



# Информационная безопасность

# Основные принципы ИБ

---

- 1 — своевременное обновление Вашего ПО;
- 2 — использование антивирусов;
- 3 — двухфакторная аутентификация (2FA) на всех сервисах;
- 4 — правильная парольная политика;
- 5 — соблюдать правила защиты от фишинга.



# Обновление ПО

---

1

Любая компьютерная программа или, как мы будем говорить чаще всего, ПО (программное обеспечение) пишется людьми, пусть и высококвалифицированными.

Программисты, как все люди, допускают ошибки. А эти ошибки используются злоумышленниками для того, чтобы получить доступ к атакуемой системе, украсть интересующую их информацию и много всего другого плохого. Так и появляются уязвимости, которые являются «окном» для хакеров.

Поэтому существующие в Вашем ПО уязвимости надо закрывать. И закрывать их надо своевременно — это существенно сократит опасность того, что ваш компьютер или сеть будут взломаны.

Отсюда следует **основной гигиенический прием информационной безопасности — своевременное обновление Вашего ПО.**

Устанавливайте обновления только из официальных источников - либо через механизм обновления внутри самой программы, либо скачивайте их с официальных сайтов производителя.



# Использование антивирусов

---

2

**Вредоносная программа** – программа, которая действует без ведома пользователя и изначально предназначена для осуществления скрытых вредоносных действий (кража информации, осуществление скрытого контроля над зараженной системой, блокировка ее работы, шифрование пользовательской информации и др.).

Вот некоторые из них:

- **троянский конь** или **троян** - вредоносы, маскирующиеся под легальные компьютерные программы;
- **вирусы** - фрагменты вредоносного кода, встраивающиеся в другие программы;
- **шпионские программы (клавиатурные шпионы, инфостилеры и пр.)** - вредоносные программы, предназначенные для сбора и кражи данных с зараженного компьютера;
- **вымогатели** - вредоносы, предназначенные для шифрования и кражи пользовательских данных с целью дальнейшего требования преступником выкупа с пользователя;
- **сетевые черви** - вредоносные программы, самостоятельно распространяющиеся через компьютерные сети;
- **руткиты** - специализированное вредоносное ПО, позволяющее злоумышленнику скрытно получать удаленный доступ и контроль над зараженной системой;
- **боты** - вредоносные программы, делающие зараженное устройство частью большой бот-сети и осуществляющие какие-то вредоносные действия по команде из вне.

**Установка и активное использование антивирусных пакетов – это одно из основных правил гигиены информационной безопасности** наряду с необходимостью своевременного обновления имеющихся на компьютере программ.

---



# Двухфакторная аутентификация (2FA)

---

3

Аутентификация (авторизация, идентификация) пользователя – процедура получения доступа к принадлежащему пользователю информационному ресурсу путем подтверждения своей подлинности.

Двухфакторная аутентификация – это такая аутентификация, в процессе которой пользователь подтверждает свою подлинность с помощью второго дополнительного фактора. Например, цифрового кода.

Когда вы устанавливаете любой мессенджер на своё устройство, то подтверждаете принадлежность этого устройства исключительно своим телефонным номером, на который придет сообщение или звонок с кодом подтверждения. В этом случае если злоумышленник каким-то образом сможет представиться вашим телефонным номером, например, перехватив смс-сообщение или продублировав вашу сим-карту, то он захватит ваш аккаунт мессенджера. При 2FA такой способ «взлома» не срабатывает, т.к. необходимо ввести дополнительный код фразы, которая придет на Вашу электронную почту.

2FA актуальна для любых сервисов, имеющих аутентификацию пользователей – электронная почта, госуслуги, сервисы онлайн банков и т.д. и т.п.



# Правильная парольная политика

4

password	12345678	наташа
123456	123456789	марина
11111	12345	максим
1q2w3e	qwerty123	кристина
qwerty	123123	андрей
йцукен	пароль	люблю
любовь	привет	

По данным NordPass, 2022



## Как злоумышленники узнают пароли?

### 1) Перебор

**перебор слов** – использование программы, которая автоматически комбинирует распространенные слова из словаря, используя их часто встречающиеся сочетания. Пользователи стараются придумывать пароли, которые легко запомнить, так что подобные методы взлома следуют очевидным шаблонам.

**перебор символов** – используются автоматические программы, перебирающие все возможные сочетания символов до тех пор, пока не найдется ваш пароль. Короткие пароли в некоторых случаях удается подобрать буквально за несколько часов.

2) **Фишинг** – это попытка заставить вас самостоятельно отдать мошеннику деньги или важную информацию.

3) **Утечки данных** – получение доступа к базам данных через взлом корпоративных систем и последующая их продажа и публикация в открытом доступе. Утечки данных представляют для вас особенно большую угрозу, если вы используете один и тот же пароль в разных местах: весьма вероятно, что ваши старые аккаунты могут быть скомпрометированы, и это открывает для злоумышленников доступ и к другим вашим данным.

# Правильная парольная политика

4

*Сколько времени займет у хакера взлом паролей*

Кол-во символов	Только числа	Буквы в нижнем регистре	Буквы в нижнем и верхнем регистре	Числа и буквы в нижнем и верхнем регистре	Числа и буквы в нижнем и верхнем регистре, символы
6	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
7	мгновенно	мгновенно	2 сек.	7 сек.	31 сек.
8	мгновенно	мгновенно	2 мин.	7 мин.	39 мин.
9	мгновенно	10 сек.	1 час	7 часов	2 дня
10	мгновенно	4 мин.	3 дня	3 недели	5 месяцев
11	мгновенно	2 часа	5 мес.	3 года	34 года
12	2 сек.	2 дня	24 года	200 лет	3 тыс. лет
13	19 сек.	2 месяца	1 тыс. лет	12 тыс. лет	202 тыс. лет
14	3 мин.	4 года	64 тыс. лет	750 тыс. лет	18 млн. лет
15	32 мин.	100 лет	3 млн. лет	48 млн. лет	1 блн. лет
16	5 часов	3 тыс. лет	173 млн. лет	3 блн. лет	92 блн. лет
17	2 дня	69 тыс. лет	9 блн. лет	179 блн. лет	7 бллр. лет
18	3 недели	2 млн. лет	467 блн. лет	11 бллр. лет	438 бллр. лет



# Правильная парольная политика

---

4

Есть 2 варианта реализации парольной политики.

**Первое** - использовать менеджер паролей. Плюс этой технологии - это автоматизация всей работы с паролями. Минус – это точно такое же программное обеспечение, которое может быть взломано и за его безопасностью нужно следить.

**Второе** - использовать правильный способ формирования стойких и запоминающихся паролей.

## небезопасно

- Листочек на экране
- Заметка в телефоне
- Сообщение в избранном
- В записной книжке

## безопасно

- Парольный менеджер
- В браузере

## супербезопасно

- OnePass





# Правильная парольная политика

4

Парольная фраза

Стол это вам не стул

Заменяем буквы на спецсимволы

Ст0л\_эт0\_в@м\_не\_стУл

Добавляем пару цифр

Ст0л\_эт0\_в@м\_не\_стУл98

Один и способ создания сложного пароля для электронной почты "bestmail@yandex. ru" :

1. Выбираем достаточно длинную кодовую фразу. Например, "вместе весело шагать по просторам и конечно припевать лучше хором".
2. Выкидываем из нее все короткие слова – "вместе весело шагать просторам конечно припевать лучше хором".
3. Записываем ее в английской транслитерации – "vmeste veselo shagat prostoram conechno pripevat luchshe horom".
4. Выбираем спецсимвол – например, \*.
5. Вам надо придумать пароль для конкретного логина. Например, для почты "bestmail@yandex. ru".
6. Считаем количество символов в названии сайта yandex, оно равно 6.
7. Выбираем из кодовой фразы седьмое (6+1) слово – это будет "luchshe". Если количество слов в кодовой фразе меньше получившегося числа, то просто считаем по второму кругу. И т.д.
8. Берем первые и последние буквы из адреса почты и названия почтового сервиса – "bestmail@yandex. ru". Первые оставляем неизменными, последние превращаем в прописные – получилось b,L,y,X.
9. Чередуем буквы из выбранного слова кодовой фразы и полученные из названия адреса и сервиса буквы – lbuLcyhXshe.
10. В начало пароля добавляем число букв в выбранном слове кодовой фразы luchshe, то есть 7. В конец пароля добавляем выбранный ранее спецсимвол - \*.

Ваш пароль для электронной почты "bestmail@yandex. ru" - "7lbuLcyhXshe\*\*".



# Правильная парольная политика

---

4

## Беспарольная авторизация

- Вход по Face ID, Touch ID
- Данные нигде не хранятся
- Фишинг не пройдет
- Утечка невозможна

- Пароль должен быть сложным, но запоминающимся.
- Старайтесь его регулярно менять и не использовать один и тот же пароль во всех сервисах.
- Хороший пароль содержит не менее 8 символов, а лучше 10-12 и больше: цифры, буквы разного регистра, специальные символы (например: %, &, #). Чем больше в пароле разнотипных символов, тем он менее предсказуем.
- Кодовые фразы надежнее, если слова в них идут в неожиданном порядке. Даже если вы используете обычные слова, берите такие, которые не связаны друг с другом по смыслу, и расставляйте их нелогичным образом. Это поможет противостоять словарному подбору. Можно использовать фразу на русском, но набрать ее на латинской раскладке (и наоборот). Использовать кодовой фразе есть ненормативные слова и орфографические ошибки



# Правильная парольная политика

---

4

Чтобы обеспечить безопасность:

- Не записывайте пароли на бумажках.
- Не храните пароли в приложении «Заметки» на телефоне.
- Не сохраняйте пароли в автозаполнении браузера.

1. **Активируйте двухфакторную аутентификацию** на всех ваших самых ценных аккаунтах.
2. **Часто обновляйте самые важные пароли.** И старайтесь, чтобы новый пароль был не похож на старый. Обязательно меняйте их хотя бы для следующих сервисов: *интернет-банкинг; оплата счетов; основной пароль менеджера паролей; социальные сети; электронная почта; личные кабинеты телефонного оператора и интернет-провайдера.*



# Правила защиты от фишинга

---

5

## Психологические векторы атак

Невнимательность

Любознательство

Страх

Жадность

Раздражение

Желание помочь

Авторитет

Срочность

**Фишинг** – хакерский прием, когда злоумышленники подменяют или подделывают какое-либо сообщение или ресурс на свой вариант, содержащий вредоносное вложение. Это может быть СМС, электронное письмо, сообщение в социальной сети или мессенджере, поддельный сайт, форма входа в Интернет-сервис и прочее.

Реальные примеры фишинга:

- электронное письмо, маскирующееся под письмо службы кадров, содержащее вредоносную ссылку на новый табель положенности или уведомление о выплате премии, в котором сидит вирус (такое ведь никто не пропустит, да?);
- электронное письмо, маскирующееся под уведомление о получении штрафа ГИБДД и содержащее ссылку на поддельную страницу входа в Госуслуги, откуда логин и пароль пользователя попадают прямо к хакеру;
- создание клона легитимной сети Wi-Fi, после подключения к которой пользователю будут представлены поддельные страницы некоторых сервисов, например тех же Госуслуг или банковского личного кабинета;
- поддельное сообщение в социальной сети от имени службы поддержки, содержащее ссылку на поддельную форму, в которую требуется внести свои логин и пароль;
- поддельная поисковая выдача, когда вместо легитимного сайта пользователю подставляют поддельный, на котором либо сидит вирус, либо собираются данные пользователя, в том числе данные банковских карт; и т.д. и т.п.



# Правила защиты от фишинга

5

## Социальная инженерия и фишинг

### Мошенник хочет получить

- логин-пароль
- данные двухфакторной аутентификации
- коды из смс
- данные банковской карты
- пин-коды
- ваши деньги

### Мошенник очень

- хорошо разбирается в видах психологического воздействия
- умеет манипулировать
- подготовлен
- хочет получить данные
- и заработать



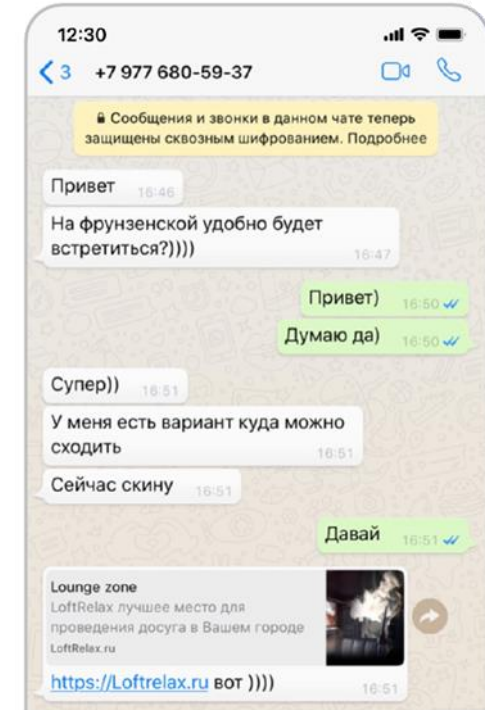
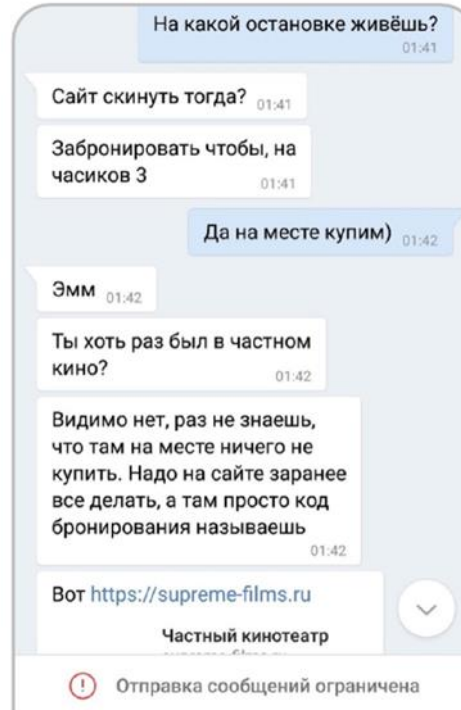
# Правила защиты от фишинга

5

## Любопытство и невнимательность

кейс 1

Что не так?

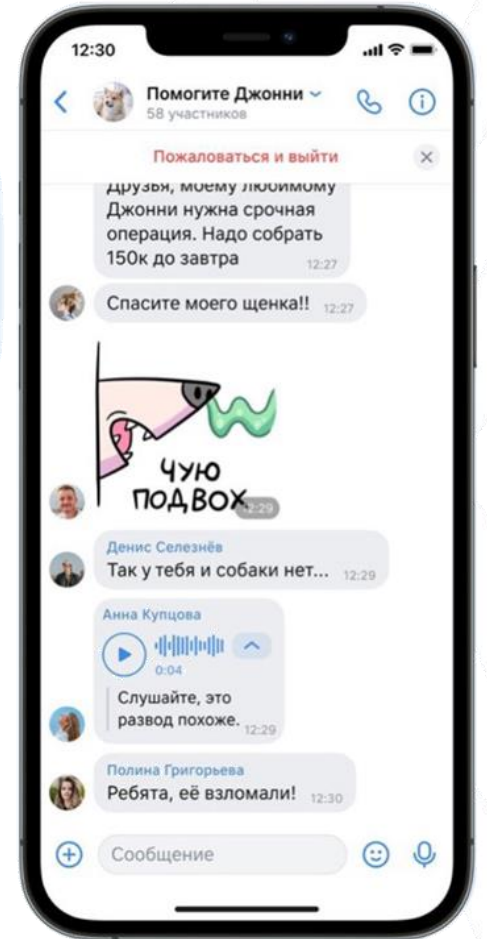
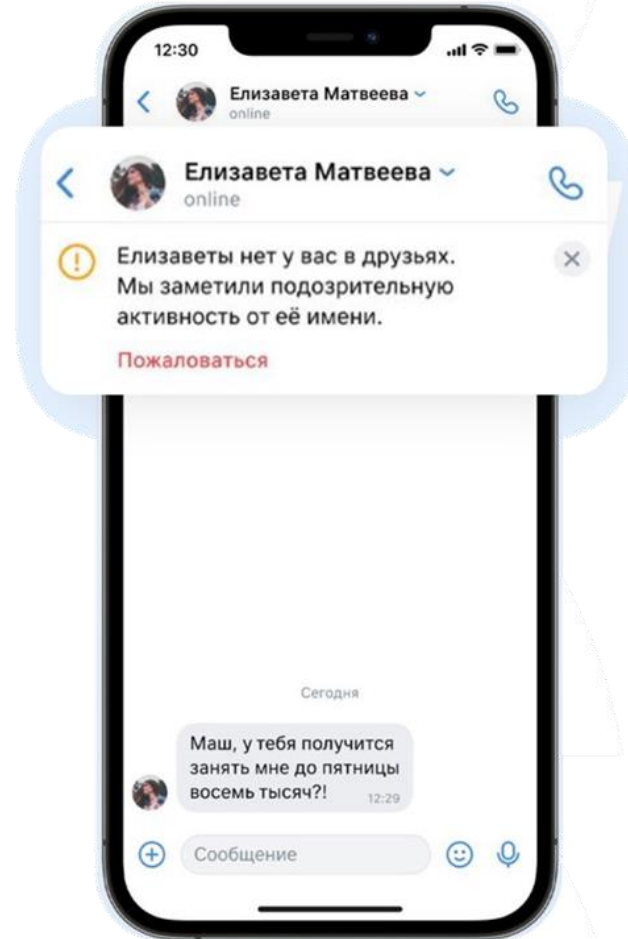
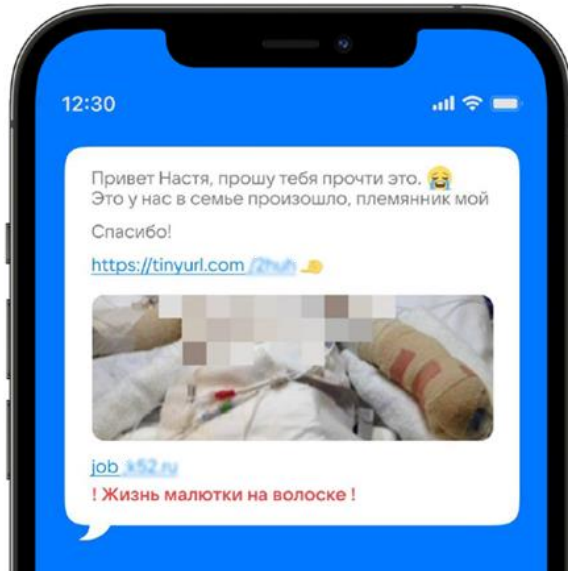


# Правила защиты от фишинга

5

## Желание помочь

кейс 2



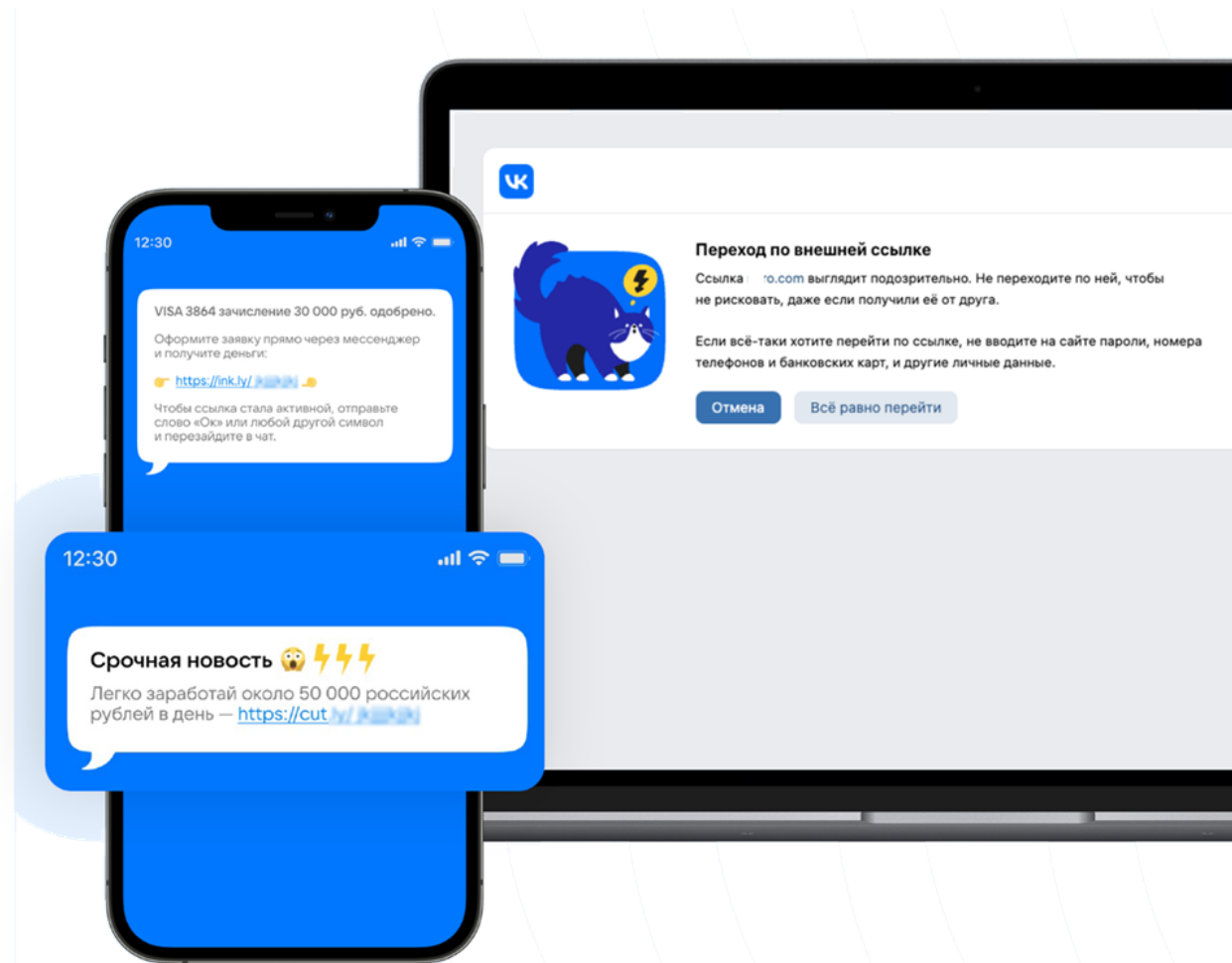
# Правила защиты от фишинга

5

## Жадность

кейс 3

- Самые популярные уловки мошенников: выигрыш в сети, высокий заработок в сети, большие скидки на популярные (или ушедшие) бренды
- Бесплатные деньги — только в мышеловке: звучит заманчиво, но соглашаться я, не буду





# Правила защиты от фишинга

---

5

Российские интернет-пользователи каждый день пытаются перейти на фишинговые ресурсы примерно 1,5 млн раз, в 90% случаев это переходы с мобильного телефона, в том числе из мессенджеров, писем и приложений.

На текущий момент с ноября 2023 года «Яндекс браузер» при помощи искусственного интеллекта (ИИ) выявил более 400 тыс. мошеннических сайтов.

*В последнее время фишинговые сайты стали всё чаще имитировать приложения банков, платформы для работы с криптобиржами и дейтинговые сервисы, которые магазины приложений у себя удалили. А также сайты, оказывающие помощь жертвам мошенников.*



# Правила защиты от фишинга

---

5

1. Правило первое, оно же основное, – не доверяйте никому и ничему. Помните – если у вас паранойя, это еще не значит, что за вами никто не следит. Если у вас есть хоть капля подозрения в том, что пришедшее уведомление, письмо или сайт являются подлинным, не постесняйтесь перепроверить.

Обратите внимание на то, что электронная почта вашего коллеги или страница Вконтакте вашего друга могут быть взломаны. Поэтому верный обратный адрес отправителя – не гарантия того, что сообщение настоящее. Лучше оценить мог ли ваш адресат направить вам такое сообщение. Если это выглядит странно – перепроверяйте.

*Интересный факт – часто хакеры искусственно увеличивают размер прикрепленного к фишинговому сообщению файла, например до 600 или 700 МБ. Из-за ограничений ряда антивирусных сервисов на размер проверяемого файла такое вложение может проскочить через защиту. Обращайте на это внимание, вложенный документ вряд ли будет занимать больше 20 Мб, даже если это презентация.*



# Правила защиты от фишинга

---

5

2. Проверяйте адреса и ссылки в сообщении, они могут быть подделаны. Злоумышленники подделывают как адрес отправителя, подставляя похожую на легитимную почту, так и ссылки в тексте самого сообщения. Более того, ссылка может быть отображать одну страницу, а переход по ней осуществляться на другую. Поэтому имеет смысл при наличии подозрений вручную ввести нужный адрес в новом окне браузера.
3. Не надо необдуманно тыкать во все ссылки и баннеры, которые вы видите. А если уж случайно потыкали – не вводите никаких персональных (особенно банковских) данных.
4. Не давайте никаких разрешений на загрузку и установку «необходимых обновлений» или «отсутствующих драйверов» при открытии вложенных файлов или переходы по вшитой ссылке. Скорее всего там будет вирус.
5. Обязательно подключите везде, где можно, двухфакторную аутентификацию, своевременно обновляйте ПО с официальных сайтов и установите антивирусные программы.



# Правила защиты от фишинга

---

5

Чек-лист, чтобы  
не попасться  
на фишинг

1

Сообщение  
неожиданное?

4

Есть акцент  
на срочность?

2

Отправитель  
не знаком?

5

Содержит  
потенциально  
опасные элементы?

3

Вызывает эмоцию?



# Правила защиты от фишинга

---

5

Если  
ответили да

1

Не торопитесь,  
дайте себе паузу

2

Критично относитесь  
к любому входящему  
контенту

3

Не стесняйтесь уточнить  
у друга/поддержки/службы  
безопасности/магазина —  
точно ли с этим  
предложением все хорошо

4

Пожалуйста  
на нехороший контент,  
а на хороший —  
не жалуйтесь



# Еще о правилах ИБ

---

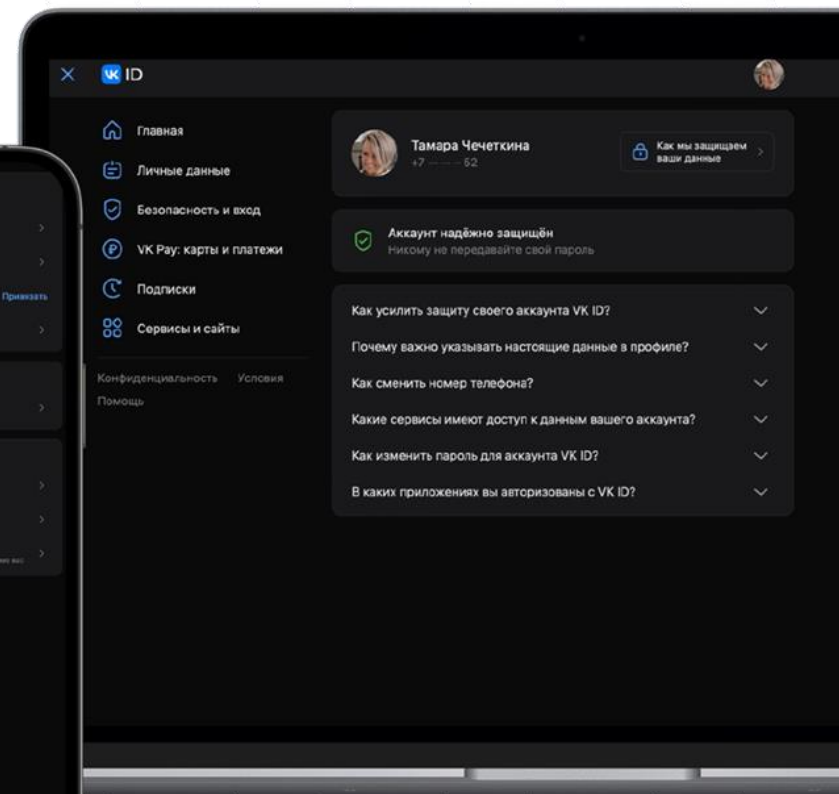
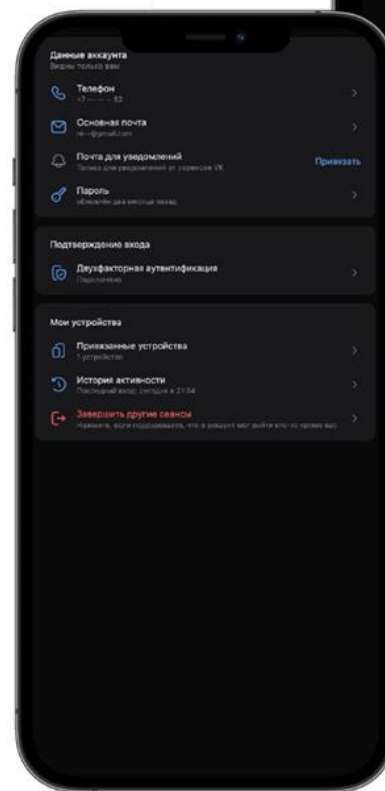
- Важно совершать выход из профиля (в любом приложении или сервисе) на компьютере, телефоне, других устройствах, если планируете оставить без присмотра, или оставлять их запароленными.
- Полностью выключайте компьютер (ноутбук) после завершения работы.
- Не стоит предоставлять доступ другим людям к вашему телефону.
- Проверьте, что у Вас выключен доступ к устройству по Bluetooth.  
*К Вашему устройству может подключиться злоумышленник.*
- Пользуйтесь открытыми сетями Wi-Fi с осторожностью.  
*Лучше не пользоваться ими вовсе: они не всегда безопасны, а злоумышленники с их помощью могут украсть данные или заразить ваши устройства вредоносным программным обеспечением. Если вам всё же приходится работать с общественным Wi-Fi, подключайте надёжные VPN-сервисы. Так ваши данные будут зашифрованы и скрыты от других участников этой сети.*



# Еще о правилах ИБ

Если что-то  
пошло не так

Проверяйте  
историю активности  
и привязанные  
устройства



# Настройки конфиденциальности

---

**Настройки конфиденциальности** – это «часть веб-сайта социальной сети, интернет-браузера, программного обеспечения и т.д., которая позволяет вам контролировать, кто видит информацию о вас». С ростом распространенности социальных сетей и мессенджеров также растет возможность для раскрытия частной жизни. **Настройки конфиденциальности позволяют человеку контролировать, какая информация передается на этих платформах.**

На всех устройствах и во всех приложениях и браузерах есть настройки, которые необходимо настроить таким образом, чтобы информация о Ваших личных данных была скрыта от посторонних людей.

К таким настройкам также относятся разрешения, которые Вы устанавливаете для всех приложений в смартфоне: доступы к контактам, доступы к камере и микрофону, управление звонками и т.д. и т.п.

Вы можете настроить – кто может Вам писать, кто может Вам звонить, какую информацию о себе и кому Вы показываете. Это позволит уменьшить риск общения с мошенниками.





# Что нужно сделать перед тем, как избавиться от старого гаджета или компьютера

---

1. Не забудьте скопировать важную информацию со старого устройства!
2. Убедитесь, что вы вышли из всех учетных записей, которые есть на гаджете.
3. Попробуйте перенести на новое устройство купленное вами программное обеспечение, незачем оставлять его новому владельцу.
4. Проверьте не остались ли в гаджете SIM-карты или карты памяти.
5. После того, как вы скопировали со старого устройства все необходимые данные, удалите всю информацию с него - сотрите и отформатируйте жесткий диск или сделайте т.н. "hard reset" (для мобильных устройств и Интернета вещей), то есть сброс к заводским настройкам.
6. Если информация, хранившаяся на старом жестком диске была чувствительной, то используйте специальное ПО для очистки данных.
7. Но если вам и этого мало - уничтожьте жесткий диск (внутренний или внешний) физически. Лучше всего это сделать с помощью молотка.



# Правила безопасности в Сферуме / VK Мессенджере

---

1. Если используете профиль ВКонтакте, удалите расширения для ВКонтакте: они могут украсть ваши логин и пароль. Например, скачивали для музыки, «Мои гости»
2. В настройках аккаунта VK ID можно посмотреть историю активности:  
<https://id.vk.com/account/#/security> → *История активности*.  
Здесь можно завершить все сеансы, то есть на всех других устройствах нужно будет вновь войти в аккаунт, чтобы просматривать его и пользоваться
3. Ссылки-приглашения в сообщество и чаты отправляйте через закрытые каналы (например СМС)
4. Удаляйте ссылки-приглашения в сообщество после их использования
5. Делайте закрытые настройки чатов
6. При создании звонков, используйте зал ожидания
7. Используйте «Настройки конфиденциальности».



# Правила безопасности в Сферуме / VK Мессенджере

---

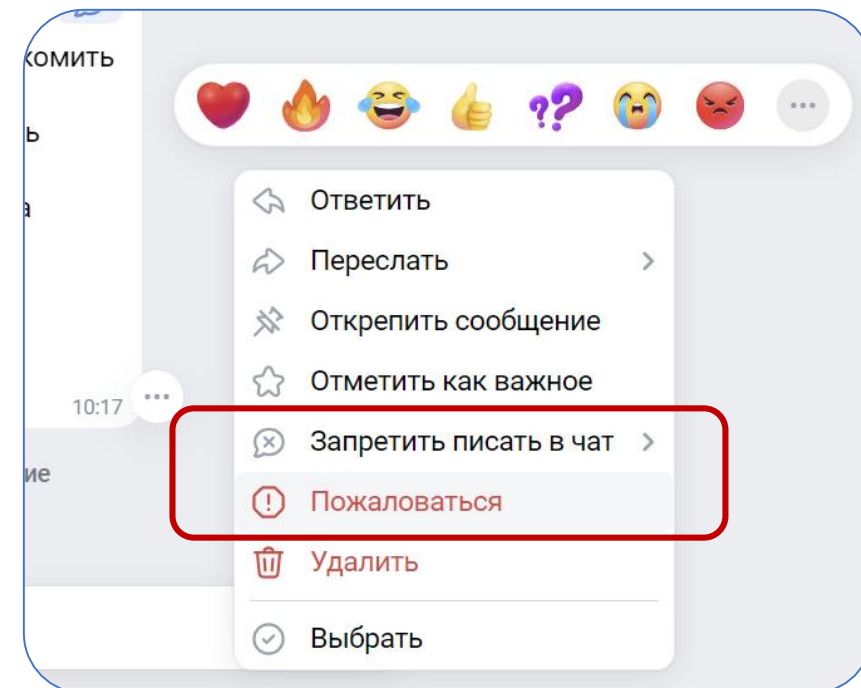
1. Если используете профиль ВКонтакте, удалите расширения для ВКонтакте: они могут украсть ваши логин и пароль. Например, скачивали для музыки, «Мои гости»
2. В настройках аккаунта VK ID можно посмотреть историю активности:  
*<https://id.vk.com/account/#/security> → История активности.*  
Здесь можно завершить все сеансы, то есть на всех других устройствах нужно будет вновь войти в аккаунт, чтобы просматривать его и пользоваться
3. **Ссылки-приглашения** в сообщество, **чаты и звонки** отправляйте через закрытые каналы (например СМС). **Не размещайте их в социальной сети и на других общедоступных ресурсах!**
4. Удаляйте ссылки-приглашения после их использования
5. Делайте закрытые настройки чатов!
6. При создании звонков, используйте зал ожидания и запрещайте анонимный вход
7. Используйте «Настройки конфиденциальности».

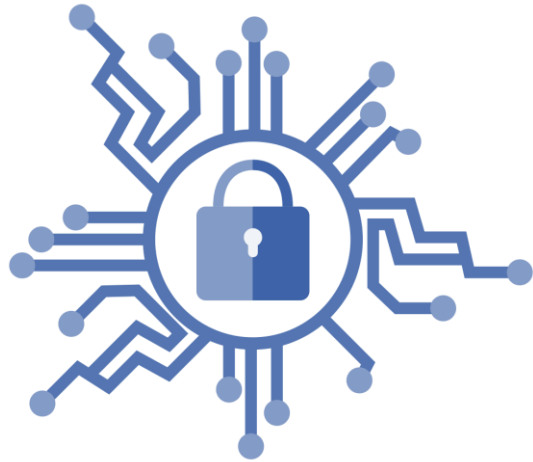


# Правила безопасности в Сферуме / VK Мессенджере

## Если увидели постороннего в чате или звонке

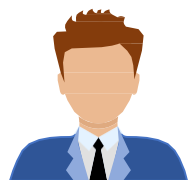
1. Зафиксируйте профиль пользователя с его ID (скриншот экрана с открытой информацией о профиле участника)
2. Используйте функционал «Пожаловаться» (возле его сообщения)
3. Заблокируйте данному пользователю возможность писать сообщения в чате
4. Исключите его из звонка без возможности вернуться в него
5. Обязательно! Отправьте сообщение о нарушителе в техподдержку Сферума через раздел «Помощь»!
6. Аннулируйте все ссылки, измените настройки чата и звонка





# Актуальные способы совершения мошеннических действий

# Захват учетной записи мессенджера






«Злоумышленник с учётной записи друга/знакомого»

Проголосуй за меня пожалуйста, если не сложно конечно)  
<https://goo.su/CTcZ34nN>

ссылка, отправляемая злоумышленниками, сделана при помощи сервиса для сокращения ссылок. Этот инструмент часто применяется, когда отправитель не хочет, чтобы реальный адрес сайта бросался в глаза.

Сайт  
злоумышленников

 <p><b>Выберите Участника</b> Заходите и голосуйте за конкурсантов</p> <p>продолжить</p>	 <p><b>Пройдите аутентификацию</b> Это нужно для подтверждения уникальности голосов</p> <p>РОССИЯ</p> <p>+7 ### ### ##</p> <p>ДАЛЕЕ</p>	 <p><b>Подтвердите код</b> Мы выслали вам сообщение в Telegram с кодом подтверждения</p> <p>Код</p>
---	--	--

Указав номер телефона, вы тут же получите код подтверждения, с помощью которого у вас угонят учётную запись



# Захват учетной записи мессенджера

## Варианты использования захваченной учётной записи мессенджера



«Злоумышленник под видом НО организации»

Добрый день. Это Станислав Викторович начальник вашего отдела. С вами не может связаться наш генеральный директор Андрей Валерьевич и просит ему перезвонить. (сообщает номер)

Злоумышленник используя чужую учетную запись указывает в ней анкетные данные действующего руководителя организации и от его имени связывается с сотрудниками данной организации и злоупотребляя их доверием переводит на диалог с подельниками.



«Злоумышленник под видом ГД организации»

Добрый день! Это Андрей Валерьевич! Наш разговор носит строго конфиденциальный характер, разглашение сведений несет за собой уголовную ответственность и будет расценено как содействие СБУ. В руки СБУ попали личные данные более 2500 сотрудников нашей организации, в том числе доступы к банковским счетам, и ваша кандидатура избрана для оказания содействия в их поиске. В настоящий момент злоумышленники оформляют кредиты на сотрудников нашей организации и все имеющиеся средства выводят предположительно в поддержку ВСУ. Для начала, чтобы пресечь попытку списания ваших денежных средств, вам необходимо исчерпать свой кредитный лимит и все имеющиеся на расчетных счетах денежные средства перевести на резервный счет, который я вам сообщу.

Как только жертва связывается с подставным генеральным директором, злоумышленник всеми возможными способами пытается завладеть денежными средствами жертвы.



# Захват учетной записи мессенджера

---

## Варианты использования фейковой учётной записи Telegram



*«Злоумышленник  
под видом другой  
учётной записи»*

Иван Сергеевич, здравствуйте. Как ваше здоровье? Как работа? Я пишу вам по делу. Хочу вас предупредить, что сегодня Вам будет звонить Нестеров Алексей Александрович, который курирует наше учреждение. У него есть к вам несколько вопросов. Звонок очень важный, обязательно пообщайтесь!

Создание фейковой учётной записи, не имеющей отношение к пользователю. Ведение переписки от имени другого лица.





# Телефонные мошенники: распространенные схемы

---



«Лжесотрудник  
банка»

«С вашей карты пытаются перевести деньги»

«Ваша карта (счет) заблокирована»

«По карте зафиксирована подозрительная операция»



«Друг,  
родственник»

«Ваш сын попал в аварию, ему срочно требуется дорогостоящее лекарство»

«Ваш сын только что в результате ДТП сбил человека. Я готов помочь избежать наказания»



# Социальная инженерия – ЗЛО

---

Телефон — основной инструмент мошенников.

Большая часть хищений происходит с помощью социальной инженерии

- ① Обман или злоупотребление доверием
- ② Психологическое давление
- ③ Манипулирование



Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для кражи средств



# Телефонные мошенники: ФОРМУЛА УСПЕХА



эффект  
неожиданности

+



яркие  
эмоции

+



психологическое  
давление, паника

+



актуальная  
тема

Увы, мы готовы сделать ВСЁ,  
что просят от нас мошенники



# Телефонные мошенники: эмоции, которые вызывает информация

## ПОЛОЖИТЕЛЬНЫЕ

- РАДОСТЬ
- НАДЕЖДА
- ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ



«Вы выиграли крупную сумму денег»  
«Вам положены социальные выплаты»  
«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере...»



## ОТРИЦАТЕЛЬНЫЕ

- СТРАХ
- ПАНИКА
- ЧУВСТВО СТЫДА

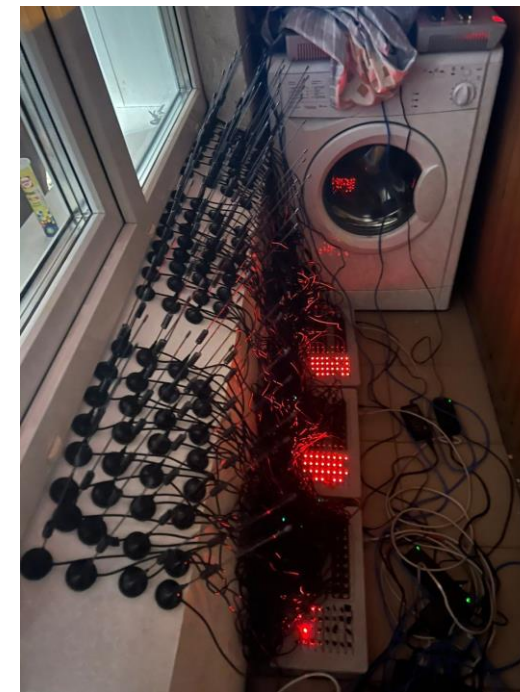


«С вашего счета списали все деньги»  
«Ваш родственник попал в аварию и сбил человека»  
«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела о... коррупции или...»



# Телефонные мошенники: как работают

## SIM-Банки

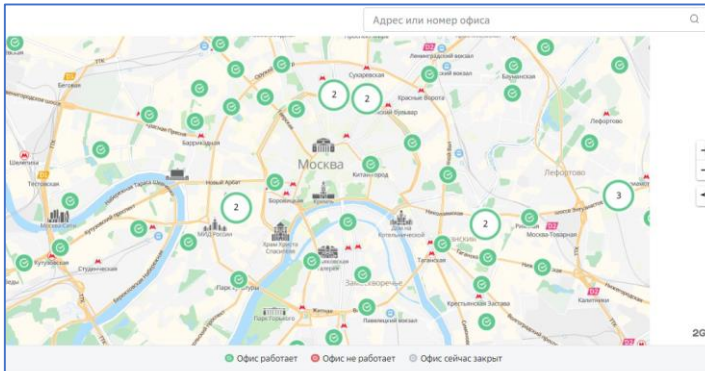


Устройства с функцией передачи сигнала через IP-сеть позволяющие размещать в нем n-ое количество сим-карт и осуществлять с них телефонные звонки

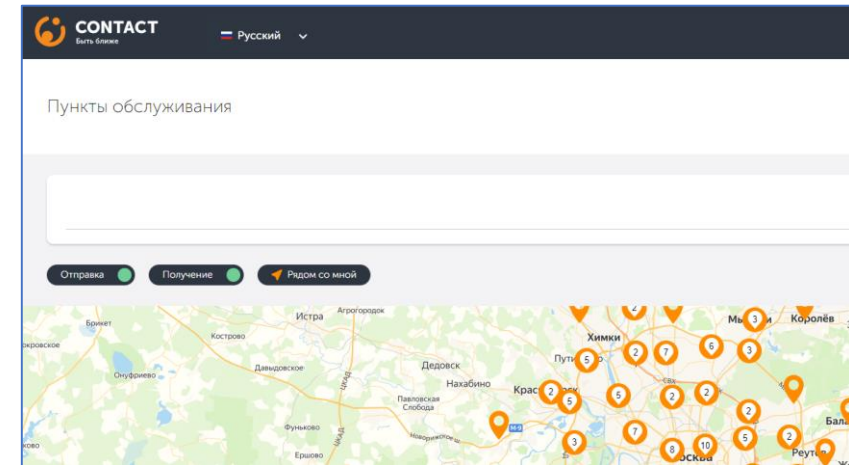
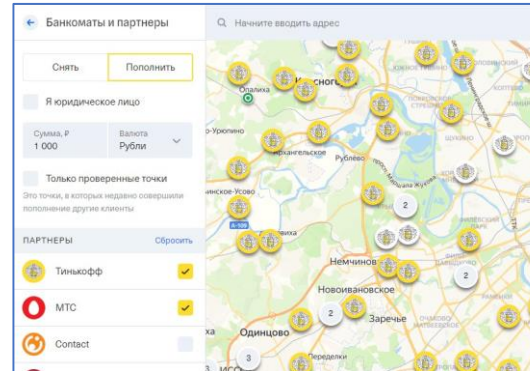


# Телефонные мошенники: как работают

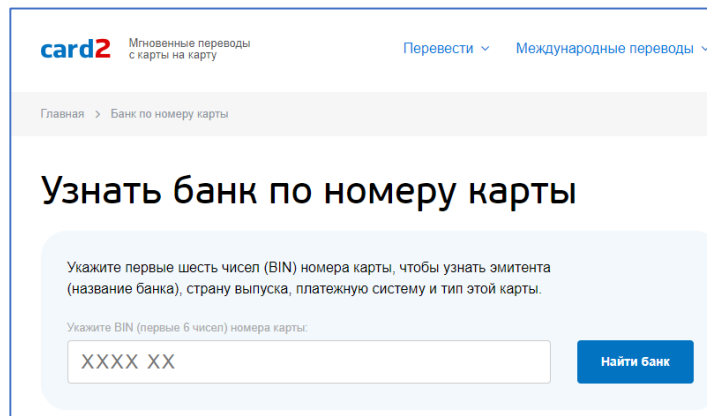
## Общедоступные сервисы в быстром доступе



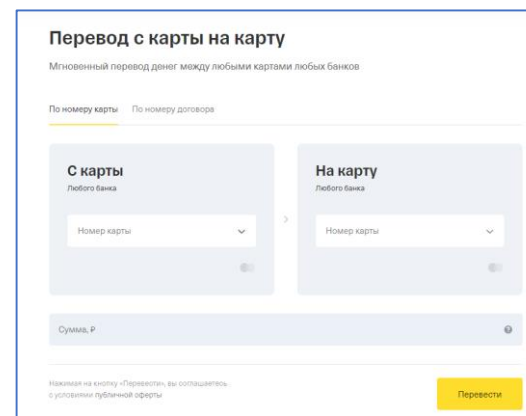
Банкоматы Сбера и Тинькофф с CASH IN



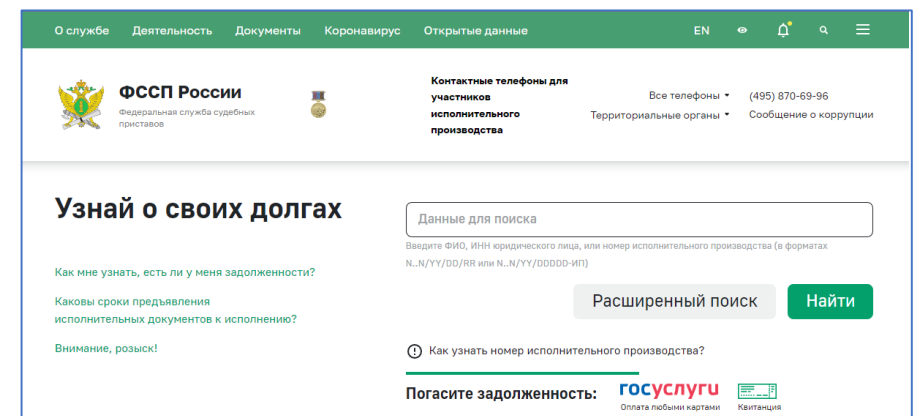
Карта терминалов Contact (денежные переводы)



База BIN банковских карт



C2C от Тинькофф



ФССП проверка долгов

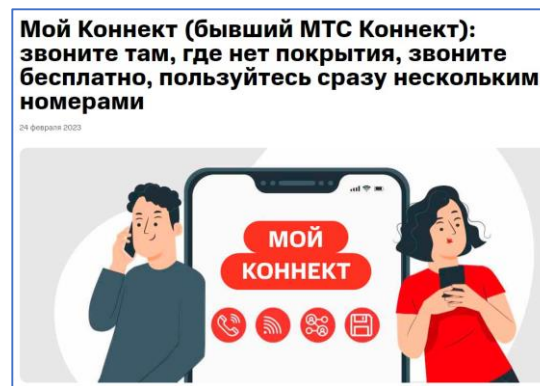


# Телефонные мошенники: как работают

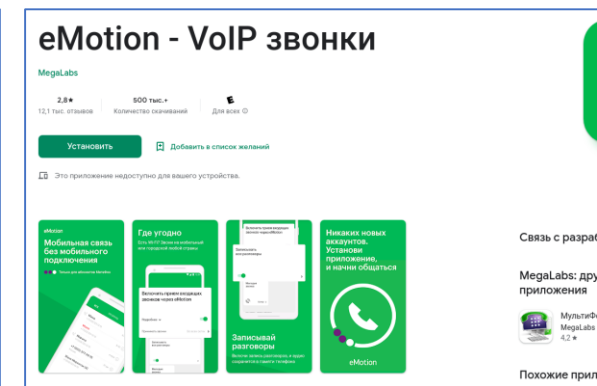
## Инструменты мошеннического колл-центра



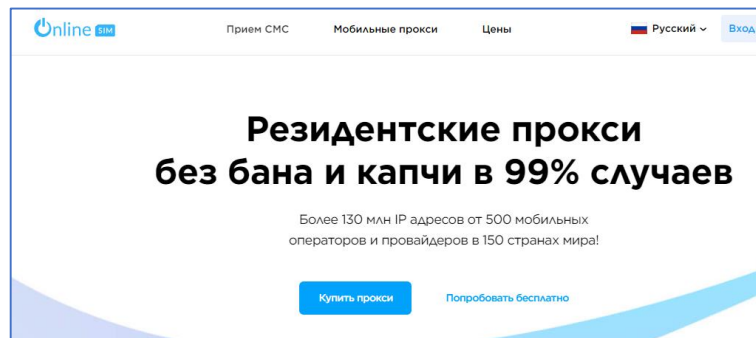
Прокси в РФ, VPN от vip72.com



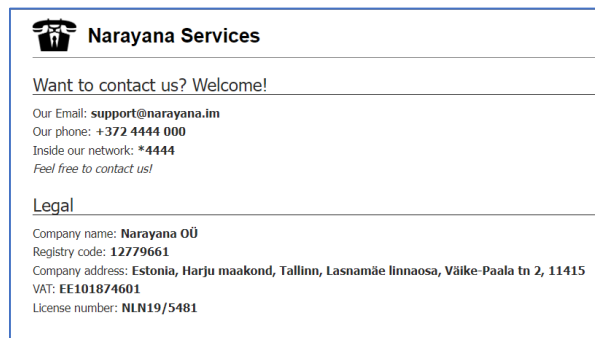
VoIP звонки через МТС Коннект



VoIP звонки eMotion от Мегафона



Прокси в РФ, виртуальные номера телефонов от OnlineSim.io



SIP телефония от Narayana (Эстония)



SIP телефония + подмена номера от Gargona Telecom

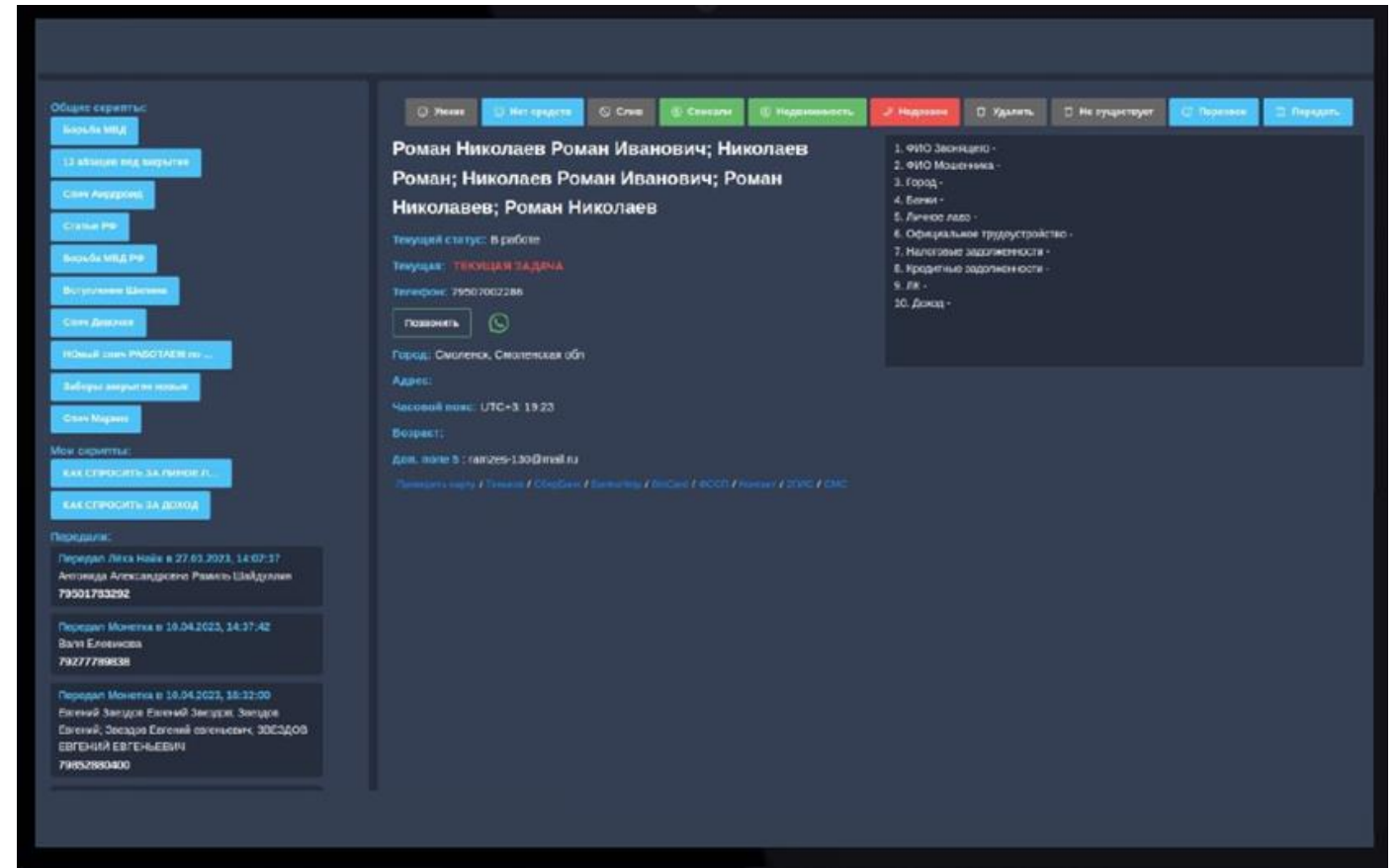


Подписка на ТГ бот «Глаз Бога» («пробив» по номеру телефона)

+ покупка номеров с балансом операторов РФ и номеров для WhatsApp

# Телефонные мошенники: как работают

- ✓ Актуализация информации о клиенте
- ✓ Быстрый доступ к 350+ вариантам скриптов разговора
- ✓ «Тегирование» клиента по результату звонка
- ✓ Онлайн редактор поддельных документов
- ✓ Онлайн тестирование Сотрудника
- ✓ Ссылки на сайты банков и проверки карт



Интерфейс оператора мошеннического КЦ







# Телефонные мошенники: как работают

## Размещение мошеннических колл-центров



### Установлено местоположение:

- ✓ Администратор управляющего CRM – г. Запорожье;
- ✓ 3 CRM – г. Запорожье;
- ✓ 5 CRM – г. Днепр, проспект Дмитрия Яворницкого;
- ✓ 3 CRM – г. Одесса, Люстдорфская дорога;
- ✓ 3 CRM – г. Одесса, Высокий переулок;
- ✓ 2 CRM – г. Киев;
- ✓ 1 CRM – г. Чернигов;
- ✓ 1 CRM – г. Черновцы;
- ✓ 1 CRM – г. Луцк;
- ✓ 1 CRM – г. Львов;



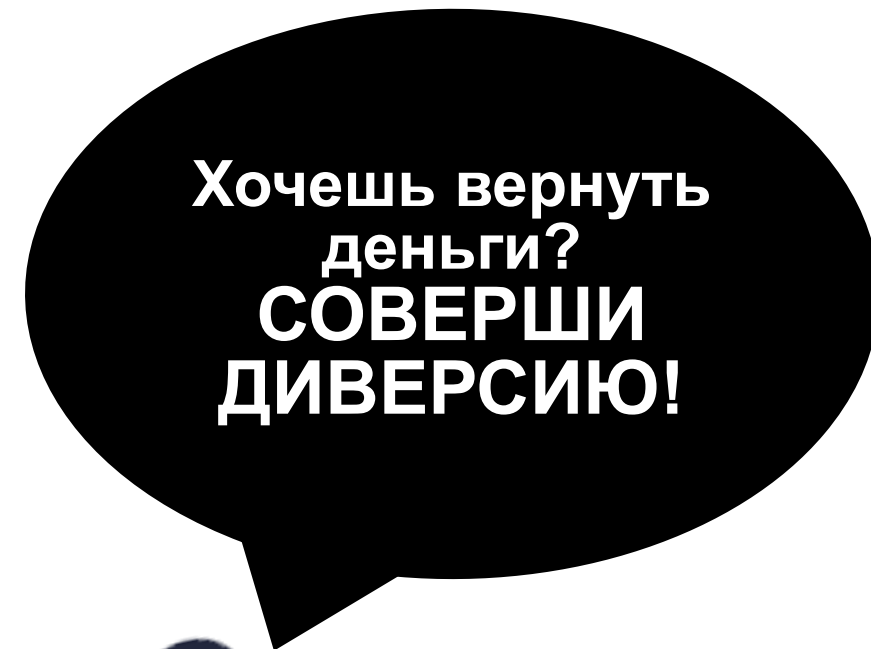
**Геолокация мошеннических КЦ**

*(Данные ПАО Сбербанк)*

# НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

---

- 1 Подтверждение сим-карт
- 2 Компьютерные игры
- 3 Фишинговые сайты
- 4 Сайты знакомств
- 5 Инвестиции
- 6 Госуслуги
- 7 АВИТО



# НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

## Не отвечайте

на звонки с незнакомых номеров

## Прервите разговор

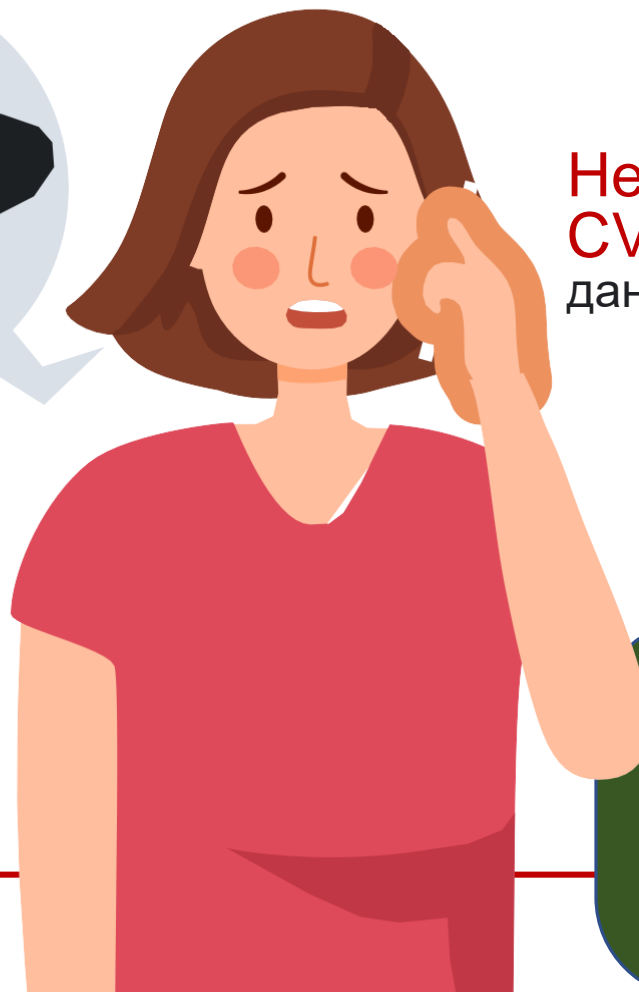
Если он касается финансовых вопросов

## Не торопитесь

принимать решение

## Проверьте информацию в Интернете

или обратитесь за помощью к близким родственникам



Самостоятельно позвоните близкому человеку /в банк / в организацию

Не перезванивайте по незнакомым номерам

Не сообщайте CVV/CVC и иные данные банковских карт

Внимательно проверьте от кого поступают сообщения



Возьмите паузу и спросите совета у родных и друзей!



Спасибо за внимание!