ФИНАНСОВАЯ БЕЗОПАСНОСТЬ ПЕНСИОНЕРА

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

СОДЕРЖАНИЕ

1

ЧЕКАП СВОЕЙ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

- Мошенничество в цифрах
- Ревизия паролей
- Двухфакторная аутентификация
- Управление согласиями на обработку персональных данных
- Верификация на значимых ресурсах
- Проверка кредитной истории

2

КЛЮЧЕВЫЕ ПРАВИЛА ЗАЩИТЫ ОТ МОШЕННИКОВ

- Защита банковских карт
- Социальная инженерия
- Телефонное мошенничество
- Мошенничество через рассылку сообщений
- Фишинг и снифферинг
- Правила кибербезопасности

Чекап своей финансовой безопасности

МОШЕННИЧЕСТВО В ЦИФРАХ: ОБЩАЯ КАРТИНА

По данным ЦБ РФ *

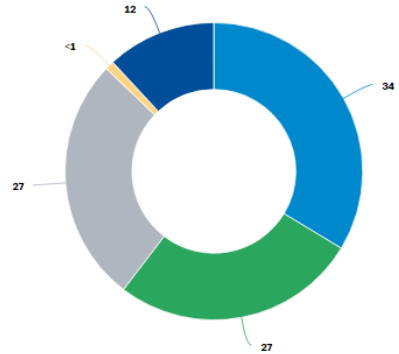
Что лидирует. Основным инструментом злоумышленников для хищения средств остается использование приемов и методов социальной инженерии. Доля таких операций по итогам 2022 года выросла по сравнению с аналогичным периодом прошлого года с 49,4 до 50,4%

Портрет типичной жертвы.
Возраст от 25 до 44 лет. Проживает в городе.
Работающий мужчина со средним уровнем дохода и средним образованием. Активно пользуется банковскими онлайн-сервисами

«Средний чек» мошенника. Средняя сумма хищения, совершенного с использованием приемов и методов социальной инженерии, у граждан в 2022 году составила 15,3 тыс. руб.

Возврат похищенного банками. По итогам 2022 года операции без согласия клиентов составили 14 165 млн руб. При этом кредитные организации вернули всего лишь 4,4% (за аналогичный период 2021 года – 6,8 %)

Типы ресурсов, используемые злоумышленниками в 2022 году (%)



- **Безлицензионная деятельность – 34 %**
- **Мошенничество – 27 %**
- **Финансовые пирамиды – 27 %**
- **Вредоносное программное обеспечение – 1 %**
- **Фишинг – 12 %**

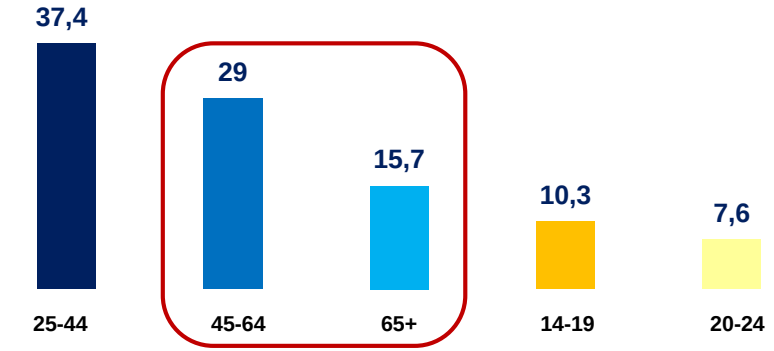
- Более трети ресурсов использовались злоумышленниками для осуществления безлицензионной деятельности в сфере рынка ценных бумаг, а также для рекламирования деятельности несуществующих кредитных, в т.ч. МФО, и страховых организаций
- Более четверти ресурсов побуждали вступить в финансовые пирамиды, и столько же привлекали фейковой информацией о псевдо-компенсациях от государства, заработках за прохождение опроса (теста), а также прочие мошеннические сайты по продаже билетов, туров и др.

- Аналитика Банка России за 2022 (февраль, 2023) «Обзор операций, совершенных без согласия клиентов финансовых организаций» - https://cbr.ru/analytics/ib/operations_survey_2022/

МОШЕННИЧЕСТВО В ЦИФРАХ: РИСКИ СТАРШЕГО ПОКОЛЕНИЯ

Каналы мошенничества, в %

Возраст жертв, в %



Социальный статус жертв, в %

Несмотря на смещение фокуса интереса мошенников в нишу с более высокими заработками, не стоит недооценивать риски для старшего поколения – массовость и универсальность телефонного мошенничества повышает уязвимость старших возрастных групп особенно

- Аналитика Банка России (февраль, 2023) «Обзор операций, совершенных без согласия клиентов финансовых организаций» - https://cbr.ru/analytics/ib/operations_survey_2022/

РЕВИЗИЯ ПАРОЛЕЙ

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 специальном сервисе

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)
- 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

Пароль аккаунта основной электронной почты, как и пароль для входа на портал «Госуслуги» - «мастер-ключ» для остальных сервисов:

- **должен принципиально отличаться от всех остальных паролей**
- **быть максимально надежным, а значит сложным**
- **регулярно обновляться с существенным изменением конструкции пароля (замены 1-2 символов недостаточно)**

* 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.

*Иллюстрация: securitylab.ru

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

УПРАВЛЕНИЕ СОГЛАСИЯМИ НА ОБРАБОТКУ ПДн

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

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

▲ **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 ПДн 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, Анаст ых 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

КонтурШкола

Согласие для распространения ПДн должно иметь чек-лист с разрешением по категориям данных

- **СОГЛАСИЯМИ МОЖНО УПРАВЛЯТЬ – ВЫДАВАТЬ, ОТЗЫВАТЬ, УСТАНАВЛИВАТЬ ОГРАНИЧЕНИЯ ПО КАТЕГОРИЯМ ПДн, СРОКАМ, ЦЕЛЯМ**
- **ПРОВЕРЯЙТЕ СООТВЕСТВИЕ ЗАПРАШИВАЕМЫХ ПДн ОЗВУЧЕННЫМ ОПЕРАТОРОМ ЦЕЛЯМ – НЕ ДАВАЙТЕ ИЗБЫТОЧНЫЕ ДАННЫЕ СВЕРХ, ТРЕБУЕМЫХ ДЛЯ ЦЕЛЕЙ ОБРАБОТКИ**
- **УЧИТЫВАЙТЕ, ЧТО СОГЛАСИЯ МОГУТ БЫТЬ В ЭЛЕКТРОННОМ ВИДЕ НА САЙТЕ И В ПРИЛОЖЕНИЯХ**
- **ПОМНИТЕ, ЧТО СОГЛАСИЕ ВСЕГДА МОЖНО ОТОЗВАТЬ ДОСРОЧНО**

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

ВЕРИФИКАЦИЯ НА ЗНАЧИМЫХ РЕСУРСАХ

Зачем нужен регулярный мониторинг текущей ситуации своих ПДн и другой чувствительной информации на ряде ресурсов в сети?

РИСКИ МОШЕННИЧЕСТВ:

- регистрация на вас юридических лиц/ИП
- незаконные сделки с вашим имуществом
- получение кредитных историй/справок о доходах для оформления на вас займов
- перевод пенсионных накоплений в другие НПФ и другие риски

Перечень ресурсов для проверки

ЕДИНЫЙ ПОРТАЛ ГОСУСЛУГ

Самый значимый ресурс, позволяющий верифицировать свой цифровой профиль по всем ключевым категориям - от земельно-имущественных отношений до социального обеспечения и здравоохранения.

Пароль от Госуслуг дает доступ к другим ресурсам, использующим авторизацию через ЕСИА: СФ, ФНС, Гис ЖКХ и другие. Региональный аналог gosuslugi.ru имеется у каждого российского региона. Например, у Москвы это pgu.mos.ru, СПб — gu.spb.ru.

ЕПГУ - горизонтальный портал с единым входом на множество значимых ресурсов через ЕСИА

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

СОЦИАЛЬНЫЙ ФОНД РОССИИ

РОСРЕЕСТР

EQUIFAX

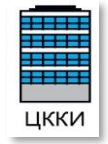
Русский Стандарт КРЕДИТНОЕ БЮРО

ОБЪЕДИНЕННОЕ КРЕДИТНОЕ БЮРО

НАЦИОНАЛЬНОЕ БЮРО КРЕДИТНЫХ ИСТОРИЙ

ПРОВЕРКА КРЕДИТНОЙ ИСТОРИИ

ПОЛУЧЕНИЕ КРЕДИТНОЙ ИСТОРИИ СОСТОИТ ИЗ 2-Х ШАГОВ, НА КАЖДОМ ВОЗМОЖНЫ ВАРИАНТЫ

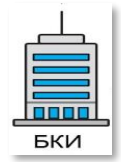


ШАГ 1 УЗНАТЬ ГДЕ ХРАНИТЬСЯ ВАША КРЕДИТНАЯ ИСТОРИЯ (ПОЛУЧИТЬ СПИСОК БКИ*)

Через портал «ГОСУСЛУГИ» — Через робота-помощника на Портале – просто задайте ему вопрос в чате
услуга доступна только для подтвержденной учетной записи (подтверждение через МФЦ или банк)

Через ЦККИ Банка России — раздел «Кредитные истории» официального сайта Банка России (https://www.cbr.ru/ckki/zh/) - заполнение формы запроса с указанием:
- адреса электронной почты, на который будет направлен ответ из ЦККИ
- кода субъекта кредитных историй**

Через посредников — партнеры БКИ (банки, МФО, финансовые интернет-порталы(banki.ru), др.) – почти всегда платно
- лично или онлайн, если предусмотрено (например, в рамках услуги онлайн-банкинга)
- требуется подтверждение личности (способ зависит от компании)



ШАГ 2 ПОЛУЧИТЬ КРЕДИТНУЮ ИСТОРИЮ (ВО ВСЕХ БКИ ИЗ ПОЛУЧЕННОГО СПИСКА)

Непосредственно в БКИ — получение досье возможно после идентификации личности
(возможно как личное обращение в каждое бюро, так и через личные кабинеты на сайтах БКИ)

С использованием портала «ГОСУСЛУГИ» — заказ КИ в бюро с использованием аккаунта от портала «Госуслуги»
(с 2020 года все БКИ это позволяют)

Через посредников
- но только в тех БКИ, с которыми посредник сотрудничает!
- способы получения (скачать на сайте, забрать в офисе, доставить курьером или заказным письмом) зависят от компании - всегда платно

ДВА РАЗА В ГОД БЕСПЛАТНО ПРОВЕРЯЙТЕ СВОЮ КРЕДИТНУЮ ИСТОРИЮ НАИБОЛЕЕ ОПТИМАЛЬНЫМ СПОСОБОМ - ЧЕРЕЗ ПОРТАЛ ГОСУСЛУГ

* Актуальный перечень БКИ, внесенных в государственный реестр - на сайте Банка России (https://www.cbr.ru/ckki/gosreestr_ckki/). Сейчас в Реестре 6 БКИ.

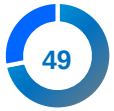
** Код субъекта КИ (аналог PIN-кода банковской карты) формируется/меняется/аннулируется при заключении договора займа (кредита), а также позднее, при обращении в любую кредитную организацию или БКИ при условии наличия КИ хотя бы в одном БКИ. Используется только на сайте ЦБ для получения сведений о БКИ.

Ключевые правила защиты от мошенников

ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Статистика мошенничеств с платежными картами (операции без согласия клиента за 2022 год, ЦБ РФ)*

- **Операции в банкоматах, терминалах, импринтерах:**
  - 129,08 тыс. случаев на общую сумму 1569,72 млн руб.,
  - из них 24,1% операций - результат социальной инженерии



- **Операции при оплате товаров и услуг в Интернете**:
  - 515,88 тыс. операций на сумму хищений 2550,54 млн руб.
  - 48,7% - социальная инженерия

- **Операции в дистанционном банковском обслуживании:**
  - более 226,79 тыс. раз системы дистанционного банковского обслуживания для физических лиц становились мишенью мошенников, сумма хищений - 9237,51 млн руб.
  - 69,5% - доля социальной инженерии

ПИН-код 4х-значный секретный код для операций в банкоматах/магазинах

CVV/CVC/CVP 3х-значный код на оборотной стороне карты для интернет-транзакций

- https://cbr.ru/analytics/ib/operations_survey_2022/

- **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 блокируйте ее (через приложение или сайт банка/ звонок в call-центр банка)**
- **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

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Социальная инженерия — это «психологическая атака на человека», психологические манипуляции и социальные приемы, методы и технологии, применяемые с целью вынудить человека добровольно сообщить ценную конфиденциальную информацию: логины, пароли, номера банковских карт и счетов

ОСНОВА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ – СЛАБОСТИ ЧЕЛОВЕКА

- Доверчивость
- Жадность
- Страх
- Невнимательность

Плохая новость: кейсы, варианты и комбинации мошенничеств с использованием СИ постоянно меняются – злоумышленники «работают» на опережение

Хорошая новость: у методов СИ, применяемых мошенниками, есть ряд отличительных признаков – а значит есть и алгоритм противодействия

«МОШЕННИЧЕСКИЙ» НАБОР ПРИЕМОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Вызов сильных эмоций

Страх за якобы совершенное нарушение закона, радость от будущего выигрыша или получения псевдо-пособия, тревога за близких и т.д.

Цель – выбить из состояния равновесия, отключив рациональное мышление

Искусственный цейтнот

По надуманной причине предлагается принять решение безотлагательно в условиях жестких временных рамок

Цель – «обработать» до момента «возврата» жертвы к рациональному поведению

Использование новостного фона

Санкции, валютные ограничения, пандемия, мобилизация, госизмена, дефицит и подорожание (лекарств, услуг и пр.)

Цель – сравнительная легкость убеждения, поскольку жертва уже частично подготовлена новостной повесткой и «в курсе»: расчет на отсутствие навыков фактчекинга у большинства населения

Оперирование личными фактами

Упоминание фактов из вашей жизни в рамках легенды мошенника, ссылки на ваших близких, друзей и коллег. Возможны технические приемы - IP-телефония

Цель – вызвать дополнительное доверие и рассеять возникающие сомнения. Расчет на неосведомленность о достаточно простом получении информации о каждом даже из открытых источников

ГЛАВНОЕ ПРАВИЛО – ВСЕГДА «БЕРИТЕ ПАУЗУ»,ЧТОБЫ ВСПОМНИТЬ, ЧТО КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ НИКОМУ НЕЛЬЗЯ ПЕРЕДАВАТЬ!

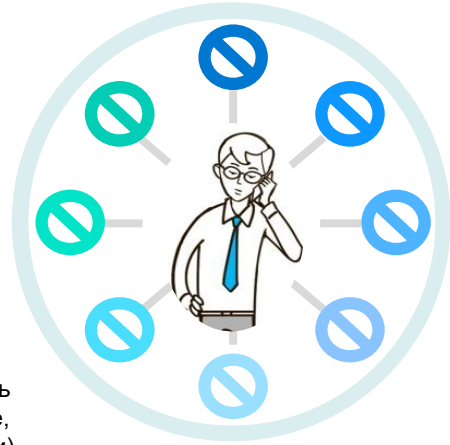
Пауза позволит успокоиться и начать рационально мыслить, а значит последовательно проверить информацию в первоисточниках, и связаться адресатам мошеннической «легенды» (банком, социальным фондом, полицией, маркетплейсом и своими близкими)

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Примеры звонков

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, налоговой инспекции** (предлагают получить материальные компенсации за неиспользованные льготы, сделав якобы возвратный «идентификационный» платеж; вернуть налог, предварительно оплатив ряд услуг)
- **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 от «представителя сотового оператора»** (предлагают перерегистрировать SIM-карту, пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного списываются деньги)



- **звонки из правоохранительных органов и силовых структур, следственного комитета, ФСБ и пр.** (псевдосотрудник госструктур сообщает, что сотрудник банка украл ваши ПДн и от вашего имени финансирует зарубежную армию, после чего предлагает «закрыть» дело о госизмене за взятку и помочь взять кредит)
- **звонки по заказам в маркетплейсах** (взломав учетку, делают отмену заказа, и после возврата вам средств звонят от имени продавца и ссылаясь на сбой платформы, просят перевести деньги напрямую, так как заказ якобы в пути)
- **звонки из МФЦ по поводу доступа на портал Госуслуг** (якобы для отправки вам письма в личный кабинет ПГУ, нужен одноразовый код)
- **«пристрелочные» звонки** (в течение недели вам звонят из разных служб и структур, уточняя информацию – так на вас собирают «досье» для применения какой-то схемы)

Новая примета времени – звонки переходят в мессенджеры

(эффект от ужесточения мер борьбы с телефонным мошенничеством*)

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.

МОШЕННИЧЕСТВО ЧЕРЕЗ РАССЫЛКУ СООБЩЕНИЙ

- 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

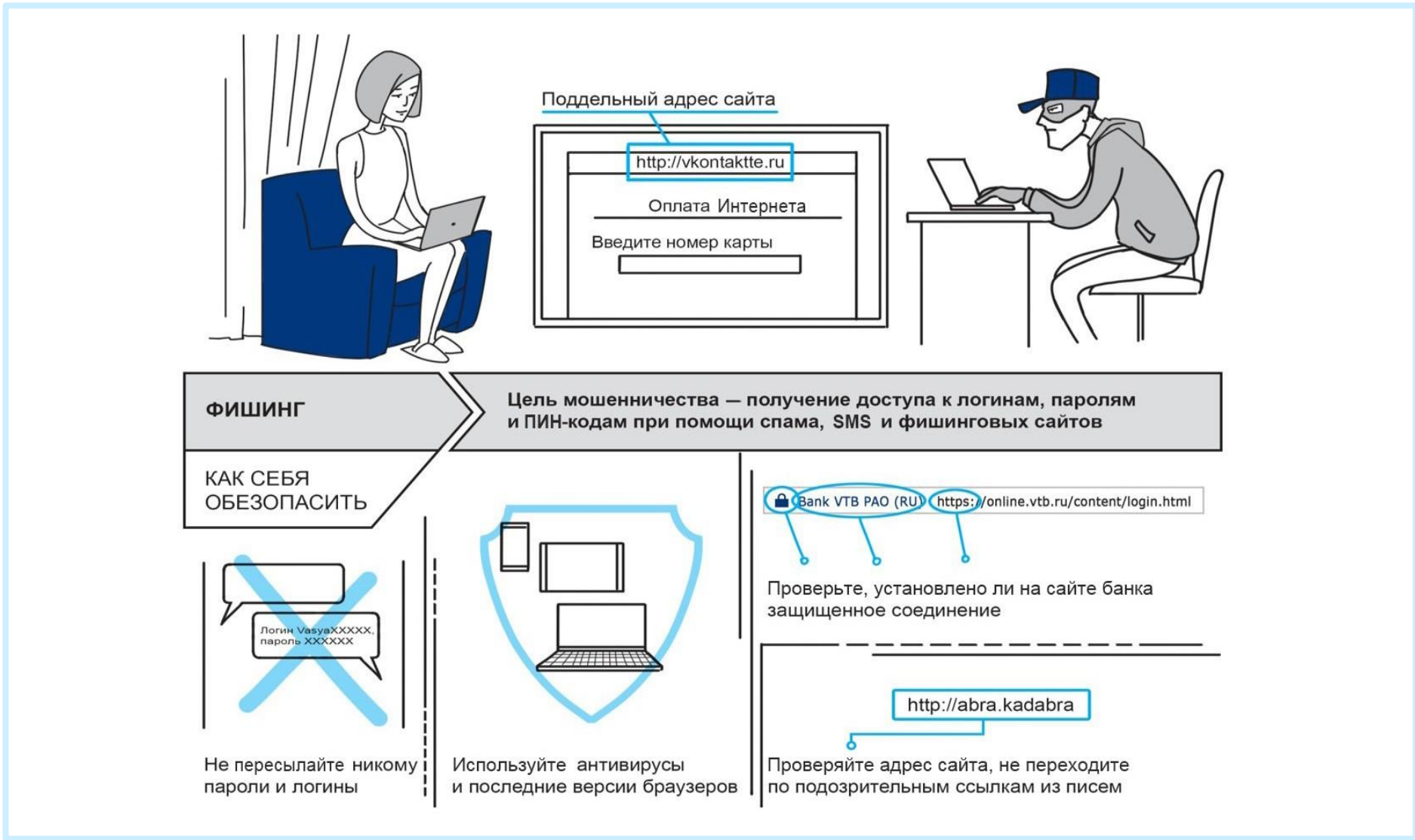
Рассылка сообщений в мессенджерах и через sms с указанием номера телефона для обратной связи

Рассылка 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 СООБЩЕНИЯХ, И НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ НИХ
- НЕ ОТПРАВЛЯЙТЕ ОТВЕТНЫЕ СООБЩЕНИЯ — ЭТО РИСК ПОДПИСАТЬСЯ НА ПЛАТНУЮ УСЛУГУ
- БУДЬТЕ БДИТЕЛЬНЫ – ПРИ ВЗЛОМЕ АККАУНТОВ МОШЕННИЧЕСКИЕ СООБЩЕНИЯ МОГУТ ПУБЛИКОВАТЬСЯ В ЧАТАХ МЕССЕНДЖЕРОВ, И РАССЫЛАТЬСЯ ОТ ИМЕНИ ВАШИХ ЗНАКОМЫХ

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
Bank VTB PAO (RU)
https://online.vtb.ru/content/login.html
Проверьте, установлено ли на сайте банка защищенное соединение
Логин VasyaXXXXX, пароль XXXXXX
Не пересылайте никому пароли и логины
Используйте антивирусы и последние версии браузеров
http://abra.kadabra
Проверяйте адрес сайта, не переходите по подозрительным ссылкам из писем

СНИФФЕРИНГ

СНИФФЕРИНГ

Цель мошенничества – перехват данных мошенниками в общественных местах

КАК СЕБЯ ОБЕЗОПАСИТЬ

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