**Вирусы и приложения**

Разговоры о соблюдении правил информационной безопасности идут давно. Банковский сектор не остается в стороне и точно также информирует своих клиентов о необходимости соблюдения простых правил, которые помогают предотвратить кражу информации и денег. Максим Сёмов, председатель Комитета по повышению финансовой грамотности АРБ, эксперт проекта НИФИ Минфина России «Моифинансы.рф» в [интервью Российской газете](https://rg.ru/2025/02/26/virus-potroshitel.html) о правилах личной финансовой безопасности мобильных устройсвт.

Увы, часто такие призывы остаются без внимания со стороны клиентов. Сколько раз мне, а также моим коллегам приходилось разбирать жалобы клиентов с вопросами «откуда мошенники узнали мои персональные данные?». И почти всегда, увы, в результате разбирательства, видно, что виноват сам клиент – установил непонятное мобильное приложение, открыл ссылку, нажал на кнопку, сообщил неизвестному код.

На встречах с гражданами, когда задают вопрос об утечках персональных данных, я прошу поднять руки тех, у кого установлено приложение Getcontact. И каждый раз поднятые руки. Люди сами добровольно отдают свои данные неизвестно кому и неизвестно для каких целей!

Я вижу, что социальная инженерия сменяется криминальной инженерией, обеспеченной программным средствами, техникой, поддержкой, исполнителями – то есть инфраструктурой, в которой использование живого человека, хотя и является необходимым, но уже не единственным условием совершенного преступления.

В реальности, никто не знает, какими данными оперирует набор установленных приложений. И речь не только про вирусы, скрывающиеся внутри приложений.

Вот приложение «Фонарик», для работы которого нужен Wi-fi. Вот приложение «Компас», требующее разрешение на управление сообщениями. А вот приложение… Так… Когда я его поставил и зачем? Установка мобильного приложения занимает несколько секунд.

Это привело к тому, что появились и собрали свой урожай приложения, имитирующие работу государственных структур (якобы собирающие информацию о положенных выплатах и льготах, но на самом деле собирающие данные доверчивых граждан и плату за «перечисление выплаты»), приложения, использующие государственную символику и также собирающие данные граждан (статистические, социальные приложения). Массово пошли в народ экономические игры, сулящие большой заработок (по сути, обычные пирамиды в новой оболочке) и многое другое.

Не приводя примеры подобных приложений, можно отметить эффективные правила информационной безопасности:

* Не устанавливайте мобильное приложение из неизвестных источников. Тем более по просьбе незнакомого человека. Также следует отнестись к просьбе знакомого – во-первых, убедитесь, что вас просит действительно ваш знакомый. Во-вторых, установка возможна только после тщательного анализа работы приложения, чтения отзывов, рекомендаций, и посещения сайта разработчика.
* Как правило, зараженные приложения попадают в смартфоны граждан, кликнувших на сообщении от незнакомого в мессенджере (обычно это сообщение «Посмотри, это ты на фото?») – значит никаких действий по просьбе или требованию незнакомых лиц, совершать нельзя!
* Не давайте приложениям лишних разрешений (вспоминайте про «Фонарик с Wi-fi)
* Любая просьба о помощи, заманчиво выгодное предложение, обращение – все это должно быть оценено на предмет безопасности.
* Обновите антивирусное ПО. Ах, да – у большинства же его нет. Значит, установите.
* Не проходите по ссылкам, пока не убедитесь, что эта ссылка точно от знакомого вам человека.
* Установите надежный пароль или PIN-код на блокировку экрана.
* Внимательно используйте бесплатный Wi-fi. Откажитесь от авторизации в такой сети через аккаунты в соцсетях или мессенджерах.
* Создавайте резервные копии ваших данных. Это делается автоматически в любой мобильной операционной системе.
* Не спешите. Не поддавайтесь на заманчивые предложения – сначала оцените их.

Скорость и удобство сервисов упрощают жизнь только тем, кто обладает критическим мышлением.