски копроментации (при переходе по фишинговой ссылке, установке вредоносного приложения на устройство, утечке паролей из внешних баз данных и пр.)

2 фактор

То, чем вы владеете

Токен, смартфон, карта, др. устройства

Чаще используют 2FA путем получения одноразовых кодов:

- смс-аутентификация с помощью смартфона или коды по e-mail (наиболее уязвимый вариант)
- через приложения-аутентификаторы
- через аппаратные генераторы паролей (лучшая защита)

Риск - использование одного устройства и для входа в аккаунт и для получения одноразового пароля.

То, что является частью вас

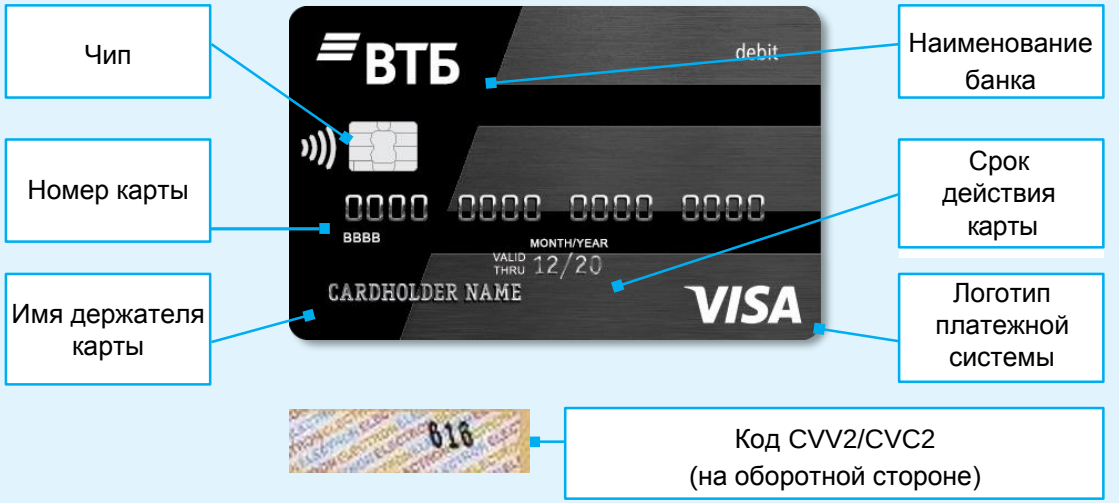
Биометрия. Отпечатки пальцев, геометрия кисти руки, очертания и размеры лица, характеристики голоса, узор радужной оболочки и сетчатки глаз, рисунок вен пальцев.

Недостатки – нет широкого распространения (кроме смартфонов). Перспективно в будущем с доработкой точности идентификации и сохранности данных.

НАДЕЖНЫЙ ПАРОЛЬ + ВВЕДЕНИЕ ДОПОЛНИТЕЛЬНОГО УРОВНЯ БЕЗОПАСНОСТИ В ВИДЕ 2FA ОБЕСПЕЧИВАЕТ СЕГОДНЯ САМУЮ ЭФФЕКТИВНУЮ ЗАЩИТУ АККАУНТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

*Иллюстрация: securitylab.ru

ОСНОВНЫЕ ЭЛЕМЕНТЫ ПЛАСТИКОВОЙ КАРТЫ



1-6-цифры – BIN (банковский идентификационный номер):

1 - код платежной системы: **2** – МИР, **4** – Visa, **5** – Mastercard

2-6 - банковский идентификатор

7-8 цифры – код продукта

9-предпоследняя цифры – индивидуальный номер клиента

Последняя цифра – проверочное число (с помощью специального алгоритма можно проверить достоверность номера)

ПИН-код — четырехзначный секретный код, необходимый для совершения операций в банкоматах/магазинах

Код CVV2/CVC2 — трехзначный код на оборотной стороне карты для идентификации при совершении интернет-транзакций

- **Храните карту отдельно от ПИН-кода**
- **Никому не сообщайте свой ПИН и CVV-коды**
- **Всегда прикрывайте клавиатуру при вводе ПИН-кода**
- **При потере карты сразу звоните в call-центр банка для её блокировки**
- **Никогда и никому не передавайте карту**
- **Используйте двухфакторную аутентификацию во время платежа онлайн — 3D Secure**
  (перенаправление пользователя на страницу банка-эмитента для ввода одноразового кода, полученного по SMS на привязанный к карте телефон)
- **Используйте мобильные приложения с технологиями для бесконтактной оплаты (NFC)**
- **Рассмотрите целесообразность страхования от мошенников**

  Возможный набор покрываемых рисков:
  - несанкционированное снятие денег со счета, в т.ч. в результате скимминга или фишинга
  - хищение наличных, снятых в банкомате в результате грабежа или разбойного нападения
  - утрата карты вследствие неисправной работы банкомата, размагничивания, утери и т.п

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ В ЦИФРОВОМ МИРЕ

ИДЕНТИФИКАЦИЯ — КОМУ И ЗАЧЕМ НУЖНА?

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ
(в государственных и частных системах)

набор данных клиента, используемых системой для его идентификации

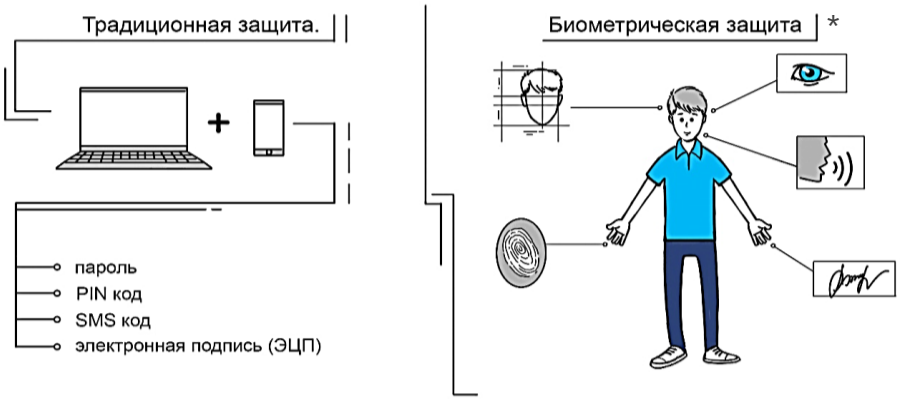
ЦИФРОВЫЕ КОММУНИКАЦИИ
(публичные и частные)

обмен информацией между устройствами через Интернет

ЦИФРОВЫЕ РАСЧЕТЫ
(счета/карты/электронные кошельки)

система безналичных расчетов между контрагентами

ЭЛЕКТРОННАЯ ПОДПИСЬ (ЭП, ранее ЭЦП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения подписывающего информацию (№ 63-ФЗ «Об электронной подписи» от 06.04.2011)



ПЕРСОНАЛЬНЫЕ ДАННЫЕ НИКОМУ НЕЛЬЗЯ ПЕРЕДАВАТЬ!

СОЧЕТАНИЕ ДВУХ ВИДОВ ЗАЩИТЫ ОБЕСПЕЧИВАЕТ ЕЕ БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ!**

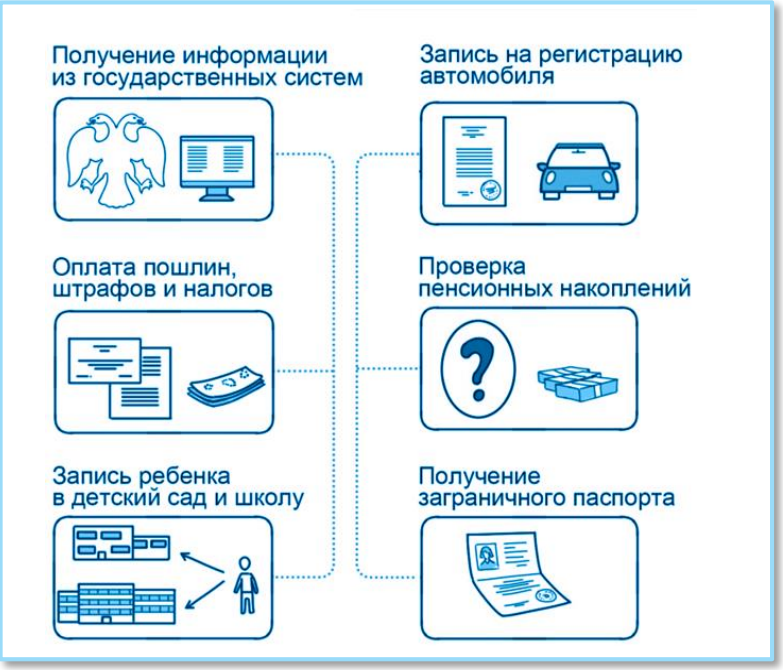
* С 30 июня 2018 года в силу вступил закон об удаленной биометрической идентификации граждан - № 482-ФЗ от 31 декабря 2017 г. «О внесении изменений в отдельные законодательные акты Российской Федерации». Рассмотрение законопроекта об обязательном сборе биометрических данных отложено. С 30.12.2021 подписан закон о создании единой государственной биометрической системы и ЕБС переведена в статус ГИС (государственных информационных систем).

** С 1 февраля 2023 года у граждан появится возможность аутентификации в ЕСИА с использованием ЕБС для доступа на единый портал госуслуг (ЕПГУ) - Постановление Правительства РФ от 21.10.22 № 1879 (первый фактор аутентификации – логин/пароль или биометрия, второй фактор – код sms). При этом с 14.05.22 (ПП № 875) физ. и юр.лицам предоставлено право на 2FA в ЕСИА с использованием биометрии пока в качестве второго фактора наряду с sms по выбору.

ЕСИА И ЕБС. ГРАЖДАНИН И ГОСУДАРСТВО

НА ЧТО НАПРАВЛЕН ЗАКОН ОБ УДАЛЕННОЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ГРАЖДАН?

НА УСТАНОВЛЕНИЕ ПОРЯДКА ПРОВЕДЕНИЯ ПОЛНОЙ УНИВЕРСАЛЬНОЙ УДАЛЕННОЙ ИДЕНТИФИКАЦИИ



ПОСРЕДСТВОМ:

ЕСИА

Доступ граждан к электронным услугам государства по системе «один пароль – доступ ко всем государственным сайтам»

Получение учётной записи ЕСИА – при удостоверении своей личности в многофункциональном центре госуслуг с помощью паспортных данных, ИНН и СНИЛС (www.gosuslugi.ru)

Оператор - Минцифры

ЕБС

Хранение БКШ (биометрических контрольных шаблонов - биометрических персональных данных физических лиц: изображение лица и голос)

Получение БКШ - банками при проведении идентификации при личном присутствии лица

Оператор - Ростелеком

ГЛАВНОЕ ПРЕИМУЩЕСТВО — ВОЗМОЖНОСТЬ ПОЛУЧАТЬ И ОФОРМЛЯТЬ УСЛУГИ ОНЛАЙН

* С переводом с 30.12.2021 ЕБС в статус ГИС порядок функционирования утверждает Правительство РФ. Обязательная аккредитация для госорганов, использующих ЕБС и иные ГИС. Граждане с 01.09.22 имеют право на саморегистрацию в ЕБС через приложение, разработанное АО «Ростелеком».
24.11.22 в 1-м чтении ГД принят законопроект о запрете сбора и хранения биометрии граждан коммерческими организациями.

ЕСИА И ЕБС. ЦИФРОВОЙ ПРОФИЛЬ

ЦИФРОВОЙ ПРОФИЛЬ ГРАЖДАНИНА (ЦП)

ЦП – совокупность:

- ✓ **всех данных о гражданине** (в распоряжении госорганов и ГИС*)
- ✓ **технических средств для управления** этими данными

ПРОЦЕСС ВНЕДРЕНИЯ ЦП

ЭКСПЕРИМЕНТ ПО ЗАПУСКУ ЦП**

В мае 2020 Минцифры совместно с ЦБ РФ запущен в эксплуатацию сервис, позволяющий гражданам через ЛК ЕСИА дистанционно получать сведения о себе из ГИС, и с помощью «платформы согласий» регулировать доступ к ним тех или иных организаций для получения от них финансовых услуг в цифровом виде

УЧАСТНИКИ ПИЛОТНОГО ПРОЕКТА

- Кредитные, страховые организации, МФО и операторы финансовых платформ - по согласованию с ЦБ
- Операторы связи, работодатели - юрлица, с которыми физлица, ищущие работу, планируют вступить в трудовые отношения - по согласованию с Минцифры
- Планируется доступ НПФ, профучастников рынка ценных бумаг, УК, операторов инвестплатформ, БКИ, АСВ, операторов информационных систем и обмена ЦФА

СВЕДЕНИЯ В ЦП

- На текущий момент в ЦП содержатся записи 38 типов (паспорт, адрес, ИНН, водительские права, электронная трудовая книжка и др.)
- На конец 2022 г. гражданами дано более 23 млн согласий

КОГДА ПРИМУТ ЗАКОН?

В январе 2022 законопроект отклонен Государственной думой***. Эксперимент продлен до конца 2023 года.

В будущем цифровой профиль станет универсальным инструментом удаленного взаимодействия между гражданами, государством и компаниями

* Государственные информационные системы

** В соответствии с постановлениями Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах», изменения от 27 марта, 24 ноября 2020 г., 16 апреля, 17 августа 2021 г., 9 декабря 2022 г.

*** Законопроект № 747513-7 "О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации) https://sozd.duma.gov.ru/bill/747513-7

КАКИМ БУДЕТ ПАСПОРТ ГРАЖДАНИНА?

УДОСТОВЕРЕНИЕ ЛИЧНОСТИ ГРАЖДАНИНА РФ НОВОГО ОБРАЗЦА
с расширенными функциями - на пластиковом носителе с чипом на базе технологии NFC

- **На пластике** - фотография владельца и персональные данные
- **На чипе** – ИНН, СНИЛС, водительское удостоверение, полис ОМС, несколько вариантов фотографий в разных ракурсах, отпечатки пальцев, снимок радужки глаз (точный перечень цифровых данных должно утвердить правительство)
- **Срок действия** – 10 лет
- **Карта снабжена** голографическим изображением, имеет российскую криптографию, QR-код
- **При потере** возможна блокировка

Постепенный процесс перехода на новый паспорт:

- с 2025 года - выдача только электронных паспортов
- к 2028 году – полный переход
- с 2030 года - прекращение хождения бумажных паспортов

Получение в первую очередь:

- при выдаче паспорта при достижении ребенком 14 лет;
- при очередной (плановой) замене в 20 и 45 лет;
- при замене паспорта ввиду утраты, повреждения и т.д.

Дополнение к пластиковой карте - **ПРИЛОЖЕНИЕ «МОБИЛЬНЫЙ ИНДЕНТИФИКАТОР ГРАЖДАНИНА»** (разработчик – Минкомсвязи)

Запланированный в начале 2023 года запуск эксперимента по переходу на электронные паспорта в пилотных зонах Москвы, Московской области и Республике Татарстан на текущий момент заморожен.

- *Не будет использоваться для значимых с юридической точки зрения услуг (продажа квартиры и т.п.)*
- *Авторизация гражданина в приложении проходит в пилотном МФЦ с получением специального QR-кода*

МОШЕННИКИ В СЕТИ
И В РЕАЛЬНОМ МИРЕ

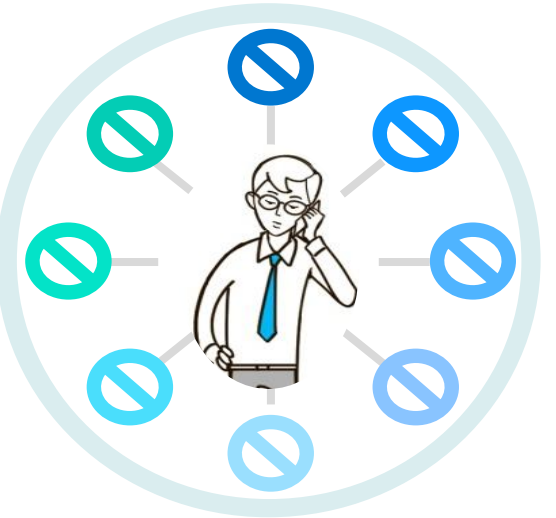
ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО И IP-ТЕЛЕФОНИЯ

Звонки с целью кражи ваших средств, выманивания реквизитов банковских карт и одноразовых паролей

✓ **звонки по размещенным объявлениям** о продаже личного имущество через сайты «Авито», «Юла» якобы для приобретения товара

✓ **Звонки из социальных служб** (мошенники сообщают о необходимости получить материальные компенсации за неиспользованные льготы; могут попросить сделать якобы возвратный «идентификационный» платеж)

✓ **звонки с номеров телефонов банка** (мошенники представляются работниками службы безопасности банка и сообщают клиенту о якобы проведенных операциях по его карте и необходимости их отмены)



✓ **звонки из налоговой** (мошенники представляются работниками налоговых служб и предлагают вернуть НДС, ссылаясь на фейковое постановление о праве на получение денежной компенсации затрат на оплату товаров иностранного производства, и просят оплатить ряд услуг: консультацию юриста, заполнение анкеты и др.)

✓ **звонки от «представителя сотового оператора»** (мошенники предлагают перерегистрировать SIM-карту, пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного списываются деньги)

❖ **МОШЕННИЧЕСТВО ЧЕРЕЗ IP-ТЕЛЕФОНИЮ*: номера мошенников могут отражаться как номера телефонов банка или любого номера из вашей телефонной книжки**

РАБОТАЕТ ТОЛЬКО НА ВХОДЯЩИЕ ЗВОНКИ - ЧТОБЫ РАЗВЕЯТЬ СОМНЕНИЯ, НУЖНО ПЕРЕЗВОНИТЬ

❖ **СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИНФОРМАЦИЮ О БАНКОВСКИХ СЧЕТАХ И КАРТАХ, А ТАКЖЕ КОНТАКТЫ РОДНЫХ И БЛИЗКИХ ЛЮДЕЙ НЕЛЬЗЯ ПРЕДОСТАВЛЯТЬ НИКОМУ!**

** С 01.12.21 в силу вступили изменения в закон "О связи". Операторы обязан прекратить оказание услуг связи и услуг по пропуску трафика при обнаружении исходящего звонка или сообщения с сети иностранного оператора соединения под российским номером, если вызывающий абонент не клиент российского оператора, находящийся за рубежом. Также услуга не может быть оказана при отсутствии у соединяющего оператора абонентского номера или идентификационного кода звонящего. Банки отмечают, что закон по блокировке звонков из-за рубежа в Россию с подменных городских номеров, операторами, не исполняется – последние ссылаются на то, что блокирующий сервис должен быть как у оператора, принимающего звонки, так и у оператора – инициатора звонка. Однако операторы других стран не обязаны соблюдать эти требования.

SMS-МОШЕННИЧЕСТВО

Напоминаем о необходимости погасить задолженность по кредиту. Ц.Б.Р.Ф. Информация 8 800 XXX XX XX

Оплата на сайте Ozon.ru на сумму 3500 руб. успешно зарезервирована. Если не совершали операцию, необходимо перезвонить по номеру 8800-511-51-36

Ваша карта заблокирована в целях безопасности. Для уточнения информации необходимо перезвонить по определившемуся номеру. +79961763523

Поздравляем!!! Пополнение Вашего телефона через карты Visa, MasterCard вошел в число призовых! Вы выиграли 100000 руб.! Информация по тел. 8-800-511-3725 или Giperkassa.ru

Рассылка SMS-сообщений с указанием номера телефона для обратной связи

Рассылка SMS-сообщений, нацеленная на вынуждение жертвы перевести деньги на счета и телефоны мошенников

Мама, пополни счет на этот номер на 1000 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!

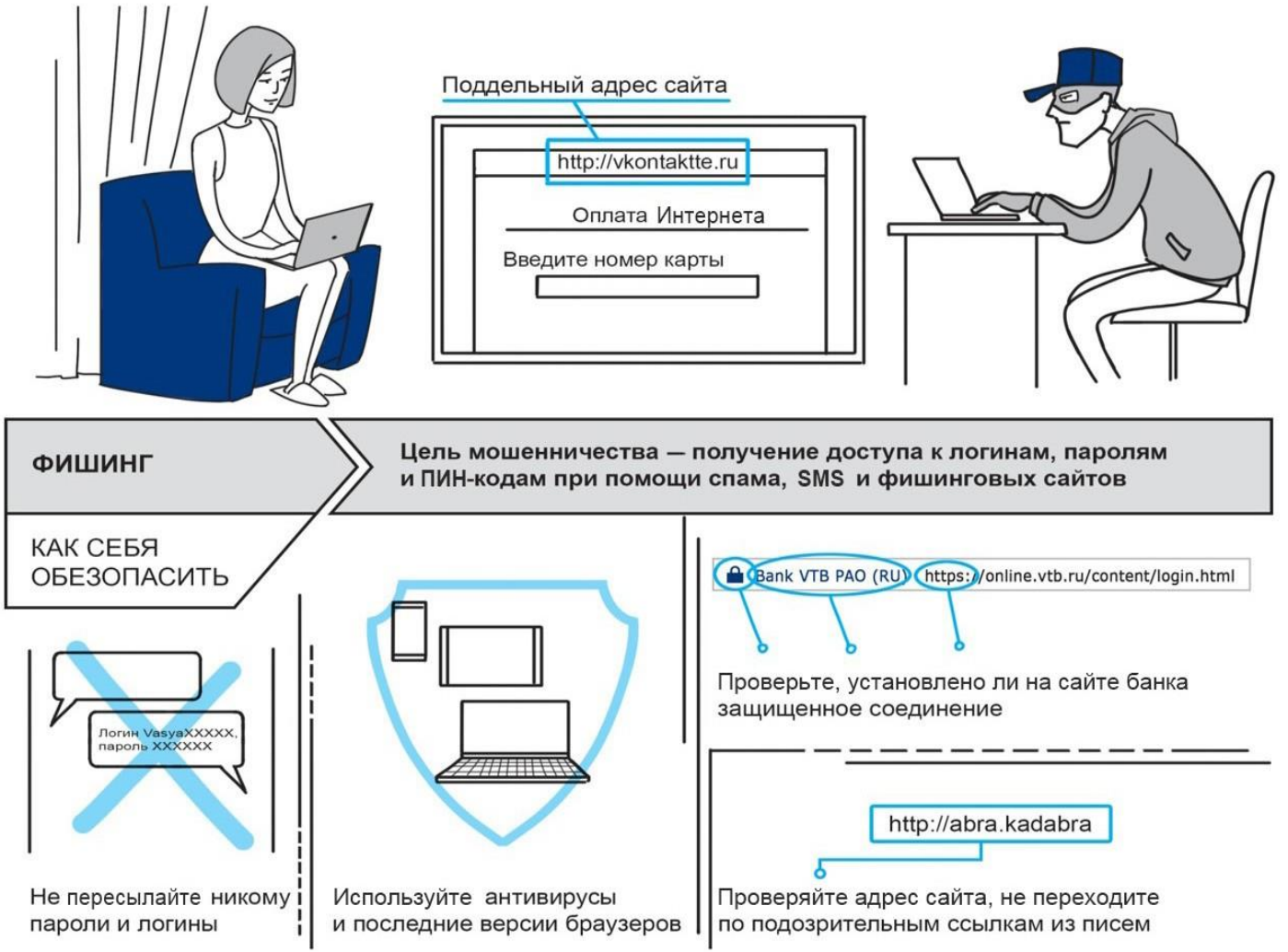
Извините, по ошибке положила вам 500 руб. Прошу вернуть на этот номер

Чтобы перейти на более выгодный тариф, отправьте смс на короткий номер XXXX

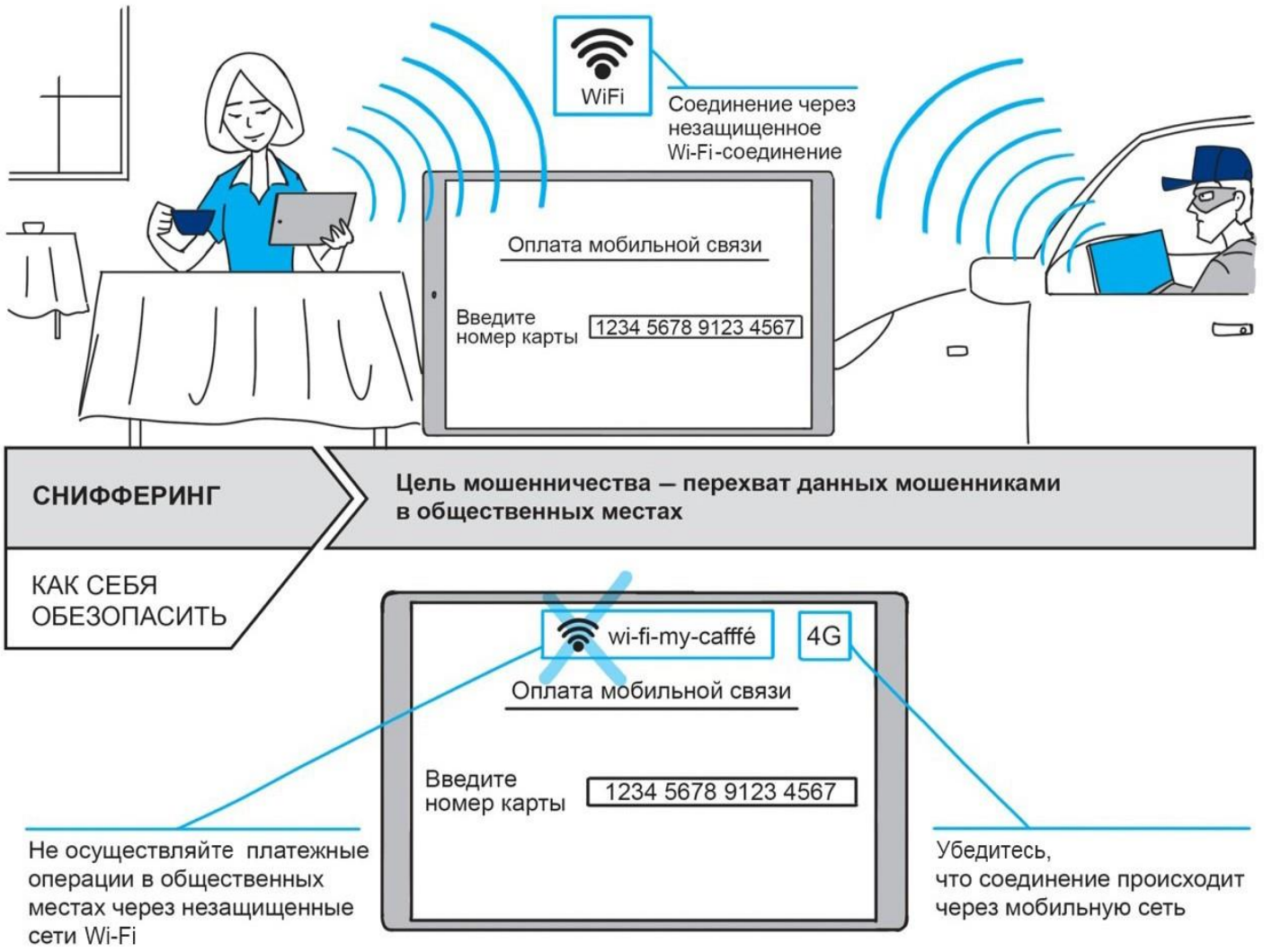
Иванова Ирина Викторовна. Согласно геолокации, вами был нарушен режим карантина согласно ст. 20.6.1 КоАП РФ. Вам необходимо оплатить штраф согласно постановлению ФСИН №168-322 от 09-04-2020года в размере 4000 рублей на номер 8 800 XXX XX XX

- НЕ ПЕРЕЗВАНИВАЙТЕ ПО ТЕЛЕФОНАМ, УКАЗАННЫМ В SMS, И НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ SMS
- НЕ ОТПРАВЛЯЙТЕ ОТВЕТНЫЕ СООБЩЕНИЯ — ЭТО РИСК ПОДПИСАТЬСЯ НА ПЛАТНУЮ УСЛУГУ

ФИШИНГ


Поддельный адрес сайта
http://vkontaktte.ru
Оплата Интернета
Введите номер карты
ФИШИНГ
Цель мошенничества — получение доступа к логинам, паролям и ПИН-кодам при помощи спама, SMS и фишинговых сайтов
КАК СЕБЯ ОБЕЗОПАСИТЬ
Логин VasyaXXXXX, пароль XXXXXX
Не пересылайте никому пароли и логины
Используйте антивирусы и последние версии браузеров
Bank VTB PAO (RU)
https://online.vtb.ru/content/login.html
Проверьте, установлено ли на сайте банка защищенное соединение
http://abra.kadabra
Проверяйте адрес сайта, не переходите по подозрительным ссылкам из писем

СНИФФЕРИНГ


WiFi
Соединение через незащищенное Wi-Fi-соединение
Оплата мобильной связи
Введите номер карты
1234 5678 9123 4567
СНИФФЕРИНГ
Цель мошенничества — перехват данных мошенниками в общественных местах
КАК СЕБЯ ОБЕЗОПАСИТЬ
wi-fi-my-cafffé
4G
Оплата мобильной связи
Введите номер карты
1234 5678 9123 4567
Не осуществляйте платежные операции в общественных местах через незащищенные сети Wi-Fi
Убедитесь, что соединение происходит через мобильную сеть

ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ

ЗАЩИТИТЕ СВОИ УСТРОЙСТВА

- обновляйте операционную систему (информационные системы и любые софты)
- используйте антивирус (следите за «свежестью» вирусных баз)
- не подключайте к своим устройствам не проверенные антивирусом новые носители информации (флешки, диски)
- создавайте резервные копии (используйте облачное хранилище или физические носители)
- следите за кибербезопасностью своего мобильного устройства (установите пароли, разделите учетные записи на личную и рабочую)

ЗАЩИТИТЕ СЕБЯ В ИНТЕРНЕТЕ

- не разглашайте личную информацию (ПИН-код, CVV/CVC, SMS-код, логин, пароль и др.)
- контролируйте содержание размещаемой информации (неразрешенное использование материала влечет гражданскую или уголовную ответственность)
- закрывайте сомнительные всплывающие окна
- используйте сложные пароли к разным ресурсам (например, с помощью менеджера паролей) и двухфакторную идентификацию
- используйте общественный Wi-Fi только в случае крайней необходимости (мобильный Интернет безопаснее)

ПРЕВЕНТИВНЫЕ МЕРЫ

- бережно храните документы, удостоверяющие личность, старайтесь не допустить их потери или кражи.
- умейте говорить «нет»! Оставляйте сканы документов только там, где этого требует закон (например, откажите охранникам, которые пытаются снять копию с паспорта, вместо того чтобы переписать данные для оформления пропуска).

Толкачева Светлана

www.youtube.com/c/SvetlanaTolkacheva

https://rutube.ru/channel/24115490/

https://vk.com/tolkacheva_sv

ХОЧУ ЗНАТЬ БОЛЬШЕ