

Основные схемы дистанционного мошенничества и советы по защите от них

1/3

Как действуют мошенники?

Двухкомпонентные атаки с использованием методов социальной инженерии

Если с первой попытки обмануть жертву не удалось, мошенники, представляясь представителями банков или служб поддержки, делают повторный звонок. В этот раз они говорят, что предыдущий запрос поступил от недоброжелателей, а они, как сотрудники госструктур, хотят помочь.

Мошенничество с применением информационно-коммуникационных технологий

Мошенники связываются с жертвами, предварительно узнав о них необходимую информацию, и сообщают, что у абонентов сотовой сети возникли проблемы со связью. Они предлагают «настроить» телефоны для устранения этих проблем. В случае отказа мошенники начинают угрожать блокировкой SIM-карт.

Как противостоять?

1. Никогда не сообщайте смс-коды доступа или пароли третьим лицам.
2. Самостоятельно позвоните во все ведомственные органы, чтобы уточнить информацию, которую вам сообщили ранее (мошенники могут использовать подмену номера).
1. Если у вас есть сомнения, позвоните в свою сотовую компанию самостоятельно.
2. Не поддавайтесь угрозам мошенников. Они стараются вызвать панику, чтобы вы действовали импульсивно и принимали необдуманные решения.



Если вам поступил подозрительный звонок, лучше всего завершить разговор.

Основные схемы дистанционного мошенничества и советы по защите от них

2/3

Как действуют мошенники?

Мошенничество по схеме «фэйк босс» в отношении сотрудников организаций

Мошенник связывается с сотрудником через мессенджер, используя личные данные и фотографию профиля, аналогичные данным профиля руководителя организации, где работает жертва или откуда она недавно уволилась. После установления контакта злоумышленник просит оказать содействие правоохранительным органам в проведении проверки, подчеркивая необходимость конфиденциальности.

Мошенничество в период распродаж через мессенджеры

Злоумышленники создают фальшивые сайты, которые внешне идентичны известным брендам, и предлагают товары с большими скидками. Главная цель — украсть данные банковских карт или собрать оплату за несуществующие товары.

Как противостоять?

- 1 Попробуйте связаться со своим руководителем самостоятельно через другие каналы связи (корпоративная почта или телефон), уточните детали.
- 2 Помните, что сотрудники правоохранительных органов никогда не звонят в мессенджерах, не проводят расследования дистанционно и не обмениваются с юридически значимыми документами в мессенджерах.
- 1 Проверяйте URL-адрес: наведя курсор на ссылку, убедитесь, что адрес не меняется на подозрительный. Будьте внимательны к символам, так как мошенники могут использовать похожие или специальные символы. Также ищите «://» в адресе, так как его отсутствие, например, в «httpsyandex.ru», может указывать на мошеннический сайт.
- 2 Не скачивайте программы из неизвестных источников.
- 3 Следите за актуальностью антивирусного программного обеспечения на своих устройствах.



Если вам поступил подозрительный звонок, лучше всего завершить разговор.

Основные схемы дистанционного мошенничества и советы по защите от них

3/3

Как действуют мошенники?

Распространение фишинговых ссылок в домовых чатах

Мошенники размещают в домовых чатах объявления о бесплатной раздаче бытовой техники или мебели, подкрепляя свои предложения фото и видео для повышения доверия. Накануне встречи они извиняются и утверждают, что товар можно отправить только с курьером, предлагая перейти по ссылке для оформления доставки. Цель злоумышленников – заразить телефон пользователя вредоносным ПО для кражи персональных данных и доступа к платежным средствам.

Получение доступа к аккаунтам приложений с помощью телефонного номера, вновь выпущенного в продажу

Мошенники покупают SIM-карты и с помощью специального программного обеспечения проверяют, имеются ли на телефонных номерах зарегистрированные аккаунты в различных приложениях, включая маркетплейсы, государственные платформы и банковские приложения. Если на номере зарегистрированы аккаунты, мошенники используют их для получения доступа к личным данным.

Как противостоять?

- 1 Будьте особенно внимательны к слишком выгодным предложениям, когда товары предлагаются бесплатно или по цене значительно ниже рыночной.
- 2 Не переходите по подозрительным ссылкам, даже если они пришли от знакомых.
- 3 Если вам предлагают оформить курьерскую доставку и просят сообщить код из смс для ее оформления, немедленно прекратите общение с таким человеком.
- 1 Если вы изменили свой номер телефона, обязательно удалите старый номер из всех сервисов, связанных с вашим мобильным банком, социальными сетями и т. д.
- 2 Если вы уже потеряли доступ к старому номеру и не можете его восстановить, рекомендуем как можно скорее привязать свои учетные записи к новому номеру.
- 3 Включайте историю входов и активностей: следите за активностью на своих аккаунтах.



Если вам поступил подозрительный звонок, лучше всего завершить разговор.