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-канала «Финансовая грамотность со Светланой Толкачевой»

ХОЧУ ЗНАТЬ БОЛЬШЕ

www.youtube.com/c/SvetlanaTolkacheva

https://zen.yandex.ru/tolkacheva_sv

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

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 17 лет работы в финансовых компаниях, включая 13 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%

У нас сейчас уже 75% платежей — это безналичные, только 25% — наличные.

Из выступления 1-го зам.председателя ЦБ РФ О. Скоробогатовой на Евразийском женском форуме, октябрь 2021

По итогам 2020 года мы вышли на уровень около 70% безналичных платежей…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 12.02.2021 и в ГД в ноябре 2019

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»

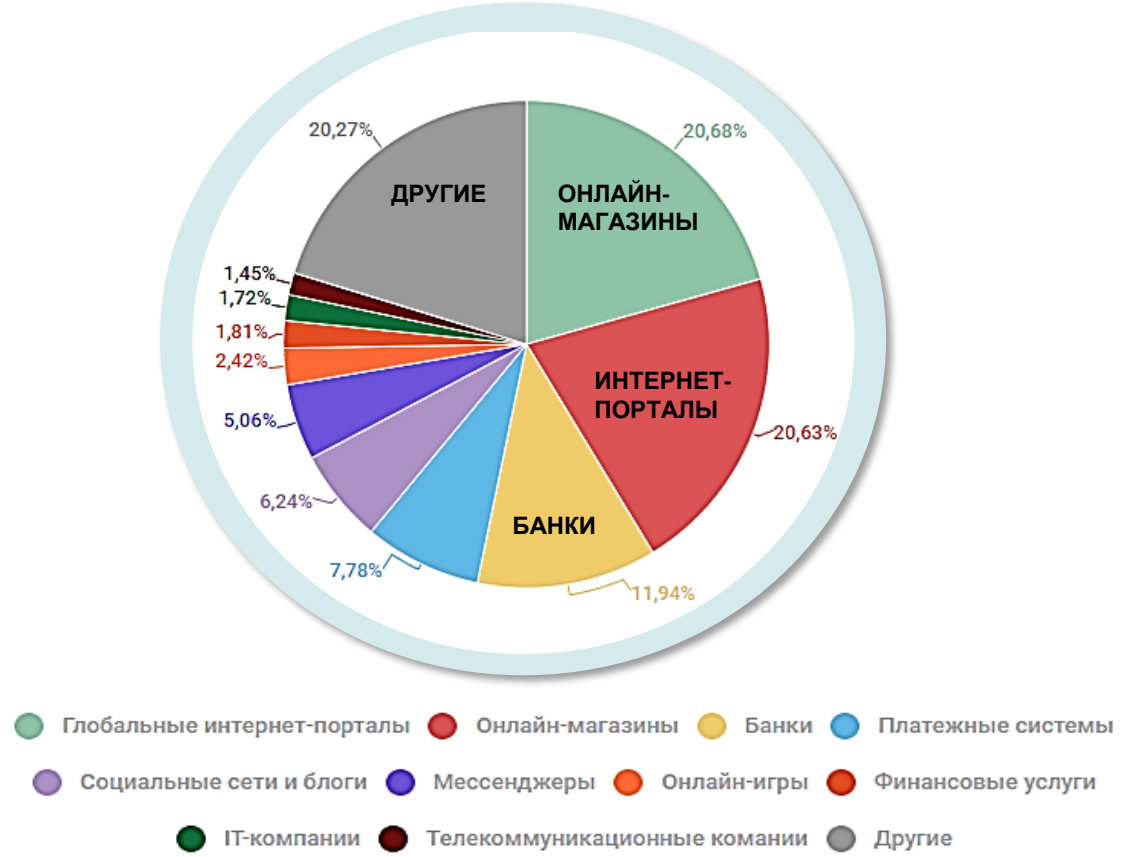
МИШЕНИ ФИШИНГОВЫХ АТАК

ОРГАНИЗАЦИИ — МИШЕНИ ФИШИНГОВЫХ АТАК В III КВАРТАЛЕ 2021*

ФИШИНГ (от англ fishing — «рыбная ловля, выуживание») - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (финансовым данным, а также логинам и паролям)

Это достигается путем:

- **проведения массовых рассылок электронных писем** от имени популярных брендов,
- **личных сообщений внутри различных сервисов**, например, от имени банков или внутри социальных сетей
- также перейти на фишинговый сайт можно **путем клика на баннеры,** всплывающие при открытии страниц в Интернете.



В ТОП-3 ПО КОЛИЧЕСТВУ ФИШИНГОВЫХ АТАК ВХОДЯТ ОНЛАЙН-МАГАЗИНЫ, ГЛОБАЛЬНЫЕ ИНТЕРНЕТ-ПОРТАЛЫ И БАНКОВСКИЙ СЕКТОР – совокупная доля атак на эти организации составила **53,25%****

* По данным с сайта https://www.kaspersky.ru/.

** Рейтинг категорий атакованных фишерами организаций основан на срабатываниях компонента системы «Антифишинг» на компьютерах пользователей.

СТАТИСТИКА КИБЕРПРЕСТУПЛЕНИЙ

ПО ДАННЫМ СТАТИСТИКИ МВД РФ за январь-ноябрь 2021*

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	**1853148**	**-2,0**	**948298**	**0,0**
совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	494126	7,1	120586	40,6

27 % - доля

24 % раскрыто

СТРУКТУРА

Почти КАЖДОЕ ЧЕТВЕРТОЕ – это киберпреступление

Из них:

- **БОЛЕЕ ПОЛОВИНЫ (56%) относится к категориям ТЯЖКИХ И ОСОБО ТЯЖКИХ (277 тыс.)**
- **70 % совершено с использованием СЕТИ ИНТЕРНЕТ (335 тыс.)**
- **СВЫШЕ 40 % - с помощью средств МОБИЛЬНОЙ СВЯЗИ (201 тыс.)**
- **БОЛЕЕ 30 % - с использованием пластиковых карт (155 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 сообщило, что 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 46 РАЗ!

2013 - 11 тыс.
2014 - 44 тыс.
2016 - 66 тыс.
2019 - 294 тыс.
2020 - 510 тыс.
2021 - ?

* Из Отчета МВД РФ за январь-ноябрь 2021 года «Состояние преступности в России»

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ В ЦИФРОВОМ МИРЕ

ИДЕНТИФИКАЦИЯ — КОМУ И ЗАЧЕМ НУЖНА?

ЦИФРОВЫЕ КОММУНИКАЦИИ

обмен информацией между устройствами через Интернет

- публичные — для открытого обмена информацией (соцсети, форумы, блоги)
- частные: в том числе для обмена значимой/ финансовой информацией (чат-боты, мессенджеры)

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ

набор данных клиента, используемых системой для его идентификации

- государственные системы: ИНН, СНИЛС, паспорт, регистрация на портале «Госуслуги»
- частные системы: Facebook, «ВКонтакте» и другие

ГРАЖДАНИН

ЦИФРОВЫЕ РАСЧЕТЫ

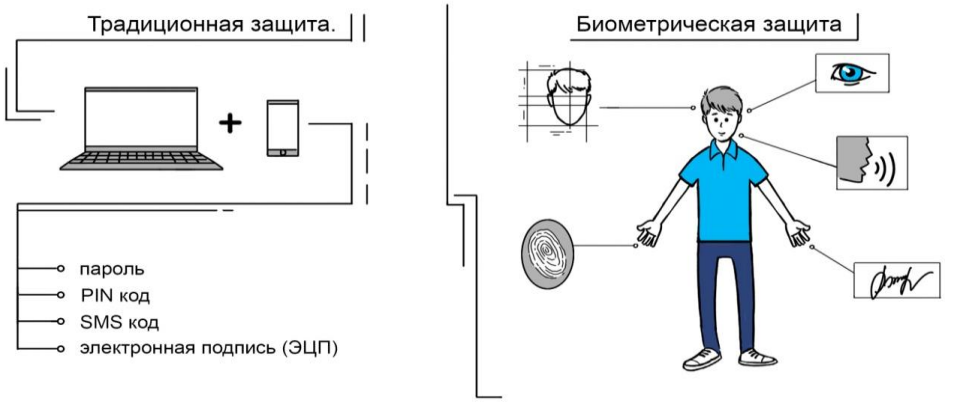
система безналичных расчетов между контрагентами с использованием банковских счетов, пластиковых карт, электронных кошельков

ГОСУДАРСТВО

ПЕРСОНАЛЬНЫЕ ДАННЫЕ НИКОМУ НЕЛЬЗЯ ПЕРЕДАВАТЬ!

ТРАДИЦИОННАЯ И БИОМЕТРИЧЕСКАЯ ЗАЩИТА

БИОМЕТРИЧЕСКИЕ ДАННЫЕ - это уникальные биологические и физиологические характеристики, которые позволяют установить личность человека (опечаток пальца, изображение лица, голос, радужная оболочка глаза, рисунок вен ладони и пальца, кровь и др.).



Карта точек банковского обслуживания ДЛЯ сдачи биометрии размещена на сайте ЦБ РФ. Сдать биометрию теперь можно и в МФЦ

«Компрометация биометрических данных — это самое страшное, что может произойти. Если человек доверил экосистеме — неважно, частной или государственной — свои биометрические данные, и эта система не оправдала его доверия, то у человека в цифровом будущем сломана жизнь» - *замминистра финансов Алексей Моисеев*

СОЧЕТАНИЕ ДВУХ ВИДОВ ЗАЩИТЫ ОБЕСПЕЧИВАЕТ ЕЕ БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ!

ЗАКОНОДАТЕЛЬСТВО

- 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 было отложено**
- В 30.12.2021 подписан закон о создании единой государственной биометрической системы. ЕБС переведена в статус ГИС, порядок функционирования утверждает Правительство РФ. Обязательная аккредитация для госорганов, использующих ЕБС и иные ГИС. Граждане смогут самостоятельно размещать свои биометрические образцы. Администратор ЕБС - Минцифры, банки и другие коммерческие организации не смогут сохранять копии данных (только сбор и передача). В 2022 году будет разработан механизм передачи шаблонов клиентов банков в ЕБС. Вступление в силу с 01.09.22.

* Внесение изменений в №115-ФЗ от 07.08.2001 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», №395-1 от 02.12.1990 «О банках и банковской деятельности»

** Принятие поправок к №115-ФЗ от 07.08.2001 было отложено в 2019 на неопределенный срок в связи с вопросами силовых структур и бизнеса

***№ 441-ФЗ от 30.12.2021 "О внесении изменений в статью 15-3 ФЗ "Об информации, информационных технологиях и о защите информации" и статьи 3 и 5 ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации»

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 - Министерство цифрового развития, связи и массовых коммуникаций

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

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 предоставлять банкам и страховщикам информацию о себе и получать услуги полностью в цифровом виде, не посещая офис.

УЧАСТНИКИ ПИЛОТНОГО ПРОЕКТА

- 20 банков, 4 страховщика, а также МФО и операторы финансовых платформ (по согласованию с ЦБ)***. ЦБ планирует в 2022 открыть доступ к ЦП россиян новой группе организаций - профучастникам рынка ценных бумаг, НПФ, УК инвестфондов, БКИ и АСВ
- Согласие на обработку сведений из ЕСИА дали более 1,55 млн.человек

СВЕДЕНИЯ В ЦП

На текущий момент в ЦП содержатся записи более 30 типов (паспорт, адрес, ИНН, водительские права, электронная трудовая книжка и др.), планируется дальнейшее расширение перечня

КОГДА ПРИМУТ ЗАКОН?

В ГД законопроект**** на стадии рассмотрения в первом чтении. Эксперимент был признан успешным и продлен до конца 2022 года

В БУДУЩЕМ ЦИФРОВОЙ ПРОФИЛЬ СТАНЕТ УНИВЕРСАЛЬНЫМ ИНСТРУМЕНТОМ УДАЛЕННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ ГРАЖДАНАМИ, ГОСУДАРСТВОМ И КОМПАНИЯМИ

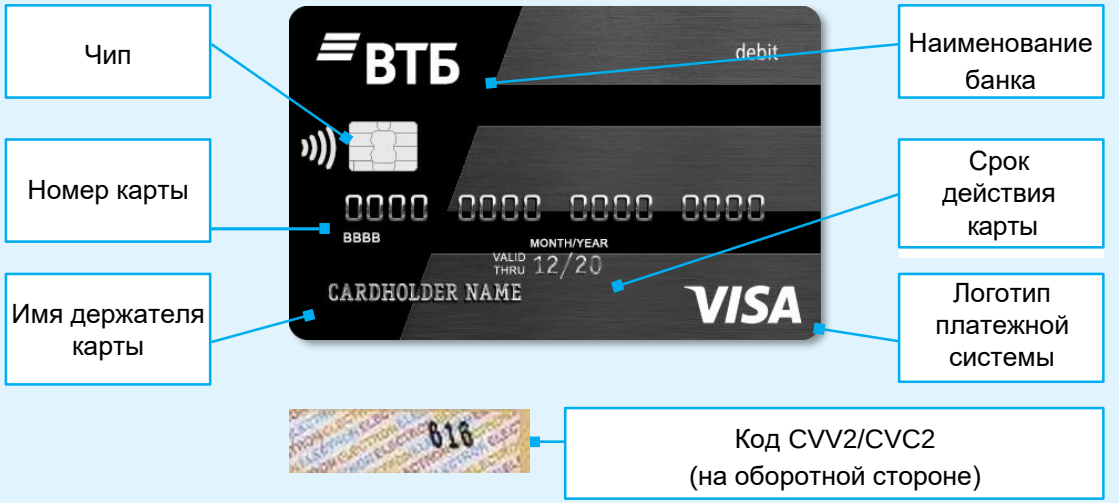
* Государственные информационные системы

** 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», от 27.03.2020 N 350 и от 24.11.2020 N 1911 (внесение изменений в ПП № 710) https://cbr.ru/press/event/?id=6723

*** Также к ЦП по согласованию с Минцифрой могут подключиться работодатели — юридические лица, с которыми граждане, ищущие работу, планируют вступить в трудовые отношения

**** 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

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 телефон, привязанный к карте)
- **Используйте мобильные приложения с технологиями для бесконтактной оплаты (NFC)**

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!**

* По данным ЦБ, с начала пандемии количество мошеннических телефонных звонков выросло примерно на 300%. На мошенников работают целые так называемые «черные call-центры» (могут находится заграницей, и даже в тюрьмах*) На ликвидацию последних ФСИН планирует потратить 3 млрд.руб. По инициативе Минкомсвязи и МВД создана межведомственная рабочая группа по противодействию телефонному мошенничеству. В нее вошли также представители ФСБ, Роскомнадзора, ЦБ РФ, банков и операторов связи

** С 01.12.21 в силу вступили изменения в закон "О связи". Оператор 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.

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!

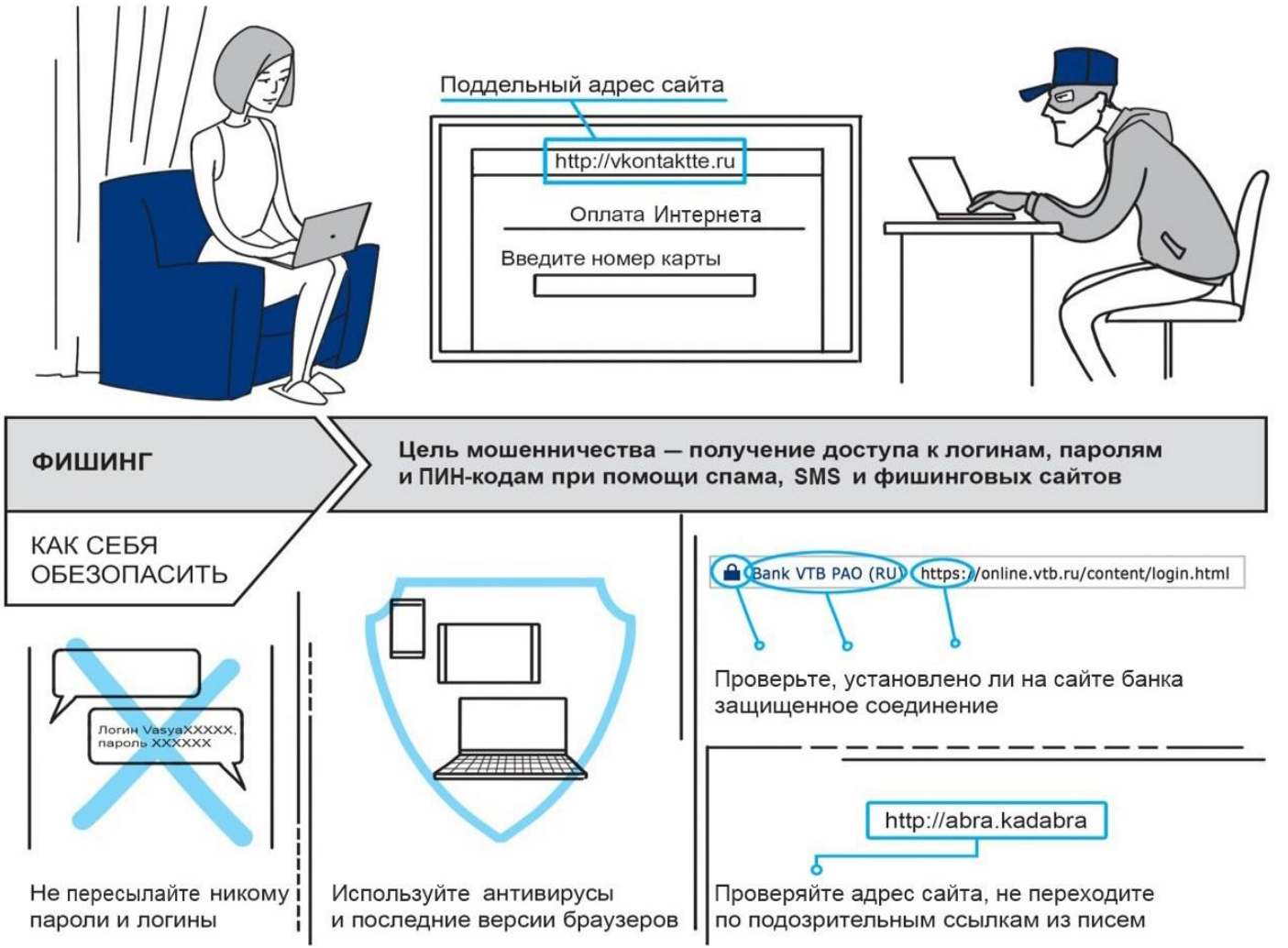
Извините, по ошибке положила вам 500 руб. Прошу вернуть на этот номер

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

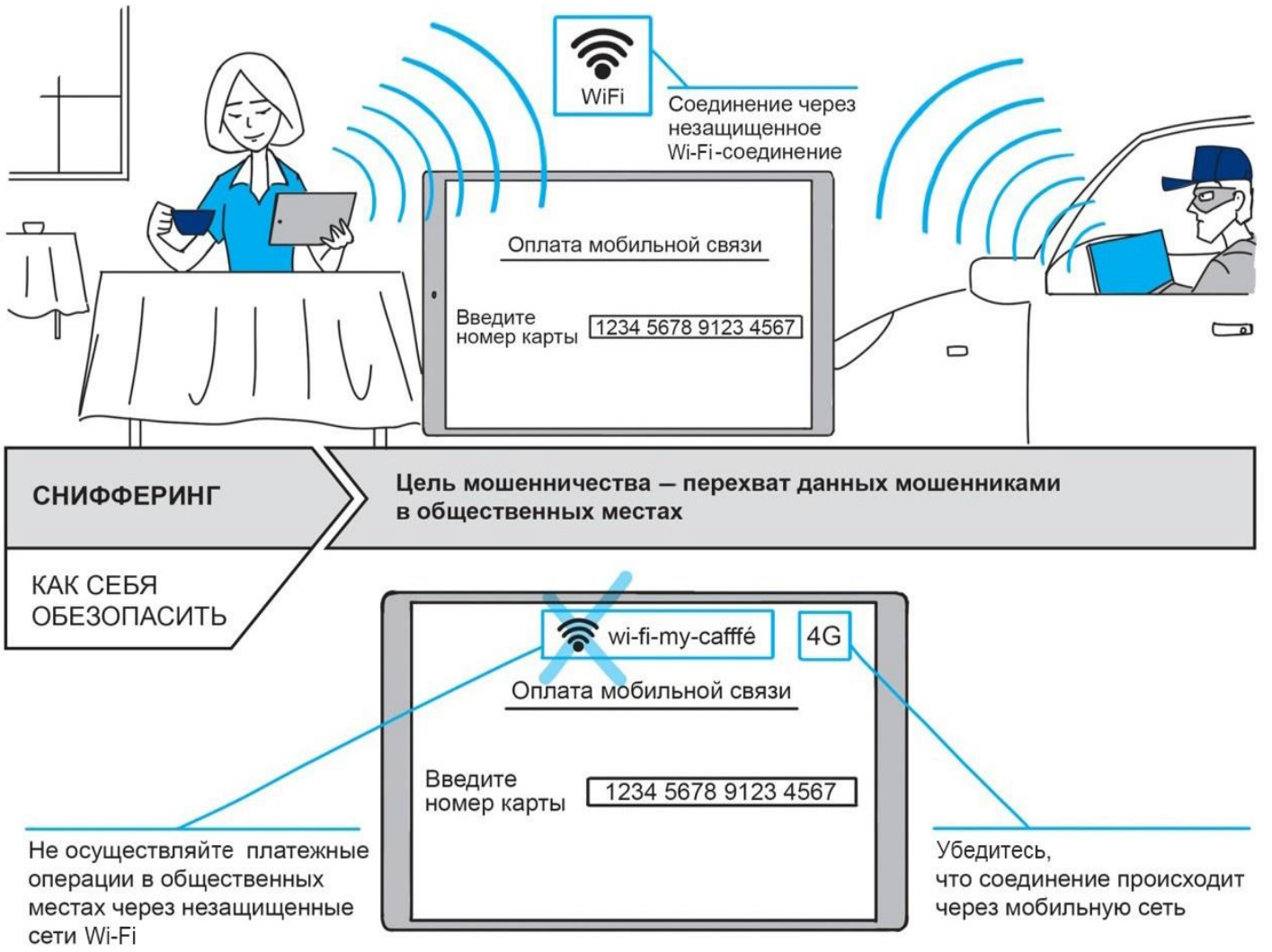
Иванова Ирина Викторовна. Согласно геолокации, вами был нарушен режим карантина согласно ст. 20.6.1 КоАП РФ. Вам необходимо оплатить штраф согласно постановлению ФСИН №168-322 от 09-04-2020года в размере 4000 рублей на номер 8 800 XXX XX XX

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

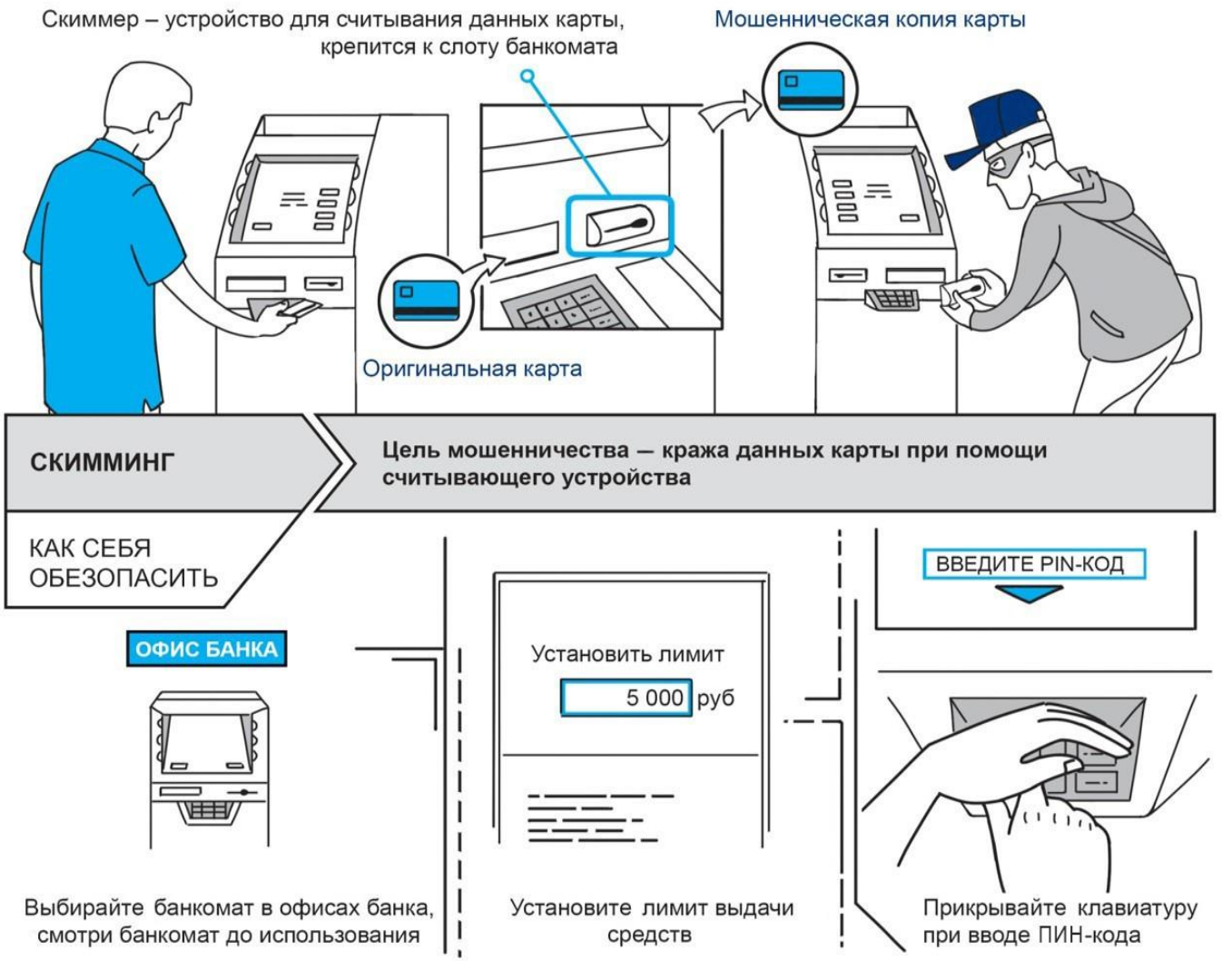
ФИШИНГ


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

СКИММИНГ


Скиммер – устройство для считывания данных карты, крепится к слоту банкомата
Мошенническая копия карты
Оригинальная карта
СКИММИНГ
Цель мошенничества — кража данных карты при помощи считывающего устройства
КАК СЕБЯ ОБЕЗОПАСИТЬ
ОФИС БАНКА
Выбирайте банкомат в офисах банка, смотри банкомат до использования
Установить лимит
5 000 руб
Установите лимит выдачи средств
ВВЕДИТЕ PIN-КОД
Прикрывайте клавиатуру при вводе ПИН-кода

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).

**ЕСЛИ ХОЧЕШЬ БЫТЬ БОГАТЫМ,
НУЖНО БЫТЬ ФИНАНСОВО ГРАМОТНЫМ.**

**РОБЕРТ КИЙОСАКИ,
АМЕРИКАНСКИЙ ПРЕДПРИНИМАТЕЛЬ**

Толкачева Светлана

www.youtube.com/c/SvetlanaTolkacheva

https://zen.yandex.ru/tolkacheva_sv

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

ХОЧУ ЗНАТЬ БОЛЬШЕ