

АЛГОРИТМ
действий несовершеннолетних
при совершении мошенничеств в отношении них

ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА

СМС от различных сервисов (Госуслуги, банки, операторы связи, социальные сети и т.п.) о взломах аккаунтов.

– может поступить *сообщение о взломе* аккаунта, страницы с указанием номеров телефона/ ссылок на страницы сайтов, по которым нужно обратиться/ перейти для решения возникшей проблемы;

– после получения смс *поступает звонок от неизвестного лица* (либо пользователь сам перезванивает по указанному номеру телефона/переходит по ссылке), которое *представляется специалистом* сервиса и предлагает помощь в решении проблемы (восстановить аккаунт, обеспечить безопасность персональных данных и т.д.), *предупреждает* о возможном мошенничестве со стороны третьих лиц, в результате которого произошел взлом, может сообщить, что *с тобой свяжется* в ближайшее время сотрудник правоохранительных органов (МВД, Следственный комитет, ФСБ, прокуратура и др.) с целью поиска и привлечения мошенников к ответственности;

– после разговора с тобой может связаться незнакомое лицо и *представиться сотрудником* перечисленных *правоохранительных органов* и сориентировать на *определенный порядок действий*, который необходимо выполнять *в связи с имеющейся угрозой* в отношении тебя со стороны мошенников либо иных лиц (пройти по ссылкам, поступившим от него или его представителей в мессенджерах, быть с ним постоянно на связи, предоставить ему персональные данные, доступ к аккаунтам в мессенджерах, запрет на информирование родителей и близких о сложившейся с тобой ситуации, покинуть город, не возвращаться домой);

– после этого могут поступить звонки от этих же лиц либо от других, но тоже представляющимися сотрудниками правоохранительных органов либо банков, о попытках перевода твоих личных сбережений на иностранные счета, финансирования таким способом терроризма либо ВС Украины и т.п.), и предложениях в целях пресечения преступных операций *о необходимости осуществления переводов* денежных средств на «безопасные счета», на которые тебе указывают звонившие, *либо получения* обманным способом *этих средств от родителей* и необходимости их перевода неизвестным.

Необходимость перевода денег на «безопасный счет».

– могут поступить звонки от неизвестных лиц, которые представляются сотрудниками банков, служб безопасности, Центрального банка России либо правоохранительных органов, и *сообщают о якобы совершающихся в отношении тебя мошеннических действиях* (оформление кредитов, микрозаймов) и для предотвращения хищения твоих денег необходимо перевести их на «безопасный счет», после чего *просят доступ к личному кабинету банка*, где у тебя есть лицевые счета;

- звонки могут поступать по несколько дней подряд либо с перерывами, так *злоумышленники входят в доверие и убеждают* в необходимости совершения тобой определенных действий;

- в ходе общения с тобой неизвестные лица для подтверждения своих слов и действий могут отправлять фото документов, похожих на подлинные.

**Взлом либо копирование аккаунта пользователя в мессенджерах
Ватсап, Вайбер, Телеграм, социальных сетей Вконтакте и т.п.**

– с использованием нейросети (искусственный интеллект) генерируются видеозвонки, голосовые *сообщения от имени твоих знакомых, родственников, друзей*, у которых взломаны аккаунты в мессенджерах / социальных сетях, с *полностью скопированными голосом и изображением*, с использованием ранее отправленных видео и аудио сообщений твоих знакомых, родственников;

– поступают *просьбы оказать финансовую помощь*, сообщить о возникшей проблеме, в том числе, что твой знакомый, родственник, родитель *попал в серьезную беду, происшествие*, после чего могут прислать фото банковской карты либо номер телефона для перевода денег.

ПОРЯДОК ДЕЙСТВИЙ (ПРАВИЛА ПОВЕДЕНИЯ)

Не верить на слово лицам, звонящим с неизвестных номеров. Все поступающие тебе звонки с неизвестных номеров нужно ставить под сомнение и перепроверять.

Сообщить звонящему, что ты являешься несовершеннолетним и пусть все разговоры ведут с твоими родителями, после этого сразу прекратить разговор.

Незамедлительно после таких звонков сообщить о них своим родителям (законным представителям), близким родственникам либо в полицию (номер телефона любой дежурной части), на единый телефон доверия (тел. 8-800-2000-122).

Не перезванивать по номерам телефона, указанным в сообщениях о взломах аккаунтов, не переходить по незнакомым ссылкам из этих сообщений.

Не сообщать свои персональные данные, не предоставлять им доступ к своим страницам, аккаунтам в социальных сетях.

Не производить онлайн оплаты, переводы по просьбам неизвестных.

Не верить сообщениям с неизвестных и известных номеров (сервисов) о выигрышах, способах быстрого заработка крупных сумм, с просьбами о помощи друзьям, родственникам, займе денег,

**ЕСЛИ ВСЁ ЖЕ ПОВЕРИЛ, ПРОШЁЛ ПО ССЫЛКЕ,
ОТВЕТИЛ НА ЗВОНОК, СООБЩИЛ СВЕДЕНИЯ О СЕБЕ**

Не паниковать. Из любой ситуации, которая может казаться очень проблемной, всегда есть выход.

Незамедлительно сообщить об этом своим родителям (законным представителям), близким родственникам либо в полицию (номер телефона любой дежурной части), на единый телефон доверия (тел. 8-800-2000-122).

Заблокировать (поместить в черный список) незнакомые номера, с которых тебе звонили, поступали сообщения.

ГЛАВНОЕ

В любой сомнительной и непонятной ситуации перед совершением действий нужно обязательно посоветоваться со взрослыми знакомыми и близкими тебе людьми, которым ты доверяешь!



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 7bf3de7b0fe97332ed5fa5607caaa443

Владелец: Гридасова Татьяна Алексеевна

Действителен с 17.03.2025 до 10.06.2026