Руководителям ОО, Ланге С.Н. для учёта в работе и доведения инф-ции до всех заинтересов-ных. 16.05.2022

МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, СВЯЗИ И ЦИФРОВОГО РАЗВИТИЯ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Ул. Сони Кривой, д. 75а, Челябинск, 454080, Россия
телефон/факс: (351) 232-33-53, E-mail: info@mininform74.ru
ОГРН 1107451016860, ИНН/КПП 7451310939/745301001, ОКПО 68647084

25.04.2022 № 1601/2090

на №________ от________

Главам городских округов
и муниципальных районов
Челябинской области

Во исполнение пп. 1.1. п. 1. Решения оперативного штаба по обеспечению кибербезопасности Челябинской области от 13.04.2022 (далее – Решение) направляю информацию об использовании методов социальной инженерии и рекомендаций по обеспечению информационной безопасности. Прошу довести до сотрудников и подведомственных организаций данную информацию в соответствии с п. 2.1. Решения.

Кроме того направляю Памятку о способах совершения правонарушений в сфере информационно-телекоммуникационных технологий и необходимых мерах безопасности. Прошу рассмотреть возможность и варианты доведения до жителей Челябинской области данной информации.

Приложения в электронном виде.

Министр

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 401934663362754782369175994820715608133313823076
Владелец: Фетисов Игорь Борисович
Действителен с 19.04.2021 по 19.07.2022

И.Б. Фетисов

Перминова Евгения Игоревна
(351) 232-08-61

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ
Вход N 05-01-31/703
«26» 04 2022
Кол-во листов 1+15

ГОРОДСКОГО ОКРУГА
Вход. № 0102-09/1655
26.04 2022
1+15

Памятка о способах социальной инженерии и необходимых мерах безопасности

Социальная инженерия или «атака на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить доступ к конфиденциальной информации.

Киберпреступники все чаще используют методы социальной инженерии для проникновения в инфраструктуру организации при целевой атаке. Согласно статистике, количество атак с использованием социальной инженерии в 2021 году выросло на 216%. Злоумышленники, предпринимая попытки найти доступ к системе или ценным данным, используют самое уязвимое звено — человека. Простой пример — телефонный звонок, где преступник выдаёт себя за кого-то другого, пытаясь узнать у абонента конфиденциальную информацию, играя на чувствах человека, обманывая или шантажируя его. К сожалению, многие продолжают попадаться на такие ловушки и доверчиво рассказывают социальным хакерам всё, что им нужно.

Человеческий фактор по-прежнему остается слабым звеном в любой системе защиты, поэтому сегодня как никогда возрастает потребность в обучении сотрудников основам информационной безопасности.

Также стоит отметить, что на текущий момент социальная инженерия установила прочную связь с киберпреступностью,

Рассмотрим самые популярные методы социальной инженерии

Так называемая «Атака на человека» может производиться по многим сценариям, но существует несколько наиболее распространённых техник работы злоумышленников.

Фишинг

Основной упор на невнимательность.

Метод сбора пользовательских данных для авторизации — обычно это массовые рассылки спама по электронной почте. В классическом сценарии на почту жертвы приходит поддельное письмо от какой-то известной организации с просьбой перейти по ссылке и авторизоваться (ввод комбинации логин/пароль). Чтобы вызвать больше доверия, мошенники придумывают серьёзные причины для перехода по ссылке: например, просят потенциальную жертву обновить пароль или ввести различного рода персональную информацию (ФИО, номер телефона, должность и т.д.).

Троян

Основной упор на невнимательность, доверие.

Вирус не зря получил своё название по принципу работы троянского коня из древнегреческого мифа. Только приманкой здесь становится email-

сообщение, которое при классическом сценарии мошенников обещает быструю прибыль, выигрыш или другие «золотые горы» — но в результате человек получает вирус, с помощью которого злоумышленники крадут его данные. Данный вид атаки тоже необходимо относить к методам социальной инженерии, потому что создатели вируса как правило хорошо знают, как замаскировать вредоносную программу, чтобы вы наверняка кликнули по нужной ссылке, скачали и запустили файл.

Часто сотрудники непреднамеренно помогают злоумышленнику в развитии атаки, пересылая зараженное письмо коллегам с просьбой открыть вложение или перейти по ссылке. Например, в теле письма используются формулировки из повседневной служебной деятельности. «Уважаемые начальники подразделений, направляем график отпусков на текущий год. Просим довести до сотрудников и т.д. С уважением, отдел кадров». При положительном для злоумышленников развитии событий письмо пересылается по организации. В свою очередь сотрудник, получивший письмо уже от своего коллеги абсолютно не подозревает о наличии ссылок на вредоносное ПО.

Как только злоумышленник убедился, что сотрудник принял его за коллегу или какое-то доверенное лицо, распространил письмо по организации, в ходе дальнейшей переписки он может попытаться получить нужную ему информацию, не вызывая подозрений. Так можно узнать версию используемого ПО, наличие антивируса на рабочем компьютере, электронную почту других сотрудников, номера мобильных телефонов, структуру компании. Все это представляет ценность и может использоваться при планировании и проведении последующих социотехнических атак.

Злоумышленники часто опираются на страх, жадность, надежды, ожидания и другие эмоции, которые могут заставить пользователя поддаться сиюминутной слабости. Когда внезапно на почту приходит письмо «список сотрудников на увольнение» — пользователь забывает об элементарных правилах техники кибербезопасности, он даже не задумывается, почему ему вообще пришло подобное письмо.

Часто бывает так, что именно тема письма побуждает сотрудника открыть его, перейти по ссылке, скачать и запустить файл, не разбираясь — кто адресат и почему домен отправителя написан как-то странно.

Если недостаточно внимательно отнестись к прочтению такого письма, то подвох заметить непросто.

Предсказуемо страх увольнения или сокращения — достаточно мощный фактор, чтобы забыть о правилах информационной безопасности: письма с такой темой в большинстве случаев побуждали пользователей совершить потенциально опасное действие. Высокий процент успеха показывают письма, где есть слова «премия», «поощрение», «повышение зарплаты»:

Злоумышленник может также попытаться привязать тему рассылки к какому-то знаменательному событию (если располагает, например, сведениями о недавно прошедшем в компании корпоративе), профессиональным и государственным праздникам.

Дорожное яблоко

Основной упор на доверчивость, любопытство

Представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того, чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

Услуга за услугу

Основной упор на доверчивость

Используя этот метод, злоумышленник представляется сотрудником службы технической поддержки и спрашивает о наличии сбоев в работе программного обеспечения, предлагает исправить возникшие неполадки в системе либо предупредить о вероятности их наступления, хотя на самом деле проблем в работе ПО не возникало. Жертва верит в наличие неисправностей и, выполняя указания хакера, лично передаёт ему доступ к важной информации.

Распространенный сценарий, когда пользователь сам говорит об отсутствии времени и сообщает необходимые пароли для того, чтобы сотрудник технической поддержки самостоятельно провел необходимые манипуляции.

Обратная социальная инженерия

Основной упор на доверчивость, невнимательность

Методика направлена на то, чтобы жертва сама обратилась к социальному инженеру и выдала ему необходимые сведения. Это может достигаться несколькими путями:

Внедрение особого ПО

Основной упор на невнимательность

На электронную почту поступает письмо, информирующее о возможных сбоях в работе часто используемого программного обеспечения (например, пакет офисных программ). В этом же письме указаны контактные данные

специалиста технической поддержки, используемые злоумышленником. При возникновении сбоя в работе вышеперечисленного ПО, пользователь вспоминает о ранее поступившем предупреждении и связывается со злоумышленником в лице технического специалиста.

Таким образом, ситуация заранее подстроена, пользователь связывается с социальным хакером. Налаживая работу ПО, производятся необходимые для взлома манипуляции. А когда взлом обнаруживается, социальный инженер остаётся вне подозрения (поскольку создается впечатления, что он помогал вам).

ЗАКЛЮЧЕНИЕ

С учетом изложенного, самые распространенные сценарии вышеуказанных атак реализуются путем email-рассылок.

Причиной тому относительная дешевизна и простота таких методов, а также высокая эффективность.

На текущий момент целевой вектор подобных атак значительно сместился от получения доступа к информации к её уничтожению (блокированию) путем применения вирусов-шифровальщиков.

Для рядовых пользователей самый актуальный и действенный совет — всегда оставаться бдительными, проверять информацию об отправителе, прежде чем перейти по ссылке или скачать предлагаемый файл — убедиться, что это не вредоносный ресурс. Полученные файлы перед открытием необходимо проверить с помощью антивирусного ПО. Стоит также удостовериться, что домен отправителя легитимный и реальный. В случае возникновения сомнений, рекомендуется проверить, действительно ли адресат отправлял данное письмо и является ли он настоящим владельцем домена и (или) электронного ящика, связавшись с ним каким-то альтернативным способом, например, через мессенджер или по телефону.

Своевременное выявление и пресечение атаки позволит избежать серьезных последствий.

Что касается организационных мер, то основой является систематическое повышение осведомленности сотрудников в области информационной безопасности.

Исследование компаний в области ИБ показывают, что 38% организаций вообще не проводят тренинги для сотрудников по вопросам ИБ, а 37% делают это формально, без какой-либо проверки эффективности. Хотя проводить периодическое обучение с контролем информированности каждого сотрудника крайне важно. При этом процесс повышения осведомленности должен в первую очередь быть направлен на практическую сторону обеспечения

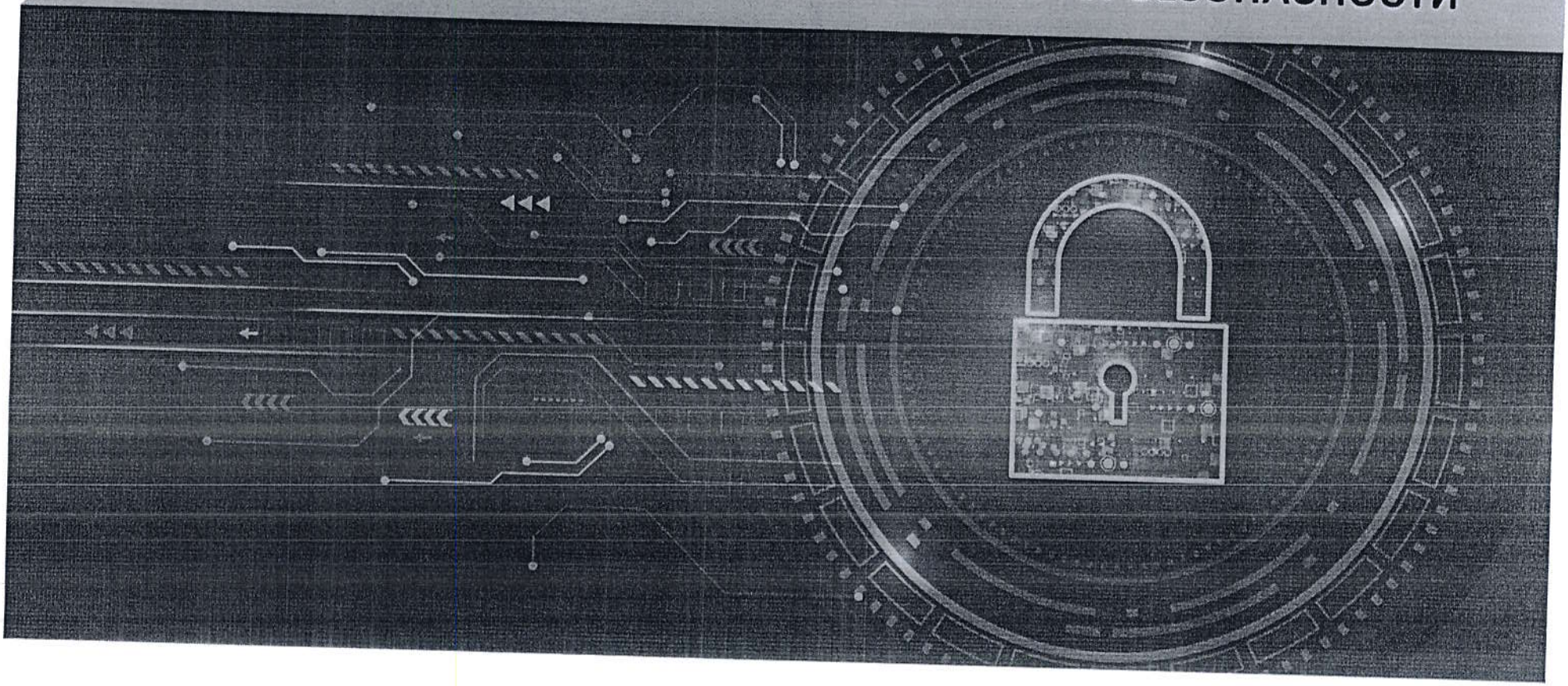
безопасности, а каждый сотрудник должен понимать свои обязанности и ответственность за обеспечение ИБ.

Отличная практика, когда сотрудники оповещают подразделения ИБ о том, что им пришло сомнительное письмо, особенно если заметно, что над рассылкой тщательно поработали. В таком случае, даже если заражение или утечка имели место, еще можно успеть оперативно отреагировать на атаку и принять контрмеры.

Основные меры по защите от вышеперечисленных видов социальных атак.

- **Сохраняйте бдительность**. Всегда обращайте внимание на отправителя писем и адрес сайта, где собираетесь ввести какие-то личные данные. Если это почта на домене крупной организации, удостоверьтесь, что домен именно такой и в нём нет опечаток. Если есть сомнения — свяжитесь с техподдержкой или представителем организации по официальным каналам.
- **Используйте только доверенные носители информации**.
- **Не переходите на подозрительные сайты и не скачивайте сомнительные файлы**, один из самых лучших помощников социальной инженерии — любопытство.
- **Не используйте один и тот же пароль** для доступа к личным и корпоративным (рабочим) ресурсам.
- **Использование антивирусного программного обеспечения**. Недопущение его отключения.
- **Систематический инструктаж**. Все сотрудники должны быть проинструктированы о том, как вести себя при обнаружении попыток или осуществления незаконного проникновения.

ПАМЯТКА О СПОСОБАХ СОВЕРШЕНИЯ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И НЕОБХОДИМЫХ МЕРАХ БЕЗОПАСНОСТИ



СТАТИСТИКА СОВЕРШЕНИЯ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИКТ С НАЧАЛА ПРОВЕДЕНИЯ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

в 10 раз

сократилось число телефонных атак мошенников

212 - 67,28%

преступлений совершено путем звонка потерпевшему от имени сотрудника банка

- динамика по сравнению с 2021 г.

1401 - 17,25%

зарегистрированных имущественных преступлений совершены с использованием ИКТ

Данные ГУ МВД России по Челябинской области, 2022 г.

925 — Мошенничество — - 3,24%

476 — Хищение средств с банковского счета — - 35,41%

+ 900%

реклама с предложением инвестировать в акции Газпрома

+ 4,07%

число звонков от имени полиции о родственнике, попавшем в беду

+ 566,67%

недостоверная информация о совместной поездке на blablacar

НОВЫЕ СООБЩЕНИЯ МОШЕННИКОВ

1

Перевод денег на безопасный счет потому что:
- банк под санкциями
- отключение банков от системы SWIFT

2

Требования немедленно погасить несуществующий кредит от лица одного из крупнейших российских банков

3

Предложения от лжеброкеров по инвестиционным инструментам или имитация рекламы известных российских инвестиционных и финансовых компаний

4

Тезисы о поддержке украинской армии и призывы к протестной активности среди матерей российских солдатов-срочников

5

Ссылки на зараженные сайты российских компаний с сообщениями о якобы полученных начислениях или выигрыше ценных призов

РАССЫЛКА ПИСЕМ И СООБЩЕНИЙ ОТ ИМЕНИ ОРГАНОВ ВЛАСТИ

КАК ОРГАНИЗОВАНО

Приходит сообщение на эл. почту или в соцсетях от лица российских органов власти:

- предупреждение о незаконности использования запрещенных в России
- веб-сайтов, соцсетей, мессенджеров и VPN-сервисов;
- информация о новых соцвыплатах

Приложение к письму: файл RTF

КАК НА САМОМ ДЕЛЕ

- При открытии документа скачивается вредоносный файл
- Активируется скрипт, с помощью которого мошенник получает удаленный доступ к данным вашего устройства
- Мошенник переводит денежные средства с банковских счетов или копирует персональную информацию

КАК ПОСТУПИТЬ

Не торопитесь!
Не открывайте файлы и не переходите по ссылкам, особенно в случае призыва к срочным действиям

Проверьте файлы активирусом
Все сомнительные файлы проверяйте антивирусными программами или на сервисах (пример opentip.kaspersky.com)

Проверьте адрес сайта
Проверьте написание адресов сайтов, прежде чем переходить по ним и вводить на них данные

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

КАК ОРГАНИЗОВАНО

- **Приходит сообщение или звонок** о том, что банковская карта заблокирована либо идет попытка перевода денежных средств
- **Предлагается совместно с банком уточнить детали**, чтобы предотвратить блокировку карты или перевод средств.
- **Мошенники по телефону просят сообщить номер карты/счета, cvc-код с оборота карты**, сумму средств на счете, код из смс

КАК НА САМОМ ДЕЛЕ

После сообщения номера карты или счета, cvc-кода или кода из смс злоумышленники снимут деньги с вашего счета

КАК ПОСТУПИТЬ

Не торопитесь!
Не сообщайте реквизиты вашей карты (никто не вправе требовать данные карты)

Проверьте информацию
Чтобы проверить информацию о блокировании или списании с карты, позвоните в службу поддержки банка

Номер телефона службы поддержки банка указан на обороте карты, мобильном приложении или официальном сайте

ОПЛАТА В ПОДДЕЛЬНОМ ИНТЕРНЕТ-МАГАЗИНЕ

КАК ОРГАНИЗОВАНО

- Злоумышленники создают фальшивый интернет-магазин
- Пользователей привлекают на сайт низкие цены, дефицитные товары и услуги
- Человек оформляет заказ

Спойлер: но не получит желаемый товар или услугу

КАК НА САМОМ ДЕЛЕ

- Поддельные сайты копируют дизайн оригинального сайта и агрессивно продвигаются на онлайн-сервисах
- Человек вводит данные банковской карты
- Информация попадает злоумышленникам
- Деньги будут украдены

КАК ПОСТУПИТЬ

Совершайте покупки только в проверенных интернет-магазинах

Будьте внимательны при оплате
Проверяйте, чтобы окно ввода данных карты было открыто в защищенном режиме

На защищенный режим указывают замок в адресной строке, https в адресе

ОБМАН ПО ТЕЛЕФОНУ: ТРЕБОВАНИЕ ВЫКУПА

КАК ОРГАНИЗОВАНО

- Поступает звонок с незнакомого номера
- Мошенник представляется знакомым, сообщает, что задержан полицией и обвинён в преступлении
- В разговор вступает якобы сотрудник полиции. Сообщает, для решения вопроса нужна не раз помогал людям. Для решения вопроса нужна определенная сумма денег

КАК НА САМОМ ДЕЛЕ

- В организации обмана участвуют несколько преступников.
- Ваш номер набран наугад, фраза мошенника - заготовлена, его действия – по обстоятельствам
- Если жертва поддалась на обман ей называют адрес, куда приехать, или счет для перевода денег. Запугивают до получения денег

КАК ПОСТУПИТЬ

Прервите разговор

Позвоните тому, в ком идет речь
Если телефон отключён - свяжитесь с его коллегами, друзьями, уточните информацию

Незнакомец требует деньги – мошенник

Задайте уточняющие вопросы «знакомому»
Примеры вопросов: Как я выгляжу? Когда мы виделись последний раз?

Уточните у полицейского номер отделения.
После наберите «02», узнайте у дежурного, действительно ли ваш родственник задержан

SMS-ПРОСЬБА О ПОМОЩИ

КАК ОРГАНИЗОВАНО

Абонент получает смс: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам»

Нередко добавляется обращение «мама», «друг» или другие

КАК НА САМОМ ДЕЛЕ

В роли вымышленного друга или родственника выступает мошенник

В зоне особого риска: пожилые или слишком юные владельцы телефонов

КАК ПОСТУПИТЬ

Проинформируйте близких
Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники

ТЕЛЕФОННЫЙ НОМЕР-ГРАБИТЕЛЬ

КАК ОРГАНИЗОВАНО

- Приходит SMS с просьбой перезвонить на указанный номер телефона
- Просьба обоснована разными причинами – помощь другу, изменение тарифов связи, проблемы со связью и др.
- После того, как вы перезваниваете, вас долго держат на линии. Когда это надоедает, вы отключаетесь. Со счёта списываются крупные суммы

КАК НА САМОМ ДЕЛЕ

- Существуют сервисы с платным звонком. Например, для развлечений. Плата взимается дополнительно за сам звонок
- Мошенники регистрируют сервис и распространяют номер без предупреждения о снятии платы за звонок

КАК ПОСТУПИТЬ

Не звоните по незнакомым номерам
Это единственный способ обезопасить себя от телефонных мошенников

ТЕЛЕФОННЫЕ ВИРУСЫ

КАК ОРГАНИЗОВАНО

- В смс или в соцсетях приходит сообщение: «Вам направлена информация. Для получения пройдите по ссылке...»
- При переходе по адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета
- С вашего номера рассылаются подобные сообщения по адресной книге

КАК ПОСТУПИТЬ

Не переходите по незнакомым ссылкам
Не переходите по ссылкам даже, если номер знакомый (его могли взломать)

Пользуйтесь официальными источниками
Для скачивания приложений используйте только официальные источники

Проверьте настройки приложений в телефоне
Не давайте лишних разрешений приложениям в настройках телефона

ВЫИГРЫШ В ЛОТЕРЕЕ

КАК ОРГАНИЗОВАНО

- На телефон приходит сообщение или звонок от якобы ведущего популярной радиостанции
- Ведущий поздравляет вас с крупным выигрышем в лотерее (телефон, ноутбук , автомобиль и др.)
- Чтобы получить приз просят представиться, назвать год рождения, данные карты и просят сообщить код из смс для подтверждения выигрыша

КАК НА САМОМ ДЕЛЕ

Полученной информации о ФИО, банковской карте достаточно, чтобы мошенники списали деньги с вашего счета.

Код из смс-сообщения нужен для подтверждения списания денежных средств

КАК ПОСТУПИТЬ

Прекратите общение

Игнорируйте сообщения с такой тематикой