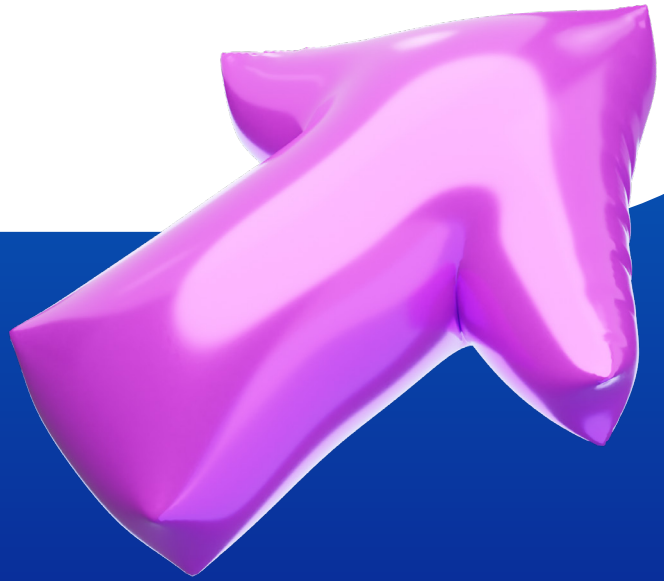
ВТБ Страна
БЛАГОТВОРИТЕЛЬНЫЙ ФОНД

# Финансовая безопасность в цифровой среде



Узнать больше о проекте: https://www.vtb.ru/bezopasnost/#faq

# Толкачева Светлана

## Топ-менеджер банка

### Общественная и профессиональная деятельность

- Член экспертного совета при Центральном банке Российской Федерации
- Член Наблюдательного совета Ассоциации развития финансовой грамотности
- Член Общественного совета при Департаменте образования и науки г. Москвы
- 20+ лет работы в финансовых компаниях, включая 16 лет в банковской сфере

### Образование

- 2023 г. — Центр исследования безопасности информационных технологий (ООО «ЦИБИТ»), специальность «Компьютерная безопасность», специальность «Информационная безопасность».
- 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.

**Автор учебника «Финансовая грамотность. Цифровой мир» (изд. «Просвещение»)**

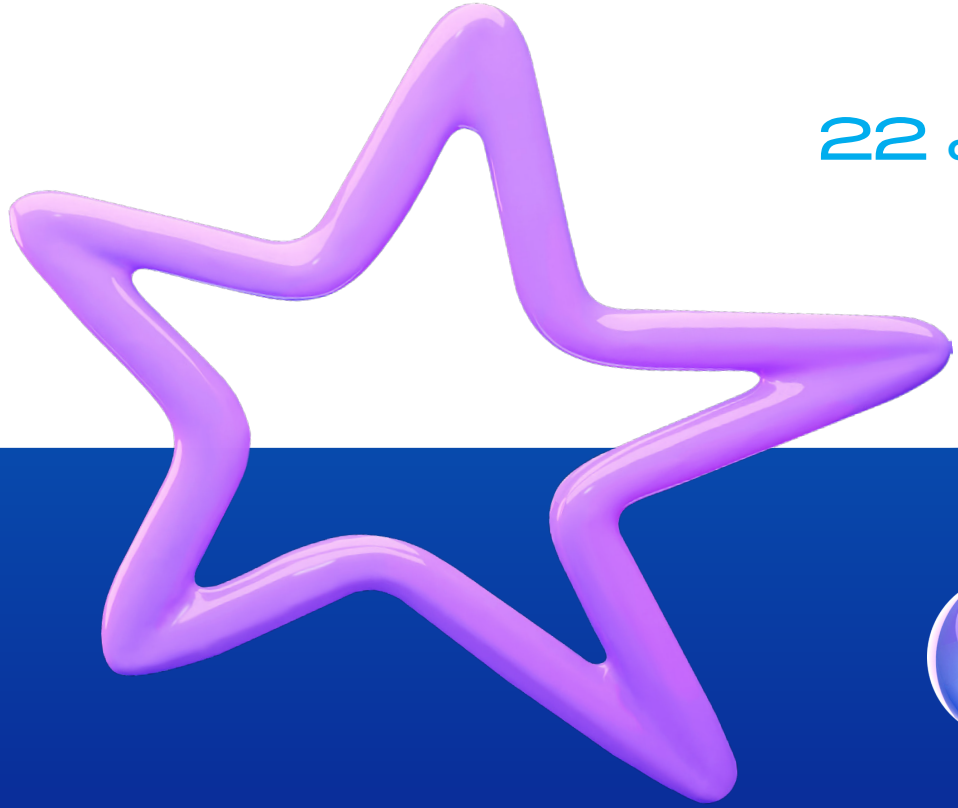
**Автор канала «Финансовая грамотность со Светланой Толкачевой» в соц. сетях**

### Светалана Толкачева в социальных сетях

| | |
|---|---|
| VK | https://vk.com/tolkacheva_sv |
| Rutube | https://rutube.ru/u/svetlanatolkacheva/ |
| Больше о проекте | https://www.vtb.ru/bezopasnost/#faq |

# Содержание





# Защита от мошенничества и социальной инженерии

**Почему мы попадаемся на психологические уловки мошенников и как этому противостоять**

# Мошенничество в цифрах

По данным Банка России *

## Статистика мошенничества и компьютерных атак:

**86%**

### Социальная инженерия

Люди самостоятельно отдают свои персональные и финансовые данные мошенникам.

**14%**

### Фишинговые атаки

Атаки с использованием вредоносного программного обеспечения и другие.

## Какие действия совершают под влиянием мошенников*, в %

**18,9%**

Переходят по ссылке, которую присылают злоумышленники.

**15,6%**

Переводят деньги злоумышленникам.

**11,2%**

Сообщают коды из смс-сообщений Госуслуг.

**10,8%**

Сообщают код из смс-сообщений или пуш-уведомлений Банка.

**7,6%**

Вводят данные банковской карты на сайте.

**6,7%**

Устанавливают вредоносное приложение.

**6,6%**

Сообщают паспортные данные.

**6,2%**

Вводят личные данные на сайте (СНИЛС, паспорт).

**5%**

Сообщают данные банковской карты.

**3,8%**

Набирают комбинацию цифр на телефоне.

* Аналитика Банка России за 2024: «Обзор операций, совершенных без согласия клиентов финансовых организаций» и «Кибермошенничество: портрет пострадавшего»

# Мошенничество в цифрах

## Сколько денег потеряли граждане в 2024

**55,3%**

ущерб до 20 тыс.руб.

**24,4%**

ущерб от 100 тыс.руб. и более**

**20,3%**

ущерб от 20 до 100 тыс.руб.

**43%**

Жертв обращаются в свой банк

**18%**

Жертв никуда не обращаются

## Портрет типичной жертвы киберпреступлений

- Возраст от 25 до 44 лет
- Проживает в городе
- Средний уровень дохода и среднее образование
- Активно пользуется банковскими онлайн-сервисами
- Работающая женщина (В 2022 лидировали мужчины)

* Аналитика Банка России за 2024: «Обзор операций, совершенных без согласия клиентов финансовых организаций» и «Кибермошенничество: портрет пострадавшего»

** На 8,8 % выросло количество случаев хищения свыше 20 тыс. руб. (по сравнению с 2023 г.).

# Основные приемы социальной инженерии

## Цель социальной инженерии

Цель — посредством психологической атаки вынудить человека добровольно сообщить ценную конфиденциальную информацию, такую как логины, пароли, номера банковских карт и счетов.

Основа социальной инженерии — манипуляции, использующие слабости человека. Такие как: доверчивость, страх, жадность, невнимательность.

## Основные приемы социальной инженерии

### Вызов сильных эмоций

Страх, радость, тревога.

**Цель:** нарушить равновесие, отключить рациональное мышление.

### Оперирование личными фактами

Упоминание личных данных, ссылки на близких и друзей.

**Цель:** вызвать доверие и рассеять сомнения; расчет на неосведомленность о простом получении информации из открытых источников.

### Использование новостного фона

Экономические и политические события.

**Цель:** легкость убеждения через подготовку жертвы новостной информацией.

### Искусственный цейтнот

Принятие решения безотлагательно, в условиях жестких временных рамок.

**Цель:** обработать жертву до возврата к рациональному поведению.

# Мошенничество через звонки и сообщения

## Социальная инженерия с использованием телефона, электронной почты и мессенджеров

Все многообразие мошеннических схем и легенд можно распределить на следующие типы по способу получения от вас информации / денег и применяемого к вам воздействия:

- Вынуждение вас **самостоятельно раскрыть коды, пароли** и иную конфиденциальную информацию, являющуюся «ключом» к получению ваших средств и имущества.
- Особая категория — схемы, основанные на легендах, выдаваемых от имени известных лично вам третьих лиц — **со взломанных / поддельных аккаунтов.**
- Призывы, побуждающие вас непосредственно к совершению действий **по передаче имущества и переводу средств** мошенникам.
- Просьбы **установить на ваши устройства программы удаленного доступа** (включая направление ссылок для установки) или **поделиться экраном** — часто с маскировкой под иные действия (установка «безопасного» ПО от сотрудника банка и пр.).

Все чаще мошеннические схемы приобретают многоступенчатый характер с комбинацией видов воздействия — в них задействованы организованные преступные группы, где у каждого участника своя роль.

Кейсы, варианты и комбинации мошенничеств с использованием СИ постоянно меняются — злоумышленники «работают» на опережение. Важно понимать общий алгоритм противодействия.

## Пример мошенничества

# Как защищаться?

## Никогда не сообщайте личные данные

Держите в секрете свои персональные данные, информацию о банковских счетах и картах, пароли от значимых ресурсов, телефона, электронной почты, одноразовые коды, а также контакты родных и близких людей.

## Проверяйте информацию

Позвоните человеку, со ссылкой на которого к вам обращаются, или в организацию, от имени которой с вами связались (попросите назвать полное имя и должность звонящего), и уточните информацию.

**Главное правило — всегда берите паузу, чтобы вспомнить, что конфиденциальную информацию никому нельзя передавать!**

# Фишинг

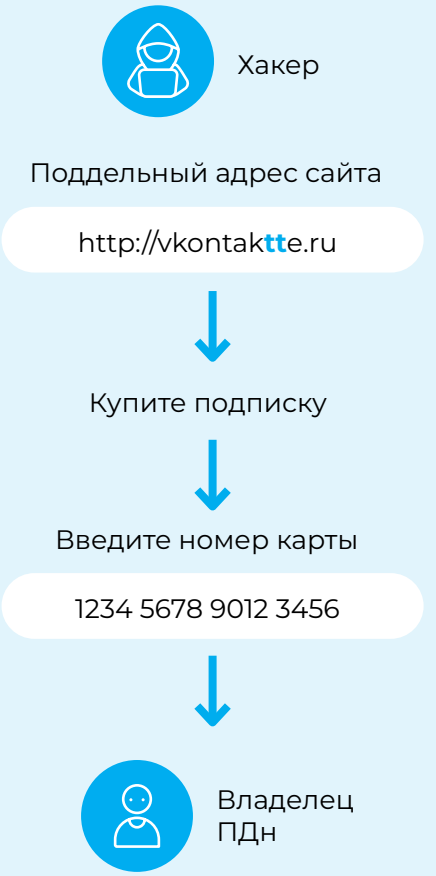
## В чем суть?

Это вид интернет-мошенничества в форме социальной инженерии, целью которого является получение конфиденциальной информации пользователей с использованием «подделки» — мошенники выдают себя за того, кем они не являются (сайт, представитель компании, государственных органов).

## Как работает?

1. Создание поддельного веб-сайта или отправка электронного письма, которое выглядит как официальное сообщение от известной организации.
2. Привлечение внимания к сообщению или сайту с помощью заголовка, который вызывает интерес или тревогу.
3. Запрос конфиденциальной информации пользователя (логины, пароли, номера карт и т.д.).
4. Использование полученной информации для кражи личных данных или денежных средств пользователя.

## Пример мошенничества



# Как защищаться от фишинга?

## Проверяйте адреса веб-сайтов

Проверяйте адреса веб-сайтов перед вводом конфиденциальной информации. На поддельных сайтах мошенники используют похожие названия популярных ресурсов.

## Электронные письма

С подозрением относитесь к электронным письмам с вложениями и ссылками. Вредоносные ссылки могут вести на фейковый сайт или активировать вирус.

## Защищенность соединения

Проверяйте защищенность соединения перед введением чувствительной информации. «http://» — вместо «https://» с «s» на конце — незащищенное соединение.

## Вводите адрес вручную

Вводите адрес вручную или сохраняйте закладки. Не переходите по ссылкам и не предоставляйте личную информацию без предварительной проверки — свяжитесь с отправителем альтернативным способом.


**Остерегайтесь слишком выгодных предложений. Это базовая «приманка» в социальной инженерии, используемая мошенниками в фишинговых атаках.**

# Снифферинг

## В чем суть?

Это процесс перехвата сетевого трафика мошенниками. В целях безопасности никогда не используйте общественный Wi-Fi для:

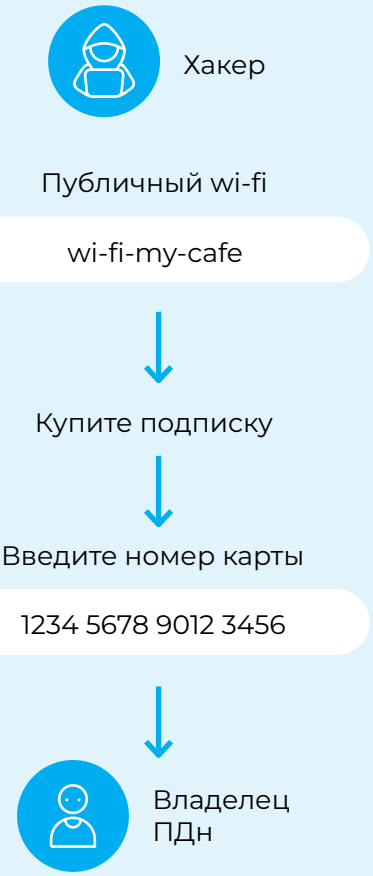
- Платежных операций.
- Ввода персональных данных (например, данных банковской карты при оплате).
- Загрузки приложений.

## Как работает?

Снифферы работают с помощью перехвата данных через публичный Wi-Fi. Это позволяет просматривать информацию, передаваемую по сети.

**Осуществляйте платежные операции, загрузки и введение ПДн только через мобильную сеть (4G).**

## Пример мошенничества



# Риски при использовании программ удаленного доступа и VPN

## В чем суть мошенничества с программами удаленного доступа?

Мошенники под различными предлогами убеждают установить приложения удаленного доступа (TeamViewer, Quick Support, AnyDesk, AweSun и т.п.) и разрешить доступ к устройству. В результате злоумышленники получают доступ не только к устройству, но и к приложениям Банка и денежным средствам клиента.

## Как защититься?

- Никогда не устанавливайте программы удаленного доступа.
- Не давайте Ваш мобильный телефон посторонним людям.

## В чем суть VPN?

VPN (англ. virtual private network — «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети.

## Риски при использовании:

- Нет гарантий безопасности (сохранения логинов, паролей и т. д.).
- Риск компрометации данных пользователя (продажа информации о трафике и действиях пользователя в сети).
- Может содержать вирус.

# Персональные данные: уязвимость и защита

**Как умение контролировать передачу и использование своих персональных данных связано с личной финансовой безопасностью**

# Персональные данные (ПДн)

## Персональные данные (информация о личности граждан) защищены законом*

«Любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу — субъекту ПДн» (п.1.1 ст.3 152-ФЗ).

Это набор данных, неразрывно связанный с личностью и позволяющий ее идентифицировать (закон не содержит конкретного перечня).

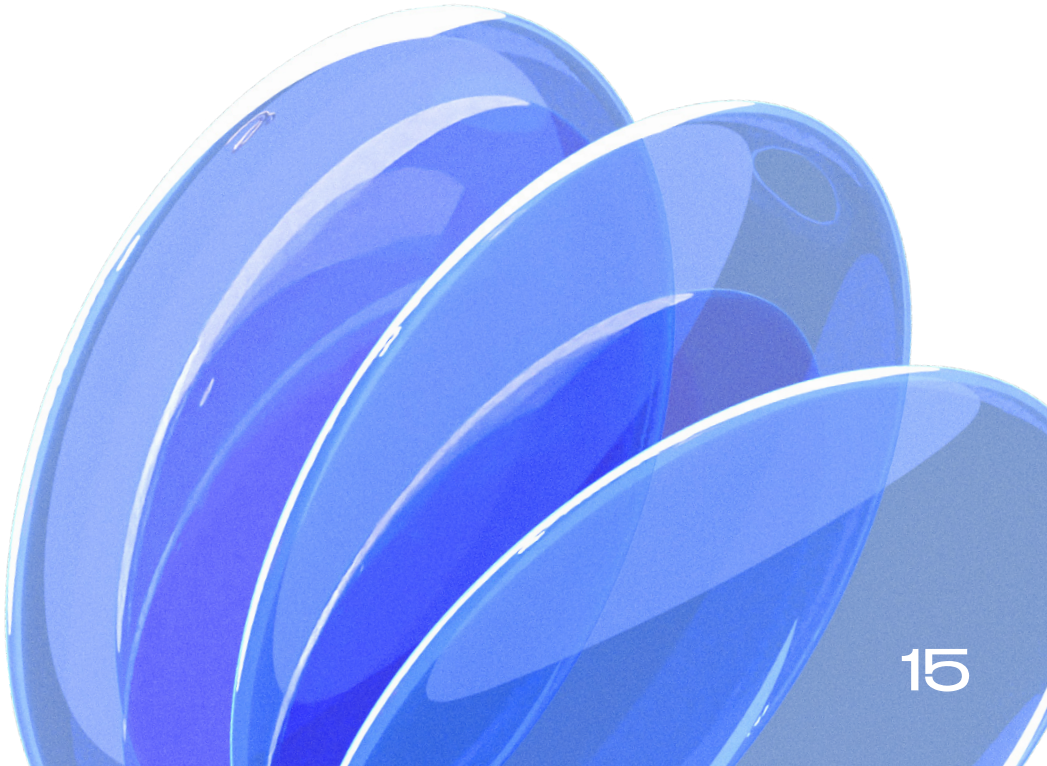
## Оператор ПДн

Лицо, обрабатывающее ПДн**. Реестр операторов доступен на сайте Роскомнадзора.

## Категории ПДн

Оператор обязан обеспечивать степень защиты ПДн по категориям:

- Общедоступные****
  ФИО, год и место рождения, адрес, абонентский номер, профессия, образование
- Биометрические*
- Специальные
  Национальность, состояние здоровья, интимная жизнь, судимость
- Иные



* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» обеспечивает защиту информации о личности граждан.
** Государственный, муниципальный орган, юридическое или физическое лицо. Оператор предварительно определяет состав, цели и действия с ПДн. имеет право, с согласия гражданина, поручить обработку другому лицу — обработчику ПДн.
*** Могут включаться в общедоступные источники (справочники, адресные книги) с согласия субъекта ПДн. Данные, которые можно найти в интернете, обрабатывать и распространять без согласия нельзя.

# Персональные данные клиента банка

## Что могут узнать мошенники?

- ФИО, дату и место рождения
- Адрес проживания
- Номер телефона
- Место работы или учёбы
- Фото с гео-меткой
- В каких банках есть счета

## Что доступно только вам?

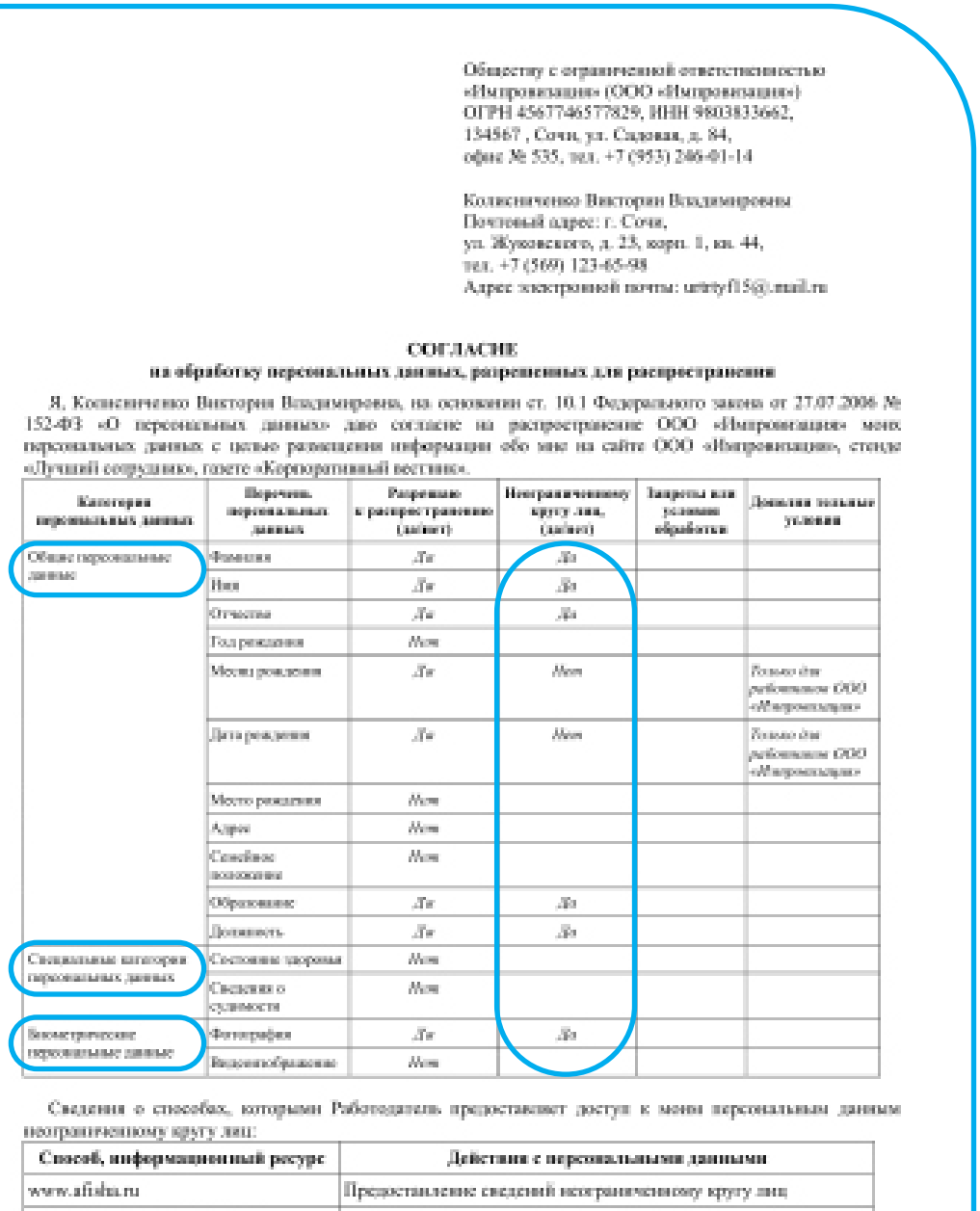
- PIN-код от карты
- CVV-код (трёхзначный код на обратной стороне)
- 3DS-код из СМС для подтверждения операций
- OTP-код для входа или смены пароля в Онлайн-банк

## Клиент несет ответственность за:

- Безопасное и конфиденциальное хранение персональной информации.
- Предоставление ложных и заведомо недостоверных сведений о себе.
- Своевременное информирование банка об изменении своих ПДн.

**Не разглашайте свою конфиденциальную информацию!**

# Согласия на обработку ПДн



Обществу с ограниченной ответственностью
«Импровизация» (ООО «Импровизация»)
ОГРН 4567746577829, ИНН 9803833662,
134567 , Сочи, ул. Садовая, д. 84,
офис № 535, тел. +7 (953) 246-01-14

Колесниченко Виктории Владимировны
Почтовый адрес: г. Сочи,
ул. Жуковского, д. 23, корп. 1, кв. 44,
тел. +7 (569) 123-65-98
Адрес электронной почты: urtrty615@.mail.ru

**СОГЛАСИЕ**
**на обработку персональных данных, разрешенных для распространения**

Я, Колесниченко Виктория Владимировна, на основании ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие на распространение ООО «Импровизация» моих персональных данных с целью размещения информации обо мне на сайте ООО «Импровизация», стенде «Лучший сотрудник», газете «Корпоративный вестник».

| Категория персональных данных | Перечень персональных данных | Разрешаю к распространению (да/нет) | Неограниченному кругу лиц, (да/нет) | Запреты или условия обработки | Дополнительные условия |
|---|---|---|---|---|---|
| Общие персональные данные | Фамилия | Да | Да | | |
| | Имя | Да | Да | | |
| | Отчество | Да | Да | | |
| | Год рождения | Нет | | | |
| | Месяц рождения | Да | Нет | | Только для работников ООО «Импровизация» |
| | Дата рождения | Да | Нет | | Только для работников ООО «Импровизация» |
| | Место рождения | Нет | | | |
| | Адрес | Нет | | | |
| | Семейное положение | Нет | | | |
| | Образование | Да | Да | | |
| | Должность | Да | Да | | |
| Специальные категории персональных данных | Состояние здоровья | Нет | | | |
| | Сведения о судимости | Нет | | | |
| Биометрические персональные данные | Фотография | Да | Да | | |
| | Видеоизображение | Нет | | | |

Сведения о способах, которыми Работодатель предоставляет доступ к моим персональным данным неограниченному кругу лиц:

| Способ, информационный ресурс | Действия с персональными данными |
|---|---|
| www.afisha.ru | Предоставление сведений неограниченному кругу лиц |

Операторы ПДн обязаны не раскрывать третьим лицам и не распространять ПДН без согласия субъекта ПДн (Конфиденциальность ПДн, ст.7 № 152-ФЗ).

Лицо, которое получает от вас ПДн, автоматически становится оператором ПДн и по закону обязано подписать с вами согласие на обработку ПДн. Отсутствие согласия должно вас насторожить.

## Виды согласий:

### 1. Согласие на обработку ПДн для определённого круга лиц

- Обработка целевого ограниченного набора ПДн.
- После достижения целей ПДн уничтожаются.

### 2. Согласие на обработку ПДн для распространения

- Оформляется отдельно с 2021 года.
- Раскрытие ПДн неопределённому кругу лиц.
- Возможность выбора ПДн по каждой категории.
- Молчание субъекта ПДн не означает его согласие.

# Управление согласиями на обработку ПДн

## Что можно и нужно делать с согласиями?

- Выдавать
- Отзывать
- Устанавливать ограничения по:
  - Категориям ПДн
  - Срокам
  - Целям

## Как правильно работать с согласиями?

- Не предоставлять избыточные ПДн сверх целей обработки
- Учитывать, что согласия есть в электронном виде

**Контролируйте безопасность устройств и актуальность оформленных на вас абонентских номеров, привязанных к значимым сервисам, содержащим ПДн**

# Надежный пароль для защиты ПДн

## Критерии хорошего пароля

- Длина:
  не менее 12 символов
- Срок действия:
  смена пароля
  каждые 90 дней
- Уникальность:
  для каждого сервиса
  отдельный пароль.
  В первую очередь,
  это касается аккаунтов
  электронной почты
  и портала «Госуслуги»
- Сложность:
  пароль должен
  быть сложным
  и запоминающимся
- Для этого используйте:
  Мнемотехники
  Менеджеры паролей
  (условие – доверие
  к провайдеру)

Проверяйте надежность пароля
по мере его усложнения
на специальном сервисе:
https://password.kaspersky.com/

**Kaspersky Password Manager**

## Как проверить надежность пароля?

### Хороший пароль!

*$1v9e8t8iK_1988*

- Стойкий ко взлому пароль
- Ваш пароль не встречается
  в базах утекших паролей

### Пароль пора менять!

sveta1988

- Часто используемое слово
- Этот пароль засветился
  в базах утекших паролей
  1 365 раз

# Двухфакторная аутентификация (2FA)

Это способ защиты вашего аккаунта, при котором, чтобы подтвердить свою личность, нужно иметь два не связанных между собой типа идентификационных данных из трех возможных.

## То, что вы знаете: логин и пароль

Пароль должен быть надёжным, чтобы хакеры не смогли его взломать. Но есть и другие способы украсть пароль, например, при переходе по фишинговой ссылке или установке вредоносного приложения.

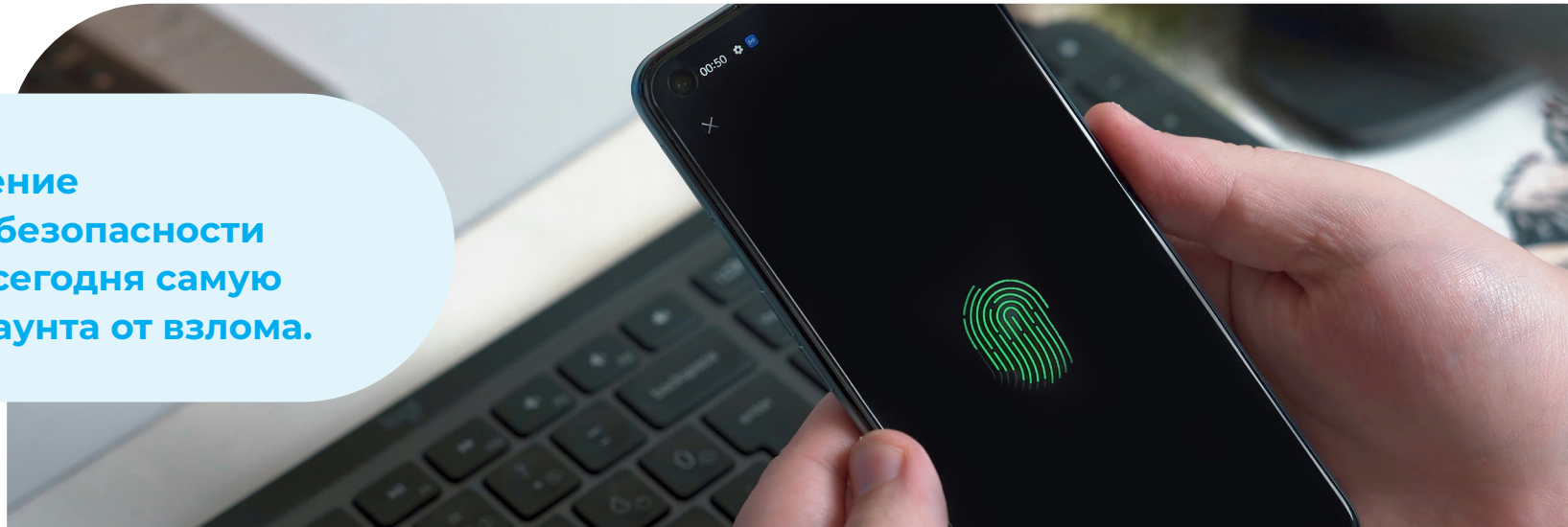
## То, что является частью вас: биометрия

Это отпечатки пальцев, геометрия кисти руки, черты лица, голос, узор радужной оболочки и сетчатки глаз, рисунок вен пальцев. Этот способ пока не очень распространён, но он перспективен в будущем с учетом доработки точности идентификации и сохранности данных.

## То, чем вы владеете: смартфон, 2 токен, карта или другое устройство

Часто используется получение одноразовых кодов через СМС на смартфон или электронную почту (самый уязвимый способ), через приложения-аутентификаторы или аппаратные генераторы паролей (самый защищённый способ). Но есть риск, что одно устройство будет использоваться и для входа в аккаунт, и для получения одноразового пароля.

**Надежный пароль + введение дополнительного уровня безопасности в виде 2FA обеспечивает сегодня самую эффективную защиту аккаунта от взлома.**



# Чекап финансовой безопасности

Превентивная мера — регулярная верификация конфиденциальной и чувствительной информации о себе на значимых ресурсах.

## Чекап и параметры для составления плана проверки

### 1. Пароли и 2FA (одноразовые коды)

- Список ресурсов (все значимые ресурсы).
- Даты смены паролей (1 раз в 90-180 дней).
- Требования к сложности паролей (лучше >12 символов).
- Наличие 2FA. Если нет 2FA — проверки чаще.

### 2. Согласия на использование ПНД

- Список и параметры выданных согласий.
- Даты регулярной проверки (мониторинг - не реже 1 раза в год).
- Используйте раздел «Согласия и доверенности» в профиле Госуслуг.

### 3. Кредитная история

- Даты проверки (1 раз в полгода).
- Список БКИ (уточняется при запросе списка БКИ через ПГУ).

### 4. Информация на значимых ресурсах

- Список значимых ресурсов (ЛК ФНС, Росреестр, СФР и др.).
- Даты регулярной проверки (не реже 1 раза в год).

### 5. Аккаунты в браузерах, соцсетях / приложения

- Аккаунты для проверки (Яндекс, Google, Вк и др.).
- Настройки безопасности/конфиденциальности.

**Сделайте чекап своей финансовой безопасности привычкой и частью образа жизни!**

# Безопасность использования банковских продуктов

**Какие базовые рекомендации по финансовой безопасности от банка стоит загрузить в свой багаж знаний грамотному пользователю банковских продуктов**

# Правила обслуживания клиентов дебетовых и кредитных карт

Карта — это физический носитель с чипом для операций по счету.
Карту можно «токенизировать» = привязать к телефону (через MIR Pay).

## Можно сообщать

- 16-символьный номер карты

Зная только номер карты, осуществить операции крайне затруднительно.

Для получения переводов через Систему быстрых платежей (СБП) используйте номер телефона.

## Нельзя сообщать

- Имя держателя карты
- Срок действия карты
- Код CVV2/CVC2 (на оборотной стороне карты, используется для проверки ее подлинности)

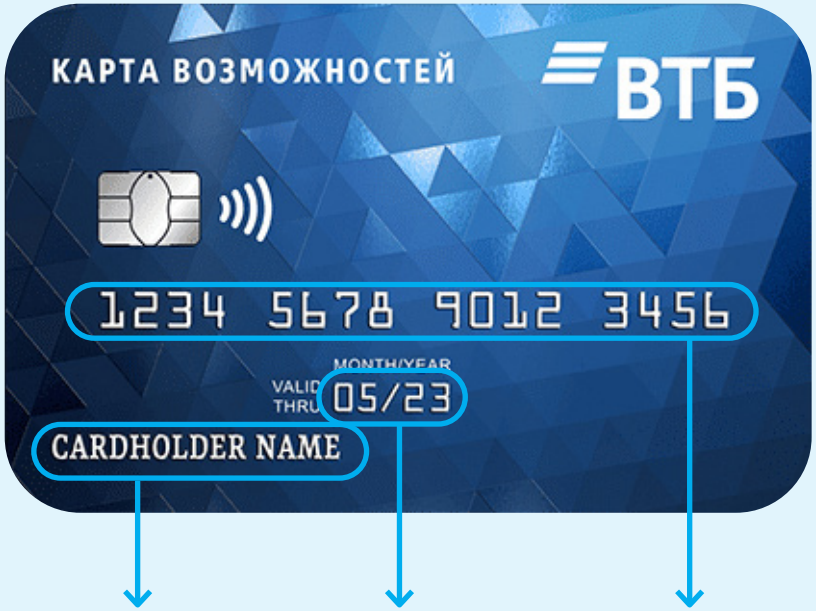
Категорически никому и никогда (вместе с PIN-кодом).

## Как защитить?

- Не сообщайте посторонним данные банковской карты.
- Не публикуйте в открытом доступе фотографии карты.

## Важно помнить!

При компрометации реквизитов или утрате карты заблокируйте её в приложении или позвоните на Горячую линию Банка.




Имя держателя карты | Срок действия карты | 16-символьный номер карты

Код из трёх цифр на оборотной стороне карты или код CVV2/CVC2 используется для проверки ее подлинности.

# Поддельные приложения

## В чем суть?

Поддельные приложения создаются мошенниками, которые имитируют официальные приложения магазинов, банков и других компаний. Их можно загрузить с сомнительных источников или даже с официальных магазинов, например, Google Play, App Store, RuStore и др.

## Как защититься?

- Загружайте приложения только из **официальных источников**.
- Никогда **не вводите личную информацию**, если не уверены в безопасности приложения.
- **Отрицательные отзывы** пользователей — признак того, что приложение поддельное.
- Используйте **антивирусное программное обеспечение.**
- Своевременно **обновляйте** приложения.
- Загружайте банковские приложения, отдавая предпочтение **ссылке с официального сайта** Банка.

**Важно помнить о том, что ответственность за безопасность устройства лежит на самом клиенте. Банк не вмешивается в настройку клиентских устройств.**

# Ответственность и риски

## Ответственность за возврат кредита, оформленного под действием мошенников, несет заемщик

- Клиент лично обязан вернуть кредит банку.
- Не платить по кредиту удастся только в том случае, если в судебном порядке доказать, что кредит был оформлен без участия клиента (например, по украденным документам).

## Не становитесь «Дропом»

«Дроп» — подставное лицо, чья банковская карта используется для вывода и обналичивания денежных средств, украденных путем мошенничества. За данные действия предусмотрена уголовная ответственность.

## Ответственность за мошенничество

- Статья 158 УК РФ Кража
- Статья 159 УК РФ Мошенничество
- Статья 159.3 УК РФ Мошенничество с использованием электронных средств платежа
- Статья 187 УК РФ Неправомерный оборот средств платежей

## Рекомендации:

- Соблюдайте безопасность при пользовании банкоматом и не соглашайтесь помогать незнакомым людям у банкоматов.
- Не соглашайтесь на предложения легкого заработка от незнакомцев.
- При ошибочном пополнении вашего счета возврат средств осуществляйте через Банк.
- Ставьте самозапрет на кредиты.
- Просвещайте близких по вопросам финансовой безопасности — особенно детей и старшее поколение.

# Проверка настроек безопасности

## Настройте лимиты на траты и переводы

## Просматривайте историю авторизаций в ВТБ Онлайн

## Подключите оповещения

Подключите оповещения и проверяйте параметры операции в SMS-сообщении / Push-уведомлении с кодом подтверждения.

## Настройте блокировку экрана

Так,  чтобы не было видно уведомлений на заблокированном экране на вашем мобильном устройстве.

## Проверяйте ссылки

Если ссылка кажется подозрительной, отправьте её на проверку в личном кабинете.

## Если подозреваете компрометацию

Если подозреваете компрометацию учётных данных или несанкционированный доступ, заблокируйте учётную запись самостоятельно или обратитесь в Банк.

## Почему операцию могут заблокировать?

Банк может приостановить сомнительный платёж или перевод для проверки личности клиента.

Если операция была инициирована не клиентом, Банк отменит её и заблокирует карту в целях безопасности.

# Безопасные каналы взаимодействия с банком ВТБ

## Официальные номера телефонов Банка ВТБ

1000
8 (800) 100-24-24
+7 (495) 777-24-24

## Официальные мессенджеры и социальные сети Банка ВТБ

Telegram https://t.me/vtb_main_bot
ВКонтакте https://vk.com/vtb

## Памятка по безопасности на официальном сайте Банка ВТБ

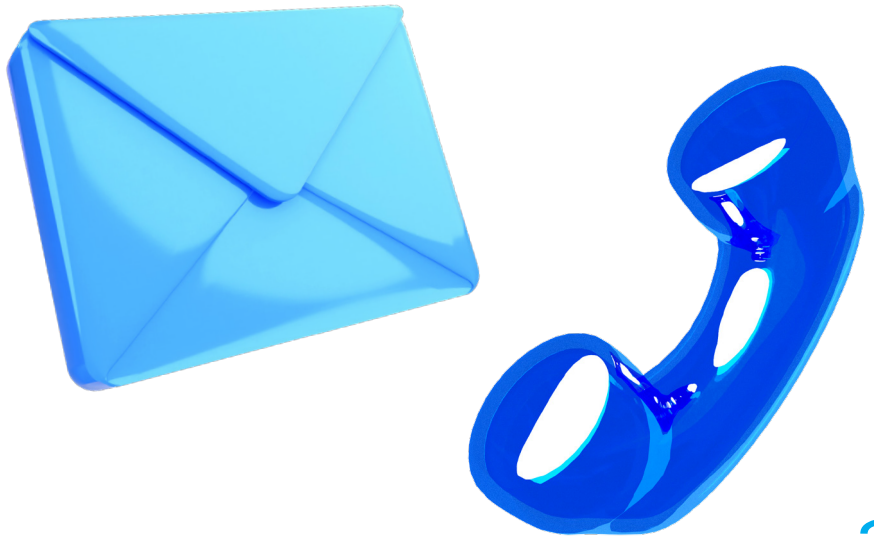
https://www.vtb.ru/bezopasnost/#faq

**Сотрудники Банка никогда не инициируют общение через мессенджеры или социальные сети с клиентом.**

Если вам поступают звонки, SMS-сообщения, сообщения в социальных сетях и мессенджерах от имени «банковских работников» с информацией, касающейся финансовых операций:

- Прекратите контактировать.
- Ни в коем случае не перезванивайте на указанные в сообщениях номера.
- Не сообщайте никому коды из SMS-сообщений / Push-уведомлений.
- Сообщите номер телефона мошенника в чат ВТБ Онлайн.
- При любых сомнениях перезвоните в банк самостоятельно.

Если пароль скомпрометирован, свяжитесь со службой Банка по телефону 1000 и заблокируйте доступ в личный кабинет.



# Толкачева Светлана

https://vk.com/tolkacheva_sv
https://rutube.ru/u/svetlanatolkacheva/