468576 265305

ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОКУРАТУРА
ВОРОНЕЖСКОЙ ОБЛАСТИ

ПРОКУРАТУРА
ОЛЬХОВАТСКОГО РАЙОНА

ул. Жуковского, д. 7, р.п. Ольховатка, 396670
Тел./факс (47395) 4-07-45

Главе администрации Ольховатского муниципального района

Берченко Г.Н.

Главам всех сельских, Ольховатского городского поселений

16.04.2025 № Исорг-20200030-340-25/-20200030

На № _____

ИНФОРМАЦИЯ
для размещения на сайте

Направляется информация для размещения на сайте администрации района, на страницах администрации района в социальных сетях, на сайтах поселений.

О результатах данной информации сообщите в прокуратуру района не позднее 30.04.2025 (на бумажном носителе) с приложением скриншота экрана с размещенной информацией.

Информация: Способы защиты цифрового профиля гражданина на портале государственных услуг Российской Федерации, защита мобильного устройства.

Защита цифрового профиля гражданина на портале государственных услуг Российской Федерации начинается с двух важнейших шагов: создания надежного пароля и активации двухфакторной аутентификации.

Надежный пароль — это первый рубеж обороны вашей учетной записи, который характеризуется следующими признаками:

- Длинный и его трудно угадать.

Надёжный пароль содержит 12 символов, включает буквы в разном регистре, цифры и специальные символы (~!@#$%^&*+-/.,\{}[]();:|?<>=).

- В нём нет последовательных комбинаций клавиш.

Не используйте последовательный набор клавиш, например «qwerty», — его легко взломать. Для надёжного пароля применяйте случайную комбинацию букв, цифр и других символов.

- Нет личных данных.

Не используйте для паролей личные данные, например фамилию, дату рождения или кличку питомца. Такую информацию легко узнать, просмотрев ваши социальные сети.

- Содержит фразу.

Выбирайте за основу не слова, а фразы — они длиннее, их сложнее угадать или перебрать. Используйте для пароля смешное событие, забавную привычку, тайную мечту — такой пароль легко запомнить и трудно подобрать: «ГотовлюБорЩ_на5+баллов!@», «Прохождение$Цивилизации-1час», «_Поеду1_вРио-де-Жанейро-вБелыхШт@н@х».

- Уникальный.

Придумайте пароль для каждого критичного сервиса — Госуслуг, интернет-банка, соцсетей. Если один и тот же пароль используется везде,

взломав один, злоумышленники получат доступ ко всем вашим учётным записям.

Как сохранить пароли в безопасности.

Не сохраняйте пароли на смартфоне, планшете или компьютере.

Если злоумышленники получат доступ к вашему устройству, они легко доберутся до паролей. Также небезопасно хранить пароли в браузерах — в них периодически находят уязвимости, которыми могут воспользоваться хакеры, чтобы добраться до ваших паролей.

Вторым шагом по защите вашего цифрового профиля на портале государственных услуг должно быть включение двухфакторной аутентификации.

Двухфакторная аутентификация (2FA) — это дополнительный уровень защиты, который значительно усложняет жизнь злоумышленникам. Принцип работы прост: после ввода пароля (первый фактор) система запрашивает дополнительное подтверждение входа (второй фактор) — обычно это одноразовый код, который приходит в SMS или генерируется специальным приложением, например, «Яндекс.Ключ».

Важно понимать, что даже если злоумышленник узнает ваш пароль, без доступа к вашему личному устройству он не сможет проникнуть в учетную запись. Именно поэтому двухфакторная аутентификация считается одним из самых эффективных способов защиты от взлома.

На Госуслугах пользователи могут настроить подтверждение входа. При каждом входе на Госуслуги будет приходить смс с одноразовым кодом (либо вы будете получать код из специального приложения, например, «Яндекс.Ключ»). Код нужно указывать после ввода пароля. Помните, что его тоже никому нельзя сообщать!

Как подключить подтверждение входа на портале Госуслуг.

Перейдите в раздел «Безопасность» личного кабинета Госуслуг. На вкладке «Вход в систему» выберите «Вход с подтверждением». Справа переведите выключатель в активное положение — он станет синего цвета. Выберите подходящий вариант: дополнительное подтверждение может приходить в виде смс либо в виде одноразового кода (TOTP). Проверьте номер телефона. Если он указан неверно, исправьте ошибку. В зависимости от выбранного способа введите пароль от Госуслуг, чтобы подтвердить действие. Теперь при каждом входе в личный кабинет вам будет приходить дополнительный код-пароль. Никогда и никому не сообщайте его.

Как узнать, что личный кабинет взломали.

Если у вас подключено подтверждение входа, то при попытке взлома вам придёт смс-код для подтверждения входа. Это означает, что кто-то пытается войти в личный кабинет, используя ваши логин и пароль. В такой ситуации следует немедленно сменить пароль. Если подтверждение входа не настроено, о взломе личного кабинета вы узнаете, когда попробуете самостоятельно зайти на портал и не сможете этого сделать, — злоумышленники наверняка сменят пароль.

Защита мобильного устройства.

Защита мобильного устройства — это не менее важный аспект безопасности, чем защита самих учетных записей от профиля на портале Госуслуг.

Современные смартфоны хранят огромное количество конфиденциальной информации, злоумышленники прекрасно понимают её ценность, поэтому активно ищут способы получить доступ к вашим устройствам. Взломав телефон, они могут получить доступ к SMS с одноразовыми кодами для двухфакторной

аутентификации на портале. Именно поэтому критически важно защищать мобильное устройство надежным паролем или биометрией, регулярно обновлять операционную систему и использовать только проверенные приложения из официальных магазинов.

Случайный доступ. При использовании одного устройства несколькими членами семьи следует контролировать доступ к конфиденциальной информации. Не разрешайте ребёнку использовать устройство, на котором хранится важная информация, а также установлены приложения мобильного банка, почты и другие.

Кража. Если у вас украли смартфон, потери могут не ограничиться самим телефоном. Вор может получить доступ к вашим учётным записям, которые привязаны к устройству. Воспользоваться мобильным банком и вывести с ваших счетов все доступные деньги. Использовать для шантажа и вымогательства вашу личную информацию — рабочие документы, фото, переписки в мессенджерах и соцсетях

Действия хакеров. Киберпреступники атакуют смартфоны с помощью вредоносных программ или файлов с вирусами, получают удалённый доступ к гаджетам и крадут с них секретные данные. Такая ситуация опаснее реальной кражи устройства — человек может не подозревать, что его информацию похитили.

Как защитить устройство на случай кражи.

Настройте блокировку экрана. Для защиты устройства включите автоматическую блокировку экрана. Для разблокировки используйте длинные пароли и сканер отпечатка пальца. Графический ключ легко подглядеть из-за плеча и несложно подобрать — люди рисуют слишком очевидные траектории.

Защитите паролем или отпечатком пальца важные приложения и файлы. Это станет дополнительным фактором защиты и не позволит вору быстро попасть в банковские приложения, диспетчер файлов, галерею, почту, ваши социальные сети

Настройте отслеживание. Установите программу, которая удалённо блокирует телефон. Такие приложения определяют местоположение устройства, включают сирену, фотографируют злоумышленника, а также стирают все личные данные.

Скачивайте только проверенные приложения. Злоумышленники распространяют вредоносные программы под видом игр и полезных приложений. Загружайте приложения только из официальных магазинов: здесь строгая модерация, рейтинг, статистика по количеству скачиваний и отзывы пользователей.

Если необходимо установить приложения банков, попавших под санкции, скачайте их с официальных сайтов организаций.

Не переходите по подозрительным ссылкам. Чтобы заразить телефон вирусом, злоумышленники часто рассылают письма и сообщения с информацией о выигрыше, выгодной акции. При переходе по ссылке из такого сообщения на смартфон может загрузиться вредоносная программа. Если случайно перешли и файл загрузился, ни в коем случае не открывайте его и удалите

Установите антивирус на смартфон. Антивирусы смогут обнаружить вредоносную программу, если она уже оказалась на устройстве. Защитные системы блокируют переходы на заражённые сайты, проверяют ссылки, которые приходят в смс и мессенджерах, выявляют небезопасные настройки на смартфоне. Не забывайте периодически обновлять антивирус.

Не давайте приложениям лишних разрешений. Не разрешайте приложениям, например планировщику дел или фонарику, получать доступ к

камере, файлам на устройстве, совершению звонков, отправке смс. Если приложение получает подобные разрешения, оно сможет пользоваться этими функциями без вашего ведома — отправлять ваши фотографии на сервер злоумышленников или подписывать на платные рассылки. Разрешения приложений можно проверить в общих настройках телефона

Постоянно обновляйте систему. Киберпреступники ищут уязвимости в программном обеспечении и приложениях, поэтому разработчики программ регулярно выпускают обновления, исправляют ошибки и уязвимости. Включите автоматические обновления операционной системы в установленных приложениях. Если обновления не устанавливать, устройство будет хуже защищено от новых киберугроз.

По возможности откажитесь от бесплатного вайфая. Публичные сети могут быть недостаточно защищёнными. Злоумышленники взламывают и перехватывают трафик, который идёт с вашего устройства. В их руках окажутся секретные данные, в том числе логины и пароли от различных аккаунтов. Кроме того, мошенники могут сами размещать точки доступа и выдавать их за бесплатный вайфай в парках, кафе и торговых центрах.

Приложение: информация.

Прокурор района

советник юстиции К.А. Кобылкин

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 0096D1B50729198A06D89F28771F7B1F2D
Владелец **Кобылкин Константин Александрович**
Действителен с 15.05.2024 по 08.08.2025

С.И. Кухарь, тел. 8 (47395) 40-7-45