Приложение №1

Рекомендуемые меры по защите учетных записей в мессенджерах и социальных сетях

1. Используйте надежный пароль. Пароль должен:
   - состоять из букв разного регистра, символов и цифр;
   - содержать не менее 12 символов;
   - быть уникальным (не повторяться в различных сервисах);
   - меняться 1-2 раза в год;
   - быть абстрактным: не означать ничего, что связано с личной жизнью.
2. Для управления и хранения паролями используйте только специальные программы-менеджеры паролей от официальных компаний-разработчиков (например, Kaspersky password manager).
3. Всегда используйте двухфакторную аутентификацию (во всех аккаунтах, мессенджерах). Включите ее в настройках конфиденциальности.
4. Не открывайте подозрительные файлы и ссылки (любая ссылка, направленная вам, особенно о которой вы не просили, является подозрительной, проявите к ней бдительность. Неважно, близкий это человек или незнакомец — любой аккаунт может быть взломан).
5. Не авторизуйтесь через социальные сети на сомнительных сайтах.
6. Регулярно проверяйте в настройках историю активности аккаунта социальной сети или мессенджера, завершайте подозрительные сеансы.
7. Установите в настройках оповещения о входах в аккаунт. При получении подозрительного сообщения о входе, незамедлительно поменяйте пароль.
8. Установите разблокировку вашего устройства код-паролем, на случай если устройство украдут.
9. Отключите в настройках автозагрузку файлов.
10. В учетной записи в Telegram необходимо в «Настройках» в разделе «Конфиденциальность» поставить отметку напротив графы «Мои контакты».

    Таким образом, вы разрешите видеть ваш номер телефона и информацию о вас только тем пользователям, которые есть в ваших контактах. Это существенно снижает риск атаки на ваш аккаунт со стороны злоумышленников. Сделайте аналогичные настройки для ваших родственников.

Если ваш аккаунт взломали аккаунт, необходимо оперативно выполнить следующее:

1. Если доступ к аккаунту есть на другом устройстве, завершите все сессии и как можно быстрее смените пароль;
2. Заблокируйте все банковские карты, привязанные к учетной записи;
3. Предупредите близких и друзей о том, что ваш аккаунт взломали;
4. При наличии служебных чатов или других коллективных чатов, разместите в них объявление о взломе вашего аккаунта или о появлении вашего личного фейкового аккаунта, сообщите об этом любым доступным способом;
5. Если доступ к взломанному профилю закрыт, попробуйте восстановить пароль через телефон или почту;
6. Оформите жалобу в службу поддержки, подтвердите, что вы настоящий владелец аккаунта;
7. Попросите друзей пожаловаться в службу поддержки на ваш взломанный/фейковый аккаунт. Чем больше жалоб, тем быстрее мошенника заблокируют;
8. Не поддавайтесь на угрозы и шантаж, не платите выкуп — нет никакой гарантии, что взломщик получит деньги и вернёт аккаунт в сохранности или не выложит ваши персональные данные в общий доступ.