ВТБ

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

В ЦИФРОВОЙ СРЕДЕ

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

https://vk.com/tolkacheva_sv

ХОЧУ ЗНАТЬ БОЛЬШЕ

Толкачева Светлана

Топ-менеджер банка / Группа ВТБ
Автор учебника «Финансовая грамотность. Цифровой мир»/ (издательство «Просвещение»)
Автор канала «Финансовая грамотность со Светланой Толкачевой» в социальных сетях

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

ОБЩЕСТВЕННАЯ ДЕЯТЕЛЬНОСТЬ

- Член экспертного совета при Центральном банке Российской Федерации
- Член Наблюдательного совета Ассоциации развития финансовой грамотности
- Член Общественного совета при Департаменте образования и науки города Москвы

ПРОФЕССИОНАЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

Более 20 лет работы в финансовых компаниях, включая 16 лет в банковской сфере

СОДЕРЖАНИЕ

- Защита от основных видов мошенничества и приемов социальной инженерии
- Персональные данные: уязвимости и защита
- Безопасность использования банковских продуктов ВТБ

Защита от основных видов мошенничества и приемов социальной инженерии

Почему мы попадаемся
на психологические уловки мошенников
и как этому противостоять

МОШЕННИЧЕСТВО В ЦИФРАХ

По данным Банка России *

Социальная инженерия — люди самостоятельно отдают свои персональные и финансовые данные мошенникам

86%

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 коды из смс-сообщений или пуш-уведомлений от 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 теряют
по данным Банка России *

55,3%
ущерб до 20 тыс.руб.

20,3%
ущерб от 20 до 100 тыс.руб.

24,4%
ущерб от 100 тыс.руб. и более**

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

работающая женщина (в 2022 лидировали мужчины)

активно пользуется банковскими онлайн-сервисами

*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 ПРИЁМЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Основа социальной инженерии – манипуляции, использующие

СЛАБОСТИ ЧЕЛОВЕКА

Цель социальной инженерии

Вынудить посредством «психологической атаки» на человека добровольно сообщить ценную конфиденциальную информацию, такую как логины, пароли, номера банковских карт и счетов

Вызов сильных эмоций

Страх, радость, тревога

Цель: нарушить равновесие, отключить рациональное мышление

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

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

МОШЕННИЧЕСТВО ЧЕРЕЗ ЗВОНКИ И РАССЫЛКУ СООБЩЕНИЙ

Применение приемов социальной инженерии с использованием традиционной телефонии, 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

Призывы, побуждающие вас непосредственно к совершению действий по передаче имущества и переводу средств мошенникам

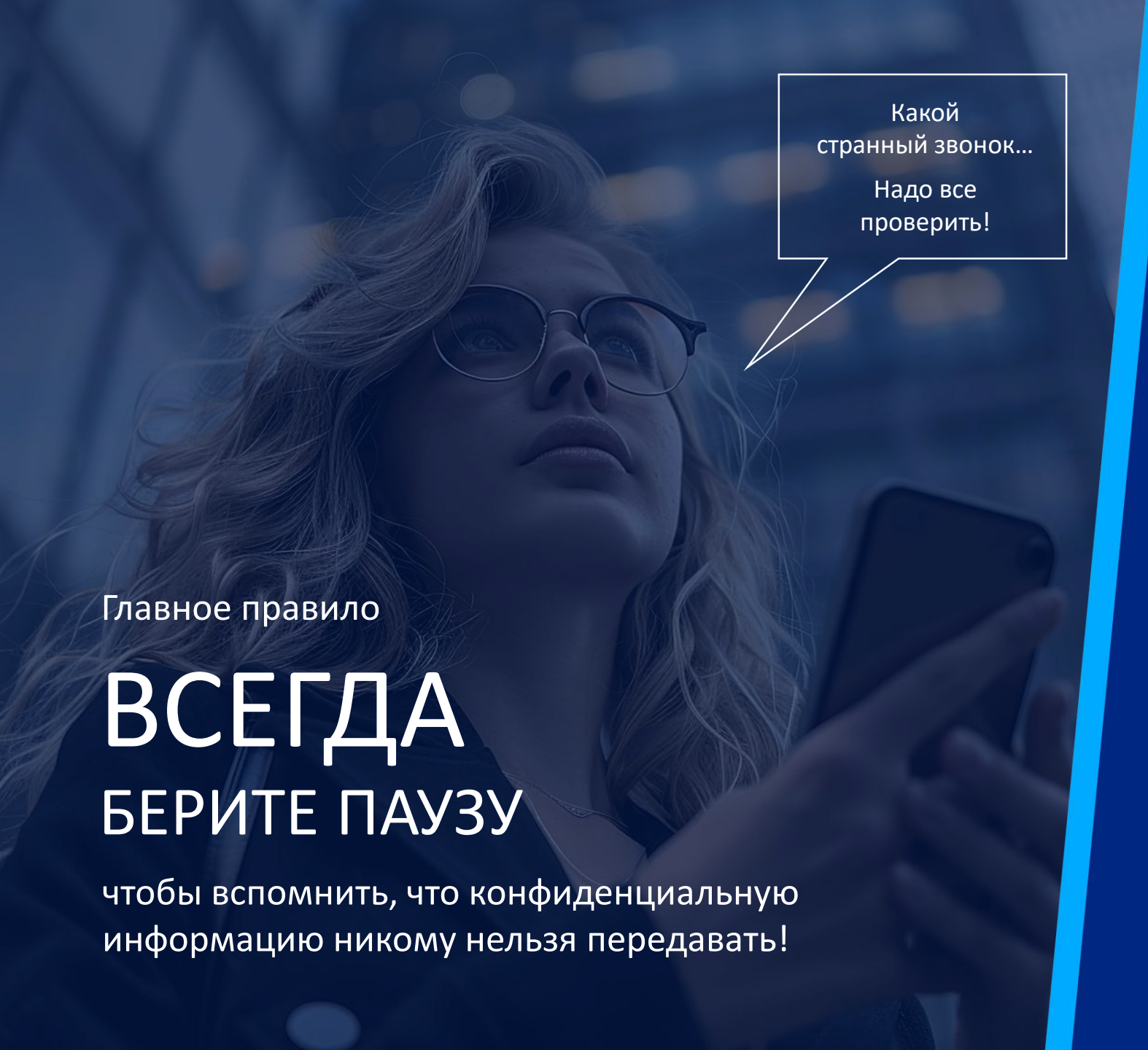
Просьбы установить на ваши устройства программы удаленного доступа (включая направление ссылок для установки) или поделиться экраном – часто с маскировкой под иные действия (установка «безопасного» ПО от сотрудника банка и пр.)

Особая категория - схемы, основанные на легендах, выдаваемых от имени известных лично вам третьих лиц – со взломанных/ поддельных аккаунтов

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



Главное правило

ВСЕГДА БЕРИТЕ ПАУЗУ

чтобы вспомнить, что конфиденциальную информацию никому нельзя передавать!

КАК ЗАЩИТИТЬСЯ?

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

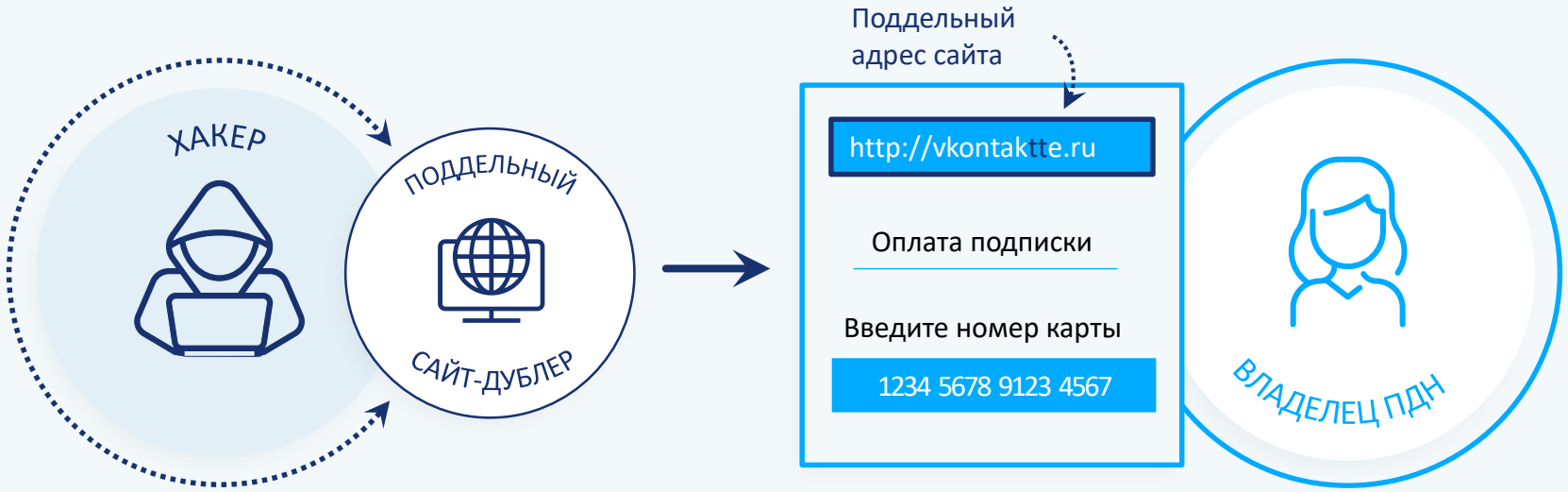
ФИШИНГ

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?

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



КАК ЗАЩИТИТЬСЯ?

от фишинга

Проверяйте адреса веб-сайтов
перед вводом конфиденциальной информации

На поддельных сайтах мошенники используют похожие названия популярных ресурсов. Вводите адрес вручную или сохраняйте закладки

Проверяйте защищенность соединения
перед введением чувствительной информации

http:// — вместо https:// с «s» на конце - незащищенное соединение

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

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)

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

УЯЗВИМОСТИ 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 к 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

Специальные

Национальность, состояние здоровья, интимная жизнь, судимость и др.

Биометрические*

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 о вас?

- 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

Не разглашайте свою конфиденциальную информацию!

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

СОГЛАСИЯ НА ОБРАБОТКУ ПДН

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

Виды согласий:

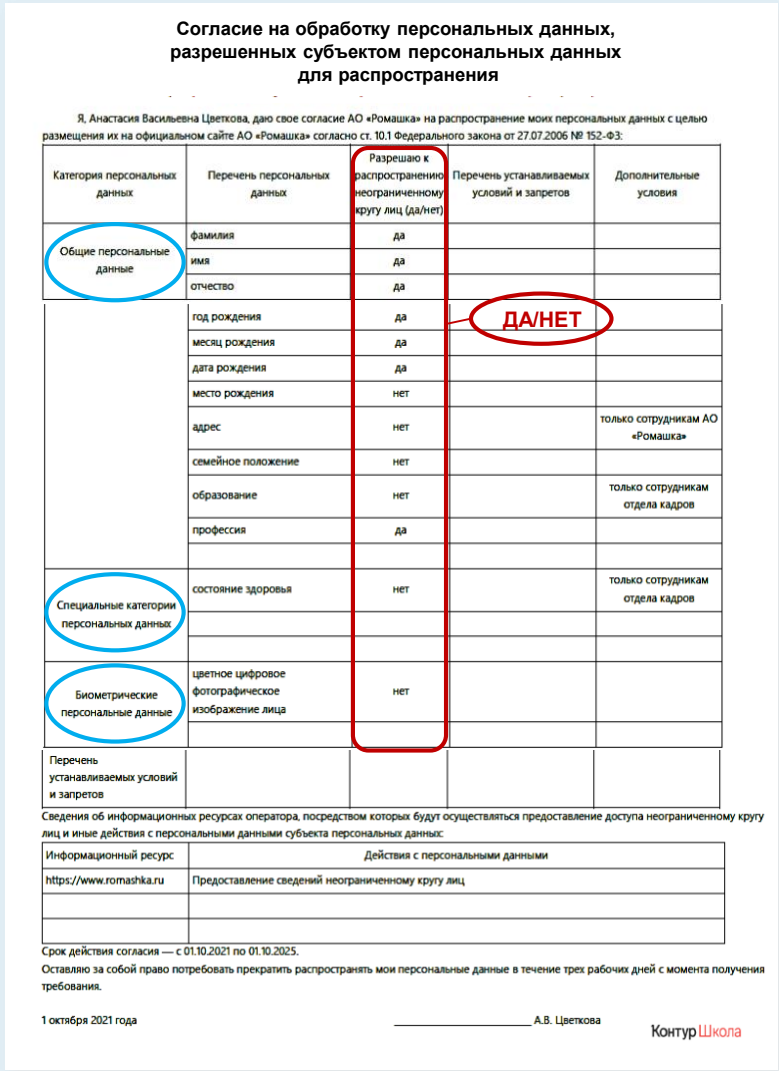
1 Согласие на обработку ПДн для определённого круга лиц:

- 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

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



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

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 могут быть **в электронном виде**

Контролируйте безопасность устройств

и актуальность оформленных на вас абонентских номеров, привязанных к значимым сервисам, содержащим ПДн

НАДЕЖНЫЙ ПАРОЛЬ ДЛЯ ЗАЩИТЫ ПДН

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:

Менеджеры паролей
условие – доверие к провайдеру

Мнемотехники

Как проверить надежность пароля?

Проверим надежность пароля по мере его усложнения на специальном сервисе

kaspersky password checker

sveta1988 → ***$1v9e8t8iK_1988***

Пароль пора срочно менять!

- часто используемое слово
- этот пароль засветился в базах утекших паролей 1 365 раз

Хороший пароль!

- у вас стойкий ко взлому пароль
- ваш пароль не встречается в базах утекших паролей

✓ **Добавили заглавные буквы, цифры и знаки**

✓ **Применили мнемотехники**

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

1 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

2 То, чем вы владеете: смартфон, 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

3 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

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

Чек-лист	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 (база - не менее 12 символов) • наличие двухфакторной аутентификации (если нет – 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 ЛК 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 ДЛЯ 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
Зная только номер карты, осуществить операции крайне затруднительно

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

НЕЛЬЗЯ сообщать
категорически никому и никогда (вместе с PIN-кодом)

16-символьный номер карты

Срок действия карты

Имя держателя карты

XXX — Код CVV2/CVC2 (на оборотной стороне карты, используется для проверки ее подлинности)

Как защитить?

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

Важно помнить!

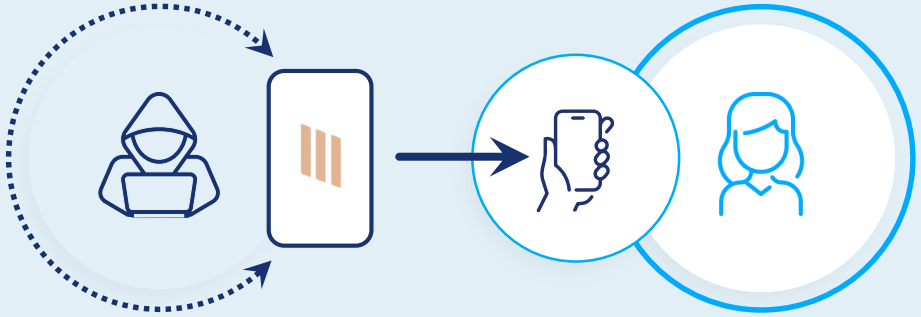
При компрометации реквизитов или утрате карты заблокируйте её в приложении или позвоните на Горячую линию Банка

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.



Важно помнить о том, что

ОТВЕТСТВЕННОСТЬ ЗА БЕЗОПАСНОСТЬ УСТРОЙСТВА ЛЕЖИТ НА САМОМ КЛИЕНТЕ

Банк не вмешивается в настройку клиентских устройств

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

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
- Подключите оповещения и проверяйте параметры операции
  SMS-сообщении / Push-уведомлении с кодом подтверждения
- Если ссылка кажется подозрительной, отправьте её на проверку
  в личном кабинете
- Просматривайте историю авторизаций в ВТБ Онлайн
- Настройте блокировку экрана
  видимости уведомлений на заблокированном экране на вашем мобильном устройстве
- Если подозреваете компрометацию
  учётных данных или несанкционированный доступ, заблокируйте учётную запись
  самостоятельно или обратитесь в Банк

Дополнительные меры безопасности от банка «поверх» ваших настроек

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

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

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

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

Памятка по безопасности на официальном сайте Банка ВТБ

Толкачева Светлана

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

https://vk.com/tolkacheva_sv

ХОЧУ ЗНАТЬ БОЛЬШЕ