УБК МВД России



Актуальные способы совершения мошеннических действий

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

1. Не отвечайте
   на звонки с незнакомых номеров
2. Прервите разговор
   Если он касается финансовых вопросов
3. Не торопитесь
   принимать решение
4. Проверьте информацию в Интернете
   или обратитесь за помощью к близким родственникам
5. Самостоятельно позвоните
   близкому человеку /в банк / в организацию
6. Не перезванивайте
   по незнакомым номерам
7. Не сообщайте CVV/CVC и иные
   данные банковских карт
8. Внимательно проверьте
   от кого поступают сообщения



Возьмите паузу и спросите совета у родных и друзей!

ФОРМУЛА УСПЕХА ТЕЛЕФОННЫХ МОШЕННИКОВ



эффект неожиданности + яркие эмоции + психологическое давление, паника + актуальная тема

Увы, мы готовы сделать ВСЁ, что просят от нас мошенники

ЭМОЦИИ, КОТОРЫЕ ВЫЗЫВАЕТ ИНФОРМАЦИЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

ПОЛОЖИТЕЛЬНЫЕ

- РАДОСТЬ НАДЕЖДА
- ЖЕЛАНИЕ ПОЛУЧИТЬ ДЕНЬГИ

ОТРИЦАТЕЛЬНЫЕ

- СТРАХ ПАНИКА
- ЧУВСТВО СТЫДА



«Вы выиграли крупную сумму денег»
«Вам положены социальные выплаты»
«Пенсионный фонд рад сообщить вам о перерасчете вашей пенсии, вам положена выплата в размере…»

«С вашего счета списали все деньги»
«Ваш родственник попал в аварию и сбил человека»
«Вас беспокоит следователь Следственного комитета, вы участник уголовного дела о… коррупции или…»

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ – ЗЛО

Телефон — основной инструмент мошенников. Большая часть хищений происходит с помощью социальной инженерии



1. Обман или злоупотребление доверием
2. Психологическое давление
3. Манипулирование

Под влиянием социальной инженерии жертва добровольно расстается с деньгами или раскрывает личные и финансовые данные, которые нужны злоумышленникам для кражи средств

Инструментарий мошеннического КЦ



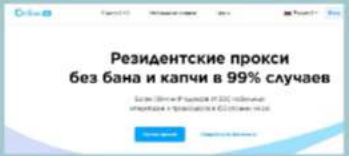
Прокси в РФ, VPN от vip72.com



VoIP звонки через МТС Коннект



VoIP звонки eMotion от Мегафона



Прокси в РФ, виртуальные номера телефонов от OnlineSim.io



SIP телефония от Narayana (Эстония)



SIP телефония + подмена номера от Gargona Telecom

Подписка на ТГ бот «Глаз Бога» («пробив» по номеру телефона)

+ покупка номеров с балансом операторов РФ и номеров для WhatsApp

Геолокация мошеннических КЦ



Данные ПАО Сбербанк

Установлено местоположение:

- Администратор управляющего CRM – г. Запорожье;
- 3 CRM – г. Запорожье;
- 5 CRM – г. Днепр, проспект Дмитрия Яворницкого;
- 3 CRM – г. Одесса, Люстдорфская дорога;
- 3 CRM – г. Одесса, Высокий переулок;
- 2 CRM – г. Киев;
- 1 CRM – г. Чернигов;
- 1 CRM – г. Черновцы;
- 1 CRM – г. Луцк;
- 1 CRM – г. Львов;

Варианты использования фейковой учётной записи Telegram



«Злоумышленник под видом другой учётной записи»

Иван Сергеевич, здравствуйте. Как ваше здоровье? Как работа? Я пишу вам по делу. Хочу вас предупредить, что сегодня Вам будет звонить Нестеров Алексей Александрович, который курирует наше учреждение.
У него есть к вам несколько вопросов. Звонок очень важный, обязательно пообщайтесь!

Создание фейковой учётной записи, не имеющей отношение к пользователю. Ведение переписки от имени другого лица.

Захват учётной записи мессенджера

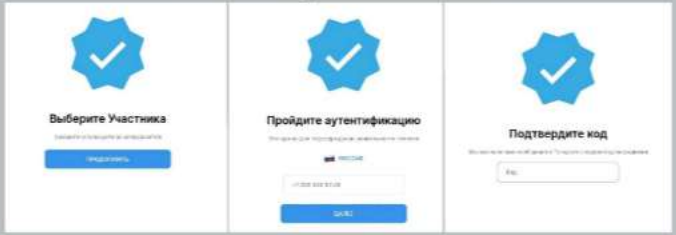


«Злоумышленник с учётной записи друга/знакомого»

Проголосуй за меня пожалуйста, если не сложно конечно) https://goo.su/CTcZ34nN

ссылка, отправляемая злоумышленниками, сделана при помощи сервиса для сокращения ссылок. Этот инструмент часто применяется, когда отправитель не хочет, чтобы реальный адрес сайта бросался в глаза.

Сайт злоумышленников



Указав номер телефона, вы тут же получите код подтверждения, с помощью которого у вас угонят учётную запись

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК ЦЕНТРОБАНКА (БАНКА РОССИИ)»

«По вашей карте зафиксирована сомнительная операция. Для сохранности денег вам нужно перевести их на «безопасный» («специальный») счет в Центробанке»



«ПРЕДСТАВИТЕЛЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ (МВД, ФСБ, СК РФ)»

«Следователь Следственного комитета.
Вы являетесь свидетелем по уголовному делу»

«Иванов В.В., капитан полиции. По вашему паспорту оформлен кредит и указана ваша карта. Нам необходимо уточнить ее реквизиты»

ТЕЛЕФОННЫЕ МОШЕННИКИ: РАСПРОСТРАНЕННЫЕ СХЕМЫ



«ЛЖЕСОТРУДНИК БАНКА»

«С вашей карты пытаются перевести деньги»

«Ваша карта (счет) заблокирована»

«По карте зафиксирована подозрительная операция»



«ДРУГ, РОДСТВЕННИК»

«Ваш сын попал в аварию, ему срочно требуется дорогостоящее лекарство»

«Ваш сын только что в результате ДТП сбил человека. Я готов помочь избежать наказания»

Варианты использования захваченной учётной записи мессенджера



«Злоумышленник под видом НО организации»

Добрый день. Это Станислав Викторович начальник вашего отдела.
С вами не может связаться наш генеральный директор Андрей Валерьевич
и просит ему перезвонить. (сообщает номер)

Злоумышленник используя чужую учетную запись указывает в ней анкетные данные действующего руководителя организации и от его имени связывается с сотрудниками данной организации и злоупотребляя их доверием переводит на диалог с подельниками.



«Злоумышленник под видом ГД организации»

Добрый день! Это Андрей Валерьевич! Наш разговор носит строго конфиденциальный характер, разглашение сведений несет за собой уголовную ответственность и будет расценено как содействие СБУ. В руки СБУ попали личные данные более 2500 сотрудников нашей организации, в том числе доступы к банковским счетам, и ваша кандидатура избрана для оказания содействия в их поиске. В настоящий момент злоумышленники оформляют кредиты на сотрудников нашей организации и все имеющиеся средства выводят предположительно в поддержку ВСУ. Для начала, чтобы пресечь попытку списания ваших денежных средств, вам необходимо исчерпать свой кредитный лимит и все имеющиеся на расчетных счетах денежные средства перевести на резервный счет, который я вам сообщу.

Как только жертва связывается с подставным генеральным директором, злоумышленник всеми возможными способами пытается завладеть денежными средствами жертвы.


Возникли сомнения?
Прерви разговор!
Звони в 112!
Подписывайся чтобы быть в курсе
и не попасть на уловки мошенников
@CYBERPOLICE_RUS
УБК МВД России