Приложение №2

Признаки фейковых[1] аккаунтов, рекомендации по их идентификации и алгоритм поведения в случае их выявления

Признаки фейкового аккаунта в социальной сети, мессенджере:

1. Скрытый номер телефона аккаунта;
2. Номер или ID пользователя не совпадает с известным вам номером пользователя;
3. Фото профиля содержит случайную картинку или фотографию пользователя из сети интернет;
4. Личная информация в профиле либо отсутствует, либо нелогична;
5. Собеседник направляет ссылки или адреса электронной почты, которых вы не просили и/или побуждает вас к какому-то действию;
6. Фейковые аккаунты недолговечны, поэтому дата регистрации пользователя всегда будет недавней;
7. Короткая подозрительная беседа с переходом к побуждающим действиям (запрос личной, финансовой, конфиденциальной, служебной информации, перенаправление на сторонние сайты).

[1] Фейковый аккаунт - это учетная запись, созданная от имени другого пользователя.

Алгоритм поведения в социальных сетях, мессенджерах с целью снижения риска атаки с фейковых страниц:

1. С максимальным подозрением относитесь к сообщениям от аккаунтов, которых нет в вашем списке контактов;
2. Старайтесь не отвечать на сообщения незнакомых людей с сомнительным содержанием;
3. Будьте бдительны, всегда тщательно проверяйте, с кем ведёте беседу, задавайте больше уточняющих вопросов. Это позволит понять с кем вы на самом деле общаетесь. В случае сомнений в реальности собеседника сразу прекратите общение, в случае уверенности в фейке – заблокируйте собеседника;
4. Если вас побуждают в мессенджере, социальной сети к какому-то действию – обязательно убедитесь в реальности собеседника. Свяжитесь с ним известным вам альтернативным способом (позвоните по мобильной связи, задайте уточняющие вопросы лично);
5. Если вам угрожают или пугают, остановите общение, проявите хладнокровие и терпение, сделайте паузу. Посоветуйтесь с близкими вам людьми, самостоятельно свяжитесь с руководством, силовыми структурами и так далее. Задача мошенников ввести вас в нестабильное состояние спешкой, паникой, испугом, ложными обещаниями;
6. Никогда не делитесь посредством мессенджеров своими личными данными, конфиденциальной, служебной информацией, информацией, содержащей персональные данные;

   Проявите бдительность, помните об установленных в вашем органе власти, учреждении правилах и способах обмена указанными видами сведений;
7. Никогда не переходите по подозрительным ссылкам из сообщений даже тех пользователей, которых знаете. Задайте уточняющие вопросы или позвоните отправителю сообщений, чтобы убедиться в актуальности ссылки;
8. Минимизируйте ввод личных данных на посторонней интернет странице.

Рекомендации по противодействию атаки с помощью методов социальной инженерии

Универсального рецепта противодействия мошенникам нет. Расчет мошенников на ваше любопытство, уважение к руководству, властям, сострадание к беде. Соблюдайте ключевые правила, которые сведут к минимуму ваши риски:

1. Всегда проверяйте источник информации, личность собеседника альтернативными способами;
2. Задавайте как можно больше уточняющих вопросов собеседнику;
3. В любой ситуации не спешите, остановитесь и подумайте. Посоветуйтесь с человеком, которому доверяете;
4. У всех должностных лиц требуйте данные, подтверждающие личность (паспорт, удостоверение, должность, место работы);
5. Проявите бдительность, оцените насколько правдоподобна ситуация, которая с вами происходит?