Библиотека Уполномоченного по правам человека в Самарской области

УПОЛНОМОЧЕННЫЙ ПО ПРАВАМ ЧЕЛОВЕКА В САМАРСКОЙ ОБЛАСТИ

ЗАЩИТА ПРАВ ГРАЖДАН ОТ МОШЕННИЧЕСТВА В ЦИФРОВОЙ СФЕРЕ

г. Самара, 2022 г.

ВСТУПЛЕНИЕ

Многие люди думают, что никогда не попадутся на уловки недобросовестных лиц, что они устарели и их легко раскусить. Но это ощущение обманчиво. Обратной стороной развития цифровых технологий, к сожалению, является развитие мошенничества в цифровой сфере. В последнее время эта сфера развивается по многим направлениям.

Недобросовестные лица хорошо организованы, пользуются услугами друг друга, активно обмениваются информацией. Этого не глупые и не безграмотные люди, они накопили много знаний, постоянно совершенствуют свои навыки, создают новые, неочевидные для граждан схемы. Периодически публикуется неутешительная статистика о том, какой ущерб был нанесен в этой сфере.

Стопроцентную гарантию защиты от таких лиц, к сожалению, сегодня не может дать никто. Но можно предпринять меры, чтобы как минимизировать риски, а так и сыграть на опережение и сделать возможные атаки невыгодными и сложными.

Цель настоящего информационного буклета - довести до граждан рекомендации экспертов, занимающихся информационной безопасностью, о том как максимально защитить данные о себе и активы в цифровой среде, а их хищение сделать сложным и бессмысленным.

Естественно, выполнение всех приведенных ниже рекомендаций является не всегда простым для каждого человека, может быть сопряжено с некоторыми неудобствами при использовании электронных устройств. Тем не менее, изучение этих рекомендаций – повод задуматься и выбрать наиболее необходимые и приемлемые для себя.

НАИБОЛЕЕ НЕОБХОДИМЫЕ ДЕЙСТВИЯ

Действие	Пояснение
Установить pin-код на sim-карту телефона	В случае утери/кражи телефона недобросовестные лица не смогут быстро воспользоваться вашим номером, вы выиграете время для его блокировки
Оформить запрет на регистрацию сделок с недвижимым имуществом без личного присутствия	Чтобы исключить отчуждение недвижимого имущества по поддельным доверенностям или электронным цифровым подписям (ЭЦП)
Оформить в офисе мобильного оператора запрет на совершения действий от вашего имени по доверенностью	Для того, чтобы недобросовестные лица не смогли сделать дубликат sim-карты либо вывести денежные средства по поддельной доверенности
Оформить запрет услуги «Мобильный перевод» в офисе мобильного оператора	В случае компрометации sim-карты, с нее не выведут деньги
Установить кодовое слово в офисе вашего мобильного оператора	Для быстрой блокировки sim-карты в экстренных ситуациях
Настроить оповещение о выпуске ЭЦП в личном кабинете Госуслуг	Если недобросовестные лица выпустят от вашего имени ЭЦП, вы об этом узнаете сразу
Настроить двухфакторную аутентификацию на портале Госуслуг, официальных интернет-сайтах Федеральной налоговой службы, Росреестра	Недобросовестные лица не смогут войти в ваши личные кабинеты, даже если узнают пароль

Установить определитель номера на смартфон	В большинстве случаев недобросовестные лица звонят с номеров, которые помечаются определителями номеров как мошеннические
Установить антивирусное программное обеспечение на смартфон	Защита вредоносного программного обеспечение, в т.ч. нацеленного на хищение ваших данных
Регулярно обновляйте программное обеспечение на вашем смартфоне, включая обновления безопасности	Защита от актуальных способов атак на ваши данные
На разные сайты и приложения установить разные пароли или пользоваться менеджером паролей	Если пароль от портала Госуслуг совпадает, например, с паролем на простой форум, то взломав этот форум недобросовестные лица получат пароль к важным сервисам и данным
Настроить оповещение о каждом входе на портал Госуслуг	Если недобросовестные лица получат доступ к вашему личному кабинету, вы об этом сразу узнаете
Установить суточные лимиты трат и переводов по банковской карте	Недобросовестные лица не смогут вывести больше установленной суммы. Изменить установленные лимиты иным лицам сложно.
Настроить получение подтверждений банковских операций через push-уведомления, а не через sms-сообщения	Sms – менее надежный протокол, чем push, он подвержен атакам. Однако если вы уезжаете в местность без интернета или в роуминг - временно верните оповещение по sms-сообщениям
Настройте смартфон скрывать тексты уведомлений на заблокированном экране	В случае кражи телефона недобросовестные лица не смогут прочитать банковские коды на заблокированном экране

ВАЖНЫЕ ДЕЙСТВИЯ

Действие	Пояснение
В аккаунте Google (Apple) указать номер запасного телефона и запасной адрес электронной почты	В случае компрометации аккаунта это понадобится для восстановления доступа
Установите автоблокировку экрана смартфона не более чем 30 секунд	Если телефон украдут, он успеет заблокироваться
Запомните кодовые слова и контрольные вопросы для всех банков, в которых обслуживаетесь	Чтобы в экстренных ситуациях, не теряя времени, подтвердить вашу личность в call-центре
Не выбирайте контрольные вопросы, на которые легко найти ответ, например девичью фамилию матери	Данная информация зачастую находится в общем доступе или в базах данных, которые недобросовестные лица могут относительно легко приобрести

Выучите наизусть номера близких	Чтобы в экстренных ситуациях позвонить близким не со своего телефона
Подключите оповещения о запросах вашей кредитной истории	Вы будете сразу уведомлены о любых намерениях оформить на вас кредит
Подключите оповещения об операциях по банковской карте	Это позволит быстро определить списания, инициированные не вами, и не теряя времени позвонить в банк
Привязанный к банковскому аккаунту телефон держите всегда при себе	В случае выпуска недобросовестными лицами дубликата sim-карты, вы об этом сразу узнаете
Для основной карты, которой расплачиваетесь в магазинах и интернете, запретите снятие наличных и покупки не в вашей стране	Зачастую украденные банковские карты используют в других странах. Если вам нужно оплачивать зарубежные товары/услуги, заведите для этого отдельную виртуальную карту. Если же вы отправились в путешествие, временно снимите данный запрет
При оплате в интернете не вводите данные банковской карты во всплывающем окне, в котором не видно адрес сайта платежной системы	Недобросовестные лица могут создать полную копию страницы оплаты, которая будет вести на иной сервер и денежные средства будут переведены вразрез с вашими намерениями
Отключите автосохранение паролей на смартфоне и компьютере	В случае кражи телефона недобросовестные лица смогут увидеть все сохраненные пароли, в т.ч. те, которые вы сохранили с компьютера
Установите лимиты на автопополнение баланса sim-карты	В случае компрометации sim-карты недобросовестные лица не выведут все деньги с банковской карты
Запишите номера горячих линий банков и мобильного оператора на основной и запасной телефоны	Чтобы в экстренных ситуациях вы могли быстро позвонить на горячую линию
Отключите автополучение MMS на вашем устройстве	Существует уязвимость, позволяющая загружать вирусы на устройство через MMS
Лишите прав на просмотр sms-сообщений и звонков те приложения, которым это не нужно	Вредоносное программное обеспечение может быть встроено во внешне безобидное приложение, у которого есть права к sms
Проведите ревизию расширений в вашем браузере, неиспользуемые расширения удалите	Недобросовестные лица выкупают старые расширения и заливают вредоносный код в качестве обновлений
Проведите ревизию приложений на смартфоне, неиспользуемое и старое удалите	Недобросовестные лица выкупают старые приложения и заливают вредоносный код в качестве обновлений

Настройте push-уведомления о письмах с электронной почты	Чтобы не пропустить важное уведомление с государственного или банковского сервиса
Пометьте как «не спам» номера телефонов мобильного оператора и банков, которыми вы пользуетесь	Чтобы не пропускать sms-сообщение касательно безопасности
Установите антивирус на домашний компьютер	Защита от вредоносного программного обеспечения
Устанавливайте на домашнем компьютере самые последние обновления операционной системы и приложений, включая обновления безопасности	Это позволит закрыть обнаруженные уязвимости, защититься от атак и последних версий вирусов
Отключите возможность удаленного соединения с вашим компьютером: запретить удаленный рабочий стол, закрыть внешние порты	Один из распространенных методов взлома заключается в переборе открытых портов у потенциальных жертв и простые пароли для доступа на удаленный рабочий стол
Обслуживайтесь в банке, через call-центр которого нельзя изменить номер привязанного телефона	Недобросовестные лица могут разными способами получить персональные данные и «привязывать» свой телефон к аккаунту жертвы
Установите отпечаток или пароль при бесконтактной оплате смартфоном (либо отключите ее)	Если мобильный телефон украдут, недобросовестные лица не смогут с его помощью совершать платежи
На wi-fi роутере установите сложный пароль администратора и смените IP-адрес устройства	Чтобы недобросовестные лица не смогли получить доступ к wi-fi роутеру как администратор
Установите сложный пароль для подключения к wi-fi роутеру	Чтобы недобросовестные лица не смогли подобрать пароль простым перебором

ЖЕЛАТЕЛЬНЫЕ ДЕЙСТВИЯ

Действие	Пояснение
Носите с собой запасной телефон с рабочей sim-картой	Чтобы быстро заблокировать основной телефон в случае его утери или кражи
Установите на смартфоне pin-код на просмотр файлов, фотографий и открытие мессенджеров	В случае кражи телефона ваши файлы, контакты и переписка не попадут недобросовестным лицам
Если это возможно, запретите удаленное восстановление доступа по дистанционным каналам	Если забыли пароль - заводите новый аккаунт

Оформите в Федеральной налоговой службе запрет на регистрацию юридического лица с использованием ЭЦП	Чтобы исключить регистрацию юридического лица на ваше имя по поддельной ЭЦП
Не используйте разблокировку смартфона по лицу	В случае кражи телефона недобросовестные лица могут разблокировать смартфон по фотографии. Вероятность этого невелика, но это случается, поэтому лучше защититься

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

Действие	Пояснение
При подозрительном или тревожном звонке от кого угодно сразу же положите трубку. Не берите трубку, пока сами не разберетесь в ситуации. Перезванивайте только на официальные номера	Защита от телефонных мошенников
Не платите вперед, откажитесь от предоплат в любых сделках и ситуациях, если организация или человек для вас малоизвестны	Защита от онлайн и офлайн мошенников
При важной и крупной покупке внимательно проверяйте документы продавца. Проявляйте должную осмотрительность.	Недобросовестные лица используют поддельные документы (паспорта, доверенности и т.д.), продают не принадлежащее им движимое и недвижимое имущество. В таких случаях покупатель может потерять и приобретенное имущество, и затраченные денежные средства
Не давайте копировать, сканировать и фотографировать свой паспорт нигде, кроме как в отделениях банков и государственных структур. Не направляйте электронные образы документов по электронной почте	Это уменьшит вероятность утечки персональных данных
Не оставляйте в залог заграничный паспорт с биометрическим чипом	Тот, у кого в руках есть биометрический заграничный паспорт, может зарегистрировать ИП. Такая услуга есть у ряда банков.
Перед оплатой в интернете внимательно проверяйте домен	Чтобы не попасться на интернет-мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей (фишинг)
Проверяйте реквизиты перевода непосредственно перед платежом	Существует вредоносное программное обеспечение, которое подменяет реквизиты в последний момент
Не держите большие суммы на банковской карте, которой расплачиваетесь в магазинах и интернете	В худшем случае недобросовестные лица смогут украсть лишь небольшую сумму

Прикрывайте ладонью терминал, когда вводите pin-код	Защита от кражи данных банковской карты
Не показывайте никому код CVV2 (не переворачивайте лишний раз карту обратной стороной)	Защита от кражи данных банковской карты
Внимательно давайте разрешения приложениям на отправку sms-сообщений и совершение звонков	Защита от вредоносного программного обеспечения, направленного на хищение данных
Не давайте доступ к записной книжке мессенджерам и банковским приложениям	Таким образом вы сообщите внешнему миру меньше информации о себе
Проверьте администраторов устройства в настройках смартфона	Там должны быть только проверенные приложения, которым эти права действительно необходимы
Установите пароль на загрузку устройства, если такой имеется в модели вашего смартфона	Дополнительный фактор защиты
Оформите eSim, если модель смартфона и оператор связи это позволяют	eSim удобнее и надежнее обычной sim-карты
Не торопитесь переходить по ссылкам, где требуется ввод личных данных. Если перешли – проверьте, что сайт настоящий	Одна из основных угроз, которые продолжают работать по сей день – это фишинговые ресурсы. Недобросовестные лица могут украсть персональные данные, узнать ответы на контрольные вопросы, подкинуть вам вредоносное программное обеспечение
Не вводите данные своей банковской карты в неизвестных онлайн-магазинах или приложениях	Их могут взломать и украсть данные всех банковских карт. Также недобросовестные лица создают легальные онлайн-магазины. При покупке в таком магазине данные вашей карты попадают в руки недобросовестных лиц
Будьте внимательны на сайтах с «пиратским» контентом	Можно наткнуться на вредоносное программное обеспечение, например – на шпионские программы, которые получают сведения о паролях
Не запускайте на своем компьютере взломанные программы и генераторы ключей	В «пиратские» программы и генераторы ключей может быть встроено вредоносное программное обеспечение
Не устанавливайте потенциально опасные приложения: неофициальное программное обеспечение для скачивания музыки, «пиратский» контент и пр.	Они могут содержать вредоносное программное обеспечение
При открытии любого файла, который вам прислали даже знакомые люди, будьте внимательны. Один из самых распространенных способов заражения компьютера - жертва сама запустила вредоносный файл	Вредоносное программное обеспечение может содержаться в файле любого формата, может быть зашифровано для обхода антивирусного программного обеспечения. Ваши знакомые могут не знать, что отправляемый ими файл содержит эту опасность

Файлы, которые вы получили по электронной почте, через мессенджеры или скачали сами из интернета, проверяйте на специальных бесплатных сервисах, например virustotal.com	Фишинговое письмо ничем не отличается от обычного, это одна из основных схем попадания вредоносного программного обеспечения. Лучше перестрахуйтесь
Не давать никому в руки банковскую карту. Все операции должны проходить в вашем присутствии	Защита от кражи данных банковской карты
Не входите в свои аккаунты с чужих устройств	На этих устройствах может быть вредоносное программное обеспечение
Не храните на компьютере очень важные файлы	Если придется форматировать жесткий диск компьютера из-за вируса-шифровальщика, данные будет невозможно вернуть. Лучше хранить на их на съемных носителях
Не храните на смартфоне важные или секретные файлы и переписку. Будьте морально готовы, что телефон может попасть в чужие руки	Чтобы исключить утечку персональных данных и личной переписки сделайте так, чтобы ваш телефон можно было дать любому человеку без каких-либо рисков
Не подключаться к бесплатным wi-fi сетям	Исключить атаки на вас через незащищенные сети
Устанавливайте приложения только из Google Play/App Store и с хорошим рейтингом	Защита от вредоносного программного обеспечения
По возможности не пользуйтесь одиноко стоящими банкоматами в местах, где мало людей	Защита от кражи данных карты при помощи специальных считывающих устройств (скимминг). Лучше всего использовать банкоматы в отделениях банков или крупных зданиях. Там недобросовестным лицам намного сложнее произвести махинации с банкоматом
Крупные суммы держите в банке, к которому не подключено дистанционное управление	Исключить вероятность дистанционной кражи
Не храните электронных образов документов в облачных сервисах	Уменьшить вероятность их утечки, например при краже телефона
Не устанавливайте root-права на смартфон	В случае попадания вредоносного программного обеспечения, оно сможет делать все что угодно на вашем устройстве
Потренируйтесь в блокировке вашего устройства с телефона близкого человека	Тренировка в случае кражи вашего устройства
Не давайте в руки телефон малознакомым людям	Защита от кражи данных и от установки вредоносных программ

Пользуйтесь проверенными крупными операторами связи	В некоторых виртуальных операторах связи социальной инженерией можно получить персональные данные
Сделать аккаунты ВКонтакте и Facebook невидимым никому, кроме друзей	Общедоступные фото получаются из аккаунтов в социальных сетях и хранятся на серверах, которыми пользуются недобросовестные лица. Удалить свои фото с таких серверов невозможно
В профилях в социальных сетях сообщайте минимум информации о себе, фотографию на аватаре сделайте в полный рост, на удалении (или удалите вовсе), замените фамилию на никнейм	Недобросовестные лица пользуются поиском по фотографии, номеру телефона, фамилии и имен, таким образом они собирают информацию и продумывают варианты атак
Имейте дома наличные деньги	На случай, если придется заблокировать банковские карты и счета, защищая их от недобросовестных лиц
Периодически меняйте кодовые слова, ответы на контрольные вопросы, пароли от личных кабинетов	Персональные данные могут утекать даже из банков, недобросовестные лица могут устраиваться в call-центры банков, поэтому хорошей практикой будет периодическая смена такой информации
Периодически проверяйте информацию на порталах Госуслуг, Федеральной налоговой службы, Росреестра, Федеральной службы судебных приставов и т.п: выданные вам ЭЦП, участие в организациях, сведения о вашем имуществе, исполнительные производства. В настройках электронной почты проверяйте, что отсутствует переадресация на неизвестные вам почтовые ящики, а также подозрительные сессии и привязанные устройства	В случае уведомлений о действиях, которые вы не совершали, надо быстро предпринимать действия

ЧТО ДЕЛАТЬ В ЭКСТРЕННОЙ СИТУАЦИИ

Если украли телефон

- С запасного телефона войдите в свой google/apple аккаунт и пометьте телефон как украденный. Или сделайте erase device. Если запасного телефона нет, то проделайте это с телефона близкого/друга который находится рядом. Если вы один, переходите сразу к следующему пункту
- Заблокируйте sim-карту по горячей линии мобильного оператора. Попросите прохожего, таксиста, охранника, полицейского дать вам телефон. Если людей поблизости нет, доберитесь до ближайшего салона связи
- Звоните на горячие линии банков, в которых обслуживаетесь, блокируйте все банковские карты и счета. Действуйте быстро
- Заблокируйте все важные аккаунты (электронная почта, Порталы Госуслуг, Федеральной налоговой службы, Росреестра, онлайн-банкинг, социальные сети, электронный документооборот)
- Сообщите близким и друзьям что ваш телефон украли, а также сделайте посты в социальных сетях, чтобы недобросовестные лица не звонили от вашего имени друзьям и не занимались шантажом. В этом случае пригодятся номера близких, которые вы помните
- Напишите заявление в полицию. Возможно с украденного номера будут совершать противоправные действия, у вас будет доказательство, что вы к ним не имеете отношения
- Выйдите из всех мессенджеров на украденном устройстве. Это необходимо чтобы похитившему не досталась переписка
- Отвяжите украденное устройство из аккаунта google, мессенджеров, государственных сервисов, финансовых приложений, социальных сетей
- Поменяйте пароли от всех важных аккаунтов: (электронная почта, Порталы Госуслуг, Федеральной налоговой службы, Росреестра, онлайн-банкинг, социальные сети, электронный документооборот). Проделайте это, когда уже будет выпущен дубликат sim-карты

Если пришло sms-сообщение о списаниях, которые вы не совершали

- Убедитесь, что sms-сообщеение пришло с настоящего номера банка или платежной системы. Проверьте, что баланс банковской карты действительно уменьшился. Если это произошло, значит вашей картой пользуется злоумышленник. Действуйте быстро
- Заблокируйте все банковские карты. Это нужно сделать максимально быстро, чтобы не были выведены все денежные средства
- Позвоните в банк, сообщите о списаниях, которые вы не совершали. Действуйте быстро, делайте скриншоты чата с банком, записывайте на диктофон разговоры с банком
- Не торопитесь писать заявление в полицию под диктовку банка. Если денежные средства украли без вашего ведома - их украли у банка. Не обращайтесь в полицию как пострадавший. Направьте в банк претензию, в которой указано, что потерпевшей стороной является именно банк.

Если на вас незаконно оформили микрозайм

- Напишите заявление о мошеннических действиях в организацию, выдавшую микрозайм
- Напишите жалобу в интернет-приемную Банка России. В качестве пострадавшей стороной укажите финансовую организацию, которая выдала микрозайм
- Напишите претензию кредитору. Потребуйте аннулировать долг

- Получите от кредитора копии поддельного договора о кредите и копию паспорта, на который он был выдан
- Напишите заявление в полицию, приложите копии документов о поддельном кредите. Формулируйте заявление так, что пострадавшей стороной являетесь не вы, а финансовая организация, которая не проявила должную осмотрительность

Если на вас оформили поддельную электронную цифровую подпись (ЭЦП)
- Обратитесь в удостоверяющий центр за аннулированием сертификата
- Заблокируйте ЭЦП на портал Госуслуг. Блокировка ЭЦП в личном кабинете госуслуг не аннулирует сертификат
- Напишите заявление в полицию

Если на вас незаконно зарегистрировали юридическое лицо
- Напишите заявление в полицию
- Напишите возражение в ФНС о незаконной регистрации

Если вы потеряли паспорт
- Напишите заявление в полицию, получите талон-уведомление
- Проверьте что по утерянному паспорту не успели зарегистрировать юридическое лица
- Проверьте что на вас не оформили кредит
- Обратитесь в Росреестр с заявлением о непроведении государственной регистрации в связи с кражей паспорта
- После получения нового паспорта обратитесь с заявлениями в Росреестр о непроведении государственной регистрации без вашего личного участия и внесении изменений в сведения о вас как о правообладателе в отношении каждого принадлежащего вам объекта недвижимого имущества

Если sim-карта внезапно отключилась
- Позвоните мобильному оператору и выясните причины отключения
- Если карту отключило третье лицо, то заблокируйте банковские карты и счета до разрешения ситуации

Если был несанкционированный вход в почтовый аккаунт
- Восстановите доступ к аккаунту и поменяйте пароль
- Поменяйте пароли на всех важных аккаунтах
- Удалить подозрительную сессию, отвяжите подозрительные устройства
- Откройте настройки аккаунта, и убедитесь, что не настроена переадресация писем на неизвестные вам адреса электронной почты
- Проверьте все важные аккаунты на предмет действий, которые вы не совершали

Если взломали ваш аккаунт на портале Госуслуг
- Заблокируйте все важные аккаунты
- Позвоните по телефону горячей линии портала Госуслуг и сообщите о взломе аккаунта. Следуйте инструкциям