**Стандарт конфиденциальности и защиты персональных данных в аккаунтах в интернете и в службах поддержки пользователей в чатах и телефонии.**

**Проблемы**

В разных сегментах интернета, на сайтах и в мессенджерах, в чатах и в телефонных поддержках операторов применяются разные параметры и объёмы затребования, обработки и конфиденциальности персональных данных граждан, зафиксированные в правилах и условиях пользования ресурсом или установленные «по умолчанию» при взаимодействии с разными сервисами и при оказании цифровых услуг. Сейчас есть немало ценных наработок в области защиты частных аккаунтов, но требуется их дальнейшее усовершенствование, унификация, тонкая настройка.

Отсутствие понимания пользователями интернета и связи, какие данные в конкретном случае они обязаны предоставлять третьим лицам (операторам, техслужбам и разработчикам приложений), какие не обязаны, как их отзывать по правилам сайта или ресурса, не всегда составленным с учётом законодательства, положениям 23 статьи Конституции РФ, ФЗ №152 «О персональных данных», ведёт к нарушениям прав и злоупотреблением доверием граждан, – к излишним запросам персональной информации, незаконному её использованию и распространению вопреки воле пользователей. Не всегда создатели интернет-ресурсов, разработчики и сотрудники технических поддержек (специалисты IT) имеют благие намерения при собирании персональной информации. Это касается и излишних запросов персональных данных в автоматизированных диалоговых окнах, в интернет-приёмных, в меню телефонных справочных, «горячих линий» с применением слабого искусственного интеллекта. Бывает, хакеры пользователей обманывают или совершают мошеннические действия, навязывают лишние сервисы для контролируемой связи, отслеживают информацию о финансах и имуществе, могут получить доступ к аккаунтам и распорядиться этими данными с целью собственной материальной выгоды, проще говоря – пытаются обмануть, взломать и украсть.

Отсутствие должного надзора и контроля за правоустанавливающими документами в интернете, за правомерностью действий владельцев сетей, технических поддержек, специалистов интернета, разработчиков и операторов, отсутствие единой, доступной круглосуточно, бесплатной службы безопасности – в МВД (отдел К), в российском интернете и в услугах мобильной и стационарной связи для ведомств и организаций – создаёт угрозу утери и мошеннических действий с ними, способствует преступлениям. Растут и технические возможности для создания фальсифицированных файлов – изображений, документов, видео, подписей, а системы шифрования применяются недостаточно или неумело.

Не стоит забывать, что бумажный паспорт гражданина России – это единственный пока удостоверяющий личность гражданина документ, с биометрическими данными, который предъявляется лично при заключении пользовательского договора об оказании услуг оператору связи или провайдеру. Большинство сайтов и социальных сетей в интернете регистрируют данные пользователя через мобильный номер телефонии, но единый договор не учитывает это взаимодействие служб, не обеспечиваются ЕДИНЫЕ условия конфиденциальности и защиты персональных и биометрических данных пользователя от провайдера и мобильного оператора по ЕДИНОМУ договору. Не все технические службы интернета и связи пока готовы идентифицировать пользователя по местоположению, мобильному номеру, IP-адресу и ID устройства, и для этого также требуется разрешение пользователя.

Добавление в персональный аккаунт (личный кабинет) данных пользователем без дополнительных методов защиты не гарантирует их безопасность и конфиденциальность, так как изначально номера телефонов или адреса электронной почты могут быть известны другим гражданам (например, по медицинским картам, при сообщении их разным организациям и ведомствам, обработчикам данных в банках, ФНС, МФЦ, МВД, в интернет-маркетах и т.д.). Гражданину же разработчики предлагают «для удобства» использовать номер телефона, банковской карты, СНИЛС, ИНН, полиса ОМС, номера счетов по услугам ЖКХ, данные паспорта в качестве логина или вспомогательной информации для восстановления доступа и входа в его аккаунт! Граждане часто не понимают, как в связке эти данные позволяют хакерам и мошенникам взламывать аккаунт, получать доступ к их личному кабинету, распоряжаться содержимым вместо владельца.

**Предлагаю:**

1. Министерству цифрового развития, Министерству связи, Правительству РФ, СБ МВД, СБ банков и портала Госуслуг, ответственным поставщикам услуг интернета и связи предпринять действия, чтобы уравнять технические возможности регистрации, входа и восстановления доступа к персональным данным для веб-версий аккаунтов в разных браузерах и мобильных приложениях, на разных устройствах и с разным программным обеспечением, и, согласно 34 статье Конституции РФ о запрете недобросовестной конкуренции, обеспечить равные условия использования браузеров, мобильных приложений, добавив повсюду встроенный перевод текстов на разные языки мира.
2. Публиковать свод правил и условий пользования услугами интернета и связи, обязанности сторон на официальном государственном сайте, в доступных для сохранения и печати форматах.
3. Изменить и стандартизировать для РФ формы, шаблоны бумажного договора с Пользователем интернета (связи), указывать в нём паспортные данные и номер телефона (электронной почты), а операторам и провайдерам вменить в обязанность ответственность за сохранность данных гражданина, соблюдение единых правил конфиденциальности. Установить способы шифрования электронных документов и архивов с задействованием разных контактов гражданина в случае необходимости соблюдения тайны переписки.
4. В качестве логина и пароля аккаунта использовать придуманные самим пользователем комбинации из букв, цифр и символов, присутствующие во всех языках мира, на разных компьютерных устройствах, гаджетах. Возможно автоматически генерировать надёжные пароли.
5. Предусмотреть возможность добавления резервных данных – номера телефона (в том числе стационарного) и дополнительного электронного адреса почты для доступа в аккаунт и обращения в поддержки. В настройках компьютерного устройства и в настройках аккаунта для пользователя обеспечить выбор варианта предпочтительного способа входа, возможность запрета входов, например, по телефонному номеру, по SMS-коду или по другим данным (кодовым словам, ответам на вопросы).
6. Адрес электронной почты и (или) телефон использовать для уведомлений пользователя о входах с незнакомых устройств или адресов, изменениях данных в аккаунте.
7. Для сим-карт мобильной связи предусмотреть более сложную защиту – 5-6-значным цифровым кодом, или двойными кодами pin и puk, применять сложные коды для подтверждения действий пользователя в личных кабинетах и приложениях. Не использовать словесные или подменяющие цифровые комбинации кодов ссылки для перехода-подтверждения пользовательских действий, так как гражданин может использовать разные мобильные гаджеты без интернета.
8. Отказаться от использования последних цифр номера входящего звонка на телефон пользователя в качестве кода-пароля для подтверждения действий в аккаунте. Для временных периодов ожидания и повторного запроса автоматических SMS-кодов установить оптимальные сроки их действия.
9. Переадресации звонков и SMS на другой номер, смена паролей и логинов, кодовых слов и контрольных вопросов, отключение и включение дополнительных функций и услуг от мобильной сети, управление по доверенности, включение в группы, заказ и изготовление дубликатов и дополнительных сим-карт при утрате или смене номера, оператора – всё это должно быть доступно только самому пользователю или с его разрешения. Заменённые сим-карты должны блокироваться операторами навсегда или уничтожаться. Запретить продажу сим-карт с подключёнными по умолчанию платными услугами интернета и связи или раскрывающими данные пользователя. Подмену телефонных номеров следует запретить!
10. Электронные чеки по проведённым платежам за услуги связи и интернета предоставлять в форматах, позволяющих сохранение на устройстве и в виртуальных облачных, дисковых хранилищах. При проведении оплаты по системе СБП указывать источник пополнения счёта сим-карты или ФИО плательщика, чтобы избежать незаконных, мошеннических действий, для отчёта по налогам.
11. Данные о входах в аккаунт, истории действий в нём, перечень используемых компьютерных устройств сайтам, компаниям и провайдерам хранить полгода, дольше – при наличии у них технической и финансовой возможности.
12. Доступ третьих лиц, сотрудников специальных служб с полномочиями (например, технических служб интернета по запросам от МВД, СК, ФСБ) к персональным данным гражданина и истории его действий в интернете, к телефонной прослушке звонков, отслеживанию местонахождения с помощью специальных средств и приложений, по закону предоставлять лишь с его личного письменного разрешения или (в случае угрозы для его жизни и здоровья) без такового, но с составлением документа, поясняющего основания и причины нарушения 23 статьи Конституции РФ в отношении данного гражданина. Отделам служб безопасности необходимо уведомлять граждан о взломе аккаунта и получении несанкционированного доступа к персональной информации.
13. Правила пользования аккаунтами разных социальных сетей, мессенджеров, сайтов компаний корректировать и совершенствовать с учётом мнений пользователей через универсальные системы обратной связи. Указывать ответственных за соблюдение правил, контролирующих качество работы сервисов и услуг. Службам безопасности и разработчикам сайтов, приложений запретить по умолчанию запрашивать без конкретных целей, обоснований необходимости данные пользователей, запретить передавать их без разрешения владельца третьим лицам.

**Решение**

1. Правила и условия пользования интернетом и связью получат официальный государственный статус, будут соответствовать законодательству России, отвечать запросам граждан, станет возможным их сохранение и перевод. Монополия в оказании услуг прекратится.
2. Установленные провайдерами и операторами мобильной связи единые параметры конфиденциальности и защиты персональных данных обеспечат их совместную ответственность за утечки данных; пользователям будет гарантирована помощь сотрудников IT и связи.
3. Владельцы разных компьютерных устройств, гаджетов смогут иметь равные функции аккаунтов в мобильных приложениях и в веб-версиях разных браузеров.
4. Система защиты сим-карт, аккаунтов и данных пользователей паролями и кодами усилится.
5. Договоры на оказание услуг и отчётные документы платёжных сервисов станут полнее и точнее.
6. Поддержки и операторы чатов, телефонии не станут запрашивать излишние данные пользователей. Несанкционированный сбор данных и доступ к личной информации будет ограничен рамками действующего законодательства. Применяемому повсеместно (хотя по ФЗ № 123 от 24.04.2020 г. это незаконно) искусственному интеллекту граждане помогут совершенствоваться быстрее.
7. Пользователю станет доступна информация об истории действий в его аккаунте, об устройствах, имеющих доступ к нему, о взаимодействии служб и сервисов интернета и связи за указанный период времени. Повысится доверие к услугам связи и интернета.