ОСТОРОЖНО! КИБЕРМОШЕННИКИ!

Кибермошенники все чаще стали использовать различные методы и техники социальной инженерии с применением технологии искусственного интеллекта для отправки сообщений от имени чужого контакта в мессенджерах и социальных сетях.

Основными из таких методов являются:

клонирование аккаунта, при этом клонируется профиль человека, включая его фотографии и информацию, чтобы создать похожий аккаунт, а затем мошенники отправляют сообщения от имени скопированного аккаунта;

подделка номера или идентификатора, при этом используются специальные программы или сервисы для изменения номера телефона или идентификатора аккаунта, связанного с мессенджером, а мошенники получают возможность отправлять сообщения, в том числе видео и голосовые, которые кажутся исходящими от определенного контакта.

Наиболее распространены сообщения от коллег, начальников и дальних родственников.

В случае получения подобных подозрительных сообщений необходимо руководствоваться следующими правилами:

не вступать в дальнейшую переписку;

не отвечать на вызовы с незнакомых номеров, о которых узнали из переписки;

не сообщать персональные данные и другую важную информацию;

сообщить о факте реальному владельцу аккаунта по другому каналу связи; необходимо настроить приватность;

запретить добавлять себя в группы людям не из вашего списка контактов; необходимо использовать функцию блокировки сеанса;

не передавать данные для входа в свой аккаунт;

не передавать через мессенджеры информацию о банковских картах; не передавать личную информацию сомнительным ботам;

обратиться в службу поддержки мессенджера или социальной сети с целью блокировки поддельного аккаунта.

Также необходимо избегать установки на смартфоны приложений, которые предоставляют доступ третьим лицам к телефонному справочнику