Цифровая гигиена и личная безопасность в интернете

Сегодня распространена фраза «Интернет помнит все». Это значит, что переписки, фото, видео, пароли, банковские карты, лайки, просмотры и другие наши данные и действия в социальных сетях хранятся в интернете, могут быть потеряны и использованы мошенниками.

Чтобы обезопасить себя от интернет-угроз, существует свод правил, который помогает оставлять меньше цифровых следов и сохранить свои личные данные. Этот комплекс мер называют цифровой гигиеной.

Утечки персональных данных

Утечки данных – распространенная проблема в мире. Только в России за 2023 год Роскомнадзор зафиксировал 168 утечек персональных данных, более 300 млн записей о россиянах попали в сеть.[1] А всего в мире за первую половину 2023 года зафиксировали 5 532 утечки информации, что в 2,4 раза больше показателей за предыдущий год.[2]

Экспертно-аналитический центр ГК InfoWatch провел исследование об утечке данных за 2023 год. Объем утекших персональных данных в 2023 году составил 1,2 млрд записей — это на 60% выше уровня 2022 года (тогда было зафиксировано 702 млн записей). Если говорить о количестве инцидентов, то в 2023 году оно сократилось на 15% и составило 656 эпизодов. Всего за отчетный период из российских компаний утекло 95 крупных баз данных, что на 28% больше, чем в 2022 году. Более 80% утечек информации произошло в результате кибератак. Каждая десятая напрямую связана с действиями персонала, однако этот показатель сократился на 45%. В InfoWatch отметили увеличение доли утечек государственной тайны в 2023 году в 3,6 раза — с 1,8 до 6,6%; из них 73,6% информации относилось к персональным данным.

---

1 В 2023 году в сеть утекло более 300 млн записей о россиянах (https://tass.ru/obschestvo/19693845). Дата обращения: 01.02.2024

2 Тайное познание: число утечек информации в мире выросло в 2,4 раза | Статьи | Известия (https://iz.ru/1563836/ivan-chernousov/tainoe-poznanie-chislo-utechek-informatcii-v-mire-vyroslo-v-24-raza). Дата обращения: 01.02.2024

Согласно исследованию, общий объем утекших из госорганов сведений вырос до 19,2%, что на 5,3 п.п. больше по сравнению с 2022 годом. Согласно данным опроса ГК InfoWatch, в ответ на ухудшение ситуации с утечками конфиденциальной информации в 2023 году 59% организаций провели обучение сотрудников основам информационной безопасности и гигиены, 27% — внедрили системы защиты от вторжений, еще 17% установили DLP-системы (программный продукт для предотвращения утечек конфиденциальных данных в корпоративной сети).[3]

По словам специалистов по информационной безопасности, персональные данные, коммерческая и государственная тайна – сведения, которые наиболее интересны злоумышленникам. По числу утечек США находятся на первом месте. За последний год почти в 7 раз выросло количество утечек данных в Индонезии, в 2,5-3 раза в странах Европы и Северной Америки.[4]

В России же, наоборот, число утечек упало на 15,5%.[5] Это связано с мерами, которые принимает государство для создания безопасного цифрового пространства. В 2022 году был принят Федеральный закон № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», согласно которому российские пользователи могут потребовать иностранные компании уничтожить персональные данные, полученные незаконно, и получить информацию, кто и как их обрабатывает.[6] Чтобы минимизировать количество утечек, Роскомнадзор разработал правила по

---

[3] Аналитики оценили рост утечек персональных данных в России (https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9?ysclid=ltmrokhruq969210881). Дата обращения: 11.02.2024

4 Там же.

5 Там же.

6 Роскомнадзор рассказал, как защищать персональные данные - Российская газета (https://rg.ru/2023/03/02/roskomnadzor-rasskazal-kak-zashchishchat-personalnye-dannye.html). Дата обращения: 01.02.2024

сохранению личных данных для операторов, которые собирают данные клиентов.[7]

Снижение количества утечек связано с адаптацией IT-подразделений и служб информационной безопасности в российских компаниях к новым типам угроз. К принятым мерам относятся и инициативы властей по импортозамещению. 12 июня Президент РФ Владимир Путин подписал поручение, что к 1 января 2025 года все государственные компании должны перейти на отечественное ПО. «Если раньше было требование только по объектам КИИ, то теперь обязательные требования по разным классам: операционные системы, офисные пакеты, офисные приложения, СУБД, средства виртуализации. В этом смысле KPI достаточно жесткий», – прокомментировал поручение Президента глава Министерства цифрового развития, связи и массовых коммуникаций Максут Шадаев.[8]

Часть российских компаний уже перешла на отечественное ПО. По словам генерального директора «МойОфис» Павла Калякина, в ноябре 2023 года в сегменте офисного ПО на долю российских разработчиков приходилось примерно 16% рынка, при этом год назад показатель не превышал 5%. А российские решения в секторе промышленного софта заняли практически 100% рынка.[9]

Российские компании уже перешли на отечественные сервисы хранения данных («Яндекс.Диск», «Яндекс.Почта» и др.), поскольку Google отказался от обслуживания российских клиентов и начал блокировку корпоративных

---

7 Власти опубликовали рекомендации по защите персональных данных (https://assistentus.ru/aktualno/roskomnadzor-rasskazal-kak-zashhitit-personalnye-dannye-ot-moshennikov/). Дата обращения: 01.02.2024

8 Максут Шадаев: Госкомпании к 1 января 2025 года должны перейти на российские ОС и офисное ПО - Российская газета (https://rg.ru/2023/06/17/maksut-shadaev-goskompanii-k-1-ianvaria-2025-goda-dolzhny-perejti-na-rossijskie-os-i-ofisnoe-po.html) Дата обращения: 01.02.2024

9 Внедрение произведенных в России программных продуктов ускоряется во всех отраслях экономики - Российская газета (https://rg.ru/2023/11/29/perehod-koda.html). Дата обращения: 01.02.2024

сервисов. По словам аналитиков, часть зарубежного ПО и облачных сервисов могли содержать опасные уязвимости.[10]

Также российские ведомства ввели запрет на использование iPhone и iPad для служебных целей.[11] Сотрудники переходят на модели российских производителей. Например, «Ростех» выбрал смартфоны собственного бренда AYYA с защищенной отечественной операционной системой «Аврора», которые используют сотрудники «Росатома» и силовых структур.[12] Это позволяет организациям лучше защитить базы данных от утечек и кибератак.

Интернет-мошенничество

Однако мошенников интересуют не только данные государственных учреждений и крупных компаний, но и обычных людей. В январе – июне 2023 года на 39,3%, по сравнению с предыдущим годом, выросло число преступлений с помощью интернета и средств мобильной связи. В Генпрокуратуре зарегистрировали более 210,8 тысяч мошенничеств.[13]

Доступ к личным данным с паролями и банковскими картами часто попадает в руки мошенников из-за действий самих людей.

Самые распространенные схемы мошенничества, при которых люди сами передают свои данные злоумышленникам:

- обзвон граждан от имени правоохранительных органов или банков
- создание фальшивых (фишинговых) сайтов для получения доступа к конфиденциальным данным пользователей
- рассылка писем о «крупном выигрыше» по электронной почте
- фальшивые сайты благотворительных организаций/туроператоров/авиакомпаний .

---

10 Тайное познание: число утечек информации в мире выросло в 2,4 раза | Статьи | Известия (https://iz.ru/1563836/ivan-chernousov/tainoe-poznanie-chislo-utechek-informatcii-v-mire-vyroslo-v-24-raza). Дата обращения: 01.02.2024

11 Российские ведомства ввели запрет на технику Apple. Чем госсектор может ее заменить? - Российская газета (https://rg.ru/2023/08/21/mobilnye-rezervy.html). Дата обращения: 01.02.2024

12 Как российские чиновники и госкорпорации отказываются от техники Apple – Ведомости (https://www.vedomosti.ru/politics/articles/2023/09/06/993630-kak-rossiiskie-chinovniki-i-goskorporatsii-otkazivayutsya-ot-tehniki-apple). Дата обращения: 01.02.2024

13 В России число совершенных через мобильную связь и интернет преступлений выросло на 39% (https://tass.ru/obschestvo/18417795). Дата обращения: 01.02.2024

- предложение выгодного заработка на подозрительных интернет-ресурсах
- взлом личных аккаунтов пользователей и рассылка сообщений
- Лотереи, викторины, конкурсы, где нужно заплатить «налог на выигрыш» или «комиссию за доставку приза»

Один из распространенных методов мошенничества – фишинг, с которым с начала 2023 года столкнулось больше половины россиян. Согласно опросу интернет-пользователей компанией «МТС Red», фишинговые рассылки приходят два и более раз в месяц. Такие письма обычно содержат предложения выгоды, быстрого заработка. Среди опрошенных 48% заинтересовались акциями с высокой доходностью, 28% – товарами с большой скидкой. Около 12% участникам опроса пришли письма о неоплаченных штрафах, задолженностях и нарушениях законодательства. Получить доступ к данным банковских карт злоумышленники пытались в 35,8% случаев, в 24,4% – узнать паспортные данные, в 17,9% – логины и пароли от разных сервисов.[14]

С каждым годом количество фишинговых атак увеличивается на 50%, как утверждают в центре мониторинга внешних цифровых угроз Solar AURA. Иногда компания фиксирует 50 фишинговых сайтов в день, которые действуют под именем определенного бренда. Создаются новые вредоносные ресурсы, фишинговые Telegram-боты, площадки для розыгрыша призов, сервисы оформления доставки товаров. В 2023 году количество мошеннических сайтов выросло на 86% и составило 207,1 тысяч.[15] Было заблокировано более 48 тысяч вредоносных доменов.

Часто злоумышленники похищают аккаунты в социальных сетях и размещают через них фишинговый контент, объявления, просят перевести деньги, а потом атакуют пользователей из списка контактов. Обычно взлом

---

14 Более половины россиян столкнулись с мошенничеством в интернете с начала года – Ведомости (https://www.vedomosti.ru/technology/articles/2023/08/02/988049-bolee-polovini-rossiyan-stolknulis-s-moshennichestvom-v-internete). Дата обращения: 01.02.2024

15 Число мошеннических сайтов в 2023 году выросло на 86% (https://iz.ru/1625951/ivan-chernousov/fishingovaia-priamaia-chislo-moshennicheskikh-saitov-v-2023-godu-vyroslo-na-86). Дата обращения: 01.02.2024

учетной записи дает доступ к паролям, документам, фотографиям паспорта и банковских карт, которые могут быть у нас в сохраненном.

Правила цифровой гигиены

Помимо сохранения своих личных данных важно позаботиться об анонимности, приватности, цифровом образе, защите от нежелательных знакомств, кибербуллинга и сохранении репутации. Чтобы обезопасить человека от интернет-угроз, разработаны правила поведения в интернет-пространстве и пользования цифровыми устройствами, которые важно знать и детям и взрослым:[16]

1. Нельзя передавать свой телефон незнакомым людям под предлогом срочного звонка. Так человек получит доступ к разблокированному телефону.
2. Пароли должны быть длинные и надежные (не менее 12 символов, с цифрами, заглавными и строчными буквами, непоследовательными комбинациями, без личной информации), усиленные биометрией и двухфакторной аутентификацией. Их нужно регулярно менять, не применять один и тот же для нескольких учетных записей и никому не сообщать. Чтобы создавать, хранить пароли и управлять ими, можно использовать менеджер паролей.
3. Необходимо установить оригинальные пароль, PIN-код и другие виды защиты для блокировки компьютера и телефона.
4. Сохранить все файлы в безопасности и не потерять помогает регулярное резервное копирование данных на внешнем жестком диске или в облаке.
5. Обращать внимание на уровень конфиденциальности в сети. Все, что вы рассказываете о себе в интернете, может быть использовано против вас. Нужно избегать публикации личной информации в социальных сетях (номер телефона, фото, домашний и рабочий адреса, номера кредитных

16 Безопасный интернет: главные правила цифровой гигиены | Национальные проекты России (https://национальныепроекты.рф/news/bezopasnyy-internet-glavnye-pravila-tsifrovoy-gigieny) . Дата обращения: 01.02.2024

и банковских карт, местоположение) и контролировать, что и кому вы говорите. Отрегулировать настройки приватности, как будет для вас комфортно.

6. Не принимать заявки в социальных сетях от незнакомых и сомнительных людей, всегда проверять наполнение страницы.
7. При установке нового приложения проверять, к каким данным на вашем устройстве у вас запрашивают разрешение. Не всегда доступ к камере и микрофону оправдан.
8. Регулярно обновлять программы, приложения и операционные системы. Старые версии могут быть более уязвимы для атак. А неиспользуемые приложения лучше удалять. При этом не рекомендуется скачивать программы и ПО с неизвестных сайтов. Это может стать причиной заражения вашего устройства и утечки данных.
9. Внимательно открывать электронные письма и их содержимое с неизвестных адресов, которые выглядят подозрительно. И не переходить по объявлениям, ссылкам и предложениям, которые обещают скидки, призы и денежные выигрыши. В них могут содержаться фишинговые ссылки или вирусы.
10. Отписываться от ненужных рассылок и подписок.
11. При использовании публичных сетей Wi-Fi быть аккуратнее, особенно при открытии мобильного банка. Злоумышленники часто используют такие сети в своих целях. При онлайн-транзакциях проверять безопасность веб-сайтов. Все адреса начинаются с https://, а не с http://, а слева от адресной строки есть значок замка. .
12. Контролировать, что вы или ваши близкие покупают в интернете. Под видом онлайн-магазина могут быть мошенники.
13. Использовать сетевой экран. Он предотвращает несанкционированный доступ к вашим веб-сайтам, почте, паролям и другой информации, которую можно получить через интернет. А при переходе на сайты

обращать внимание на маркировку надежности и на что требуется разрешение.

14. Использовать хорошее антивирусное программное обеспечение, регулярно проводить автоматическую проверку устройства на вредоносные программы.
15. При продаже старых гаджетов отформатировать и очистить жесткий диск, чтобы не произошло передачи личных данных.[17]

Безопасное поведение в сети

Как мы сказали выше, к цифровым следам относятся любые ваши действия с контентом. От того, какие публикации вы лайкаете, комментируете, чем делитесь и на чем задерживаете свой взгляд, зависит лента и реклама, которую подбирают для вас алгоритмы сети. Бездумное потребление информации ведет к рассеиванию внимания и потреблению лишнего и даже опасного контента.

Не нужно реагировать на материалы, которые нарушают законодательство, распространяют недостоверную информацию или призывают к противоправным действиям, и при этом создавать такой контент самим.

Сегодня особенно важно распознавать фейки, это одно из главных правил цифровой гигиены. На что обратить внимание:

- насколько эмоциональный заголовок;
- какие источники у новости и насколько они авторитетны;
- какое качество у фотографий и видео;
- новость содержит факты или субъективный взгляд;
- есть ли опечатки и ошибки в тексте;
- корректен ли адрес домена — защищенное соединение всегда будет иметь адрес, который начинается с https://

17 Кибергигиена: определение и чек-лист (https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-hygiene-habits). Дата обращения: 01.02.2024

Также уделяйте внимание надежности ваших аккаунтов в Сети. Устанавливайте длинные пароли и регулярно меняйте их. Чем короче и легче пароль, тем быстрее его можно подобрать при использовании метода полного перебора (брутфорс). Чем надежнее пароль, тем больше времени потребуется для его подбора. Так, злоумышленники могут потратить на вас от 1 секунды до нескольких миллиардов лет.

Также, чтобы отличить достоверные новости от фейковых и не попасться на уловки мошенников есть ряд общих рекомендаций:

1. Доверяйте только проверенным источникам.
2. Дайте новостям время: перепроверяйте информацию, добытую «по горячим следам».
3. Проверяйте факты самостоятельно в нескольких авторитетных и официальных источниках.
4. Следите за порталами, которые раскрывают фейки и сообщают о них
5. Проверяйте видео на дипфейки: следите за артикуляцией говорящего и его мимикой. При любом несовпадении проверьте данную информацию.

Помимо соблюдения всех перечисленных правил цифровой гигиены, важно делать перерывы и разгрузку от информационного шума. Сегодня потоки информации поступают к нам отовсюду. На работе ведем деловую переписку, собираем данные, пишем отчеты. В свободное время потребляем новости из телевидения, радио, прессы, интернета, следим за другими людьми в социальных сетях, смотрим фильмы, читаем книги, слушаем подкасты. Переизбыток любого контента ведет к информационным перегрузкам.

Такое состояние может сказаться на самочувствии, качестве работы, отношениях с близкими. Чтобы избежать негативного сценария, нужно соблюдать цифровую гигиену. Рекомендации, приведенные выше, помогут не подвергать себя постоянному стрессу, оставаться энергичными и сохранить

активность и гибкость мозга, а самое главное, защитить себя от мошеннических действий.