Рекомендации по выявлению фейк-аккаунтов

При получении подозрительных сообщений (пример – Рис. 1) стоит руководствоваться следующими правилами:

1. Не отвечать на сообщение, до момента выяснения информации об отправителе;
2. Не переходить по ссылкам указанным в переписке;
3. Не открывать и не загружать подозрительные вложения.

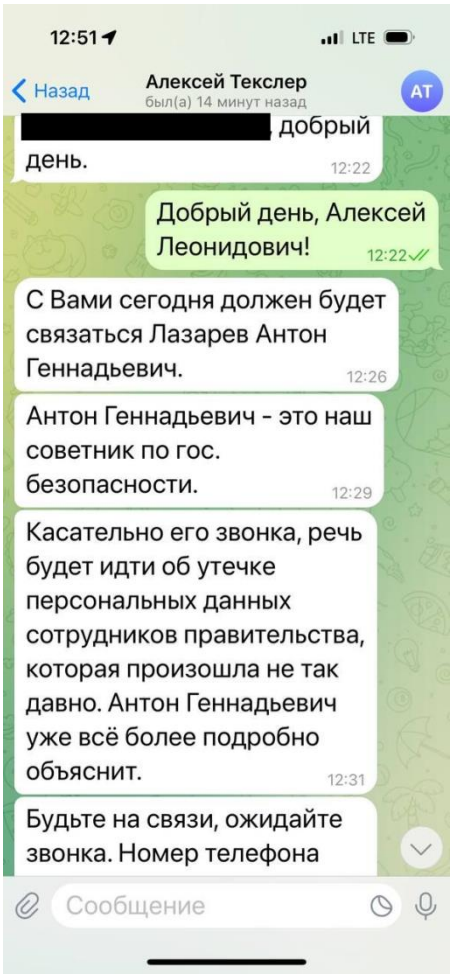

Рис. 1 – Пример подозрительной переписки.

Для однозначной идентификации пользователя, приславшего подозрительное сообщение, необходимо перейти в карточку пользователя и проверить его контактные данные, а именно: телефон (если известен) и «тэг» пользователя (имя пользователя). Если данная информация скрыта, то с большой долей вероятности, общение с вами ведет фейковый аккаунт.

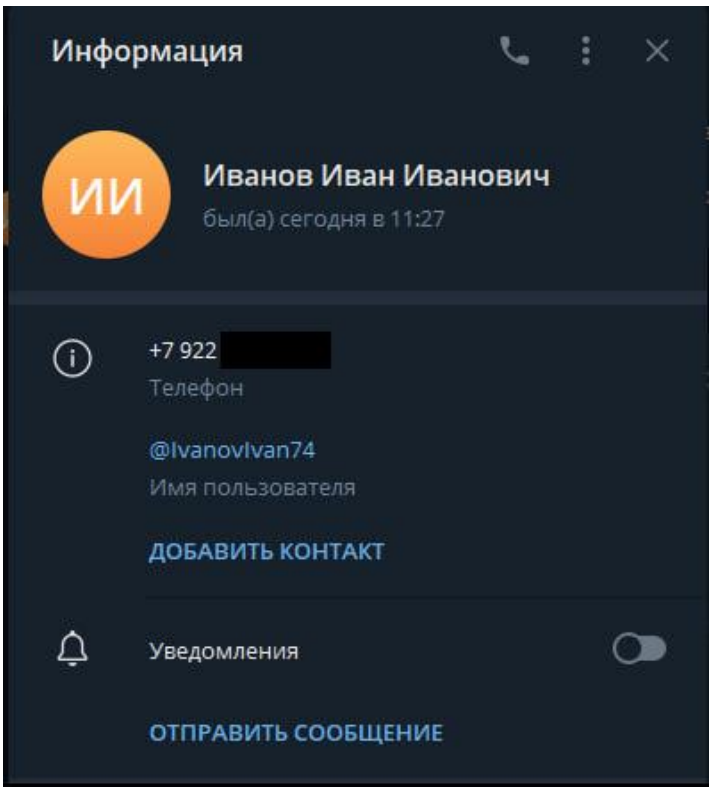

Рис. 2 – Пример достоверной карточки пользователя.

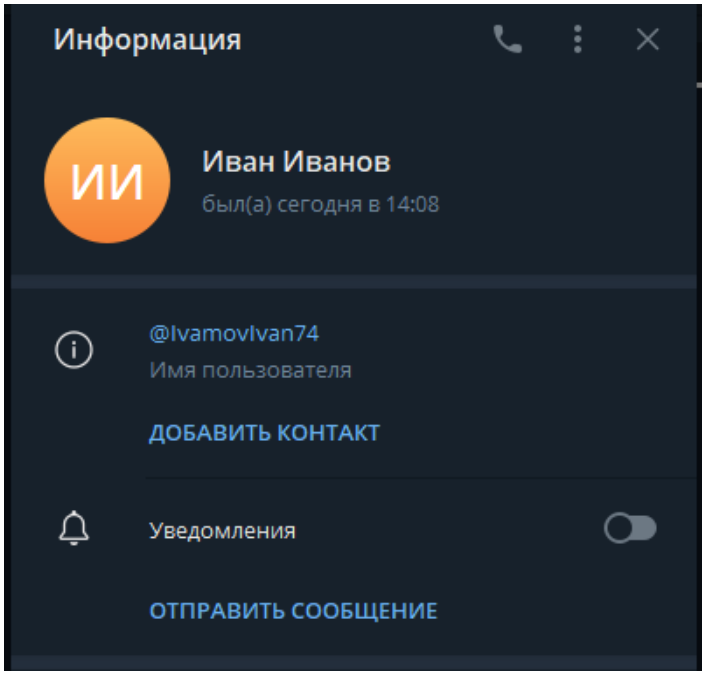

Рис. 3 – Пример карточки фейкового аккаунта

Обратите внимание на примеры (Рис. 2 и Рис. 3). У настоящего пользователя в карточке отображаются его номер телефона и настоящий «тэг». В то время как у фейка, отображен только «тэг» и для создания большего доверия к жертве, «тэг» прописан с 1 незаметной ошибкой. Буква «N» заменена на «M».