ГОСУСЛУГИ

Мошенник звонит от компании **вашего сотового оператора**, узнать это не составит труда (10 сек.), а узнать как вас зовут - по слитым базам доступны за небольшую оплату есть все данные включая ваш паспорт, предлагают все что угодно, улучшить условия тарифа, сменить тариф, предложить новый тариф, подтвердить персональные данные, указанные при подключении, сменить сим-карту, все что угодно, связанное с компанией оператором и т.д.….

Введя в заблуждение, предлагают сообщить пароль из СМС, и как не странно пароль приходит из СМС-сервиса «gosuslugi»!!!!!!!. В этот момент злоумышленник, просто находясь хоть на луне, вводит для доступа ВАШ телефон, а пароль ему нужен для восстановления доступа к госуслугам. После чего, приходит второй, уже 6-значный пароль, из того же СМС-сервиса «gosuslugi»!!!!!!!, сообщив его, мошенник включает вторичную защиту, чтобы вы не смогли восстановить доступ самостоятельно! Придется уже идти в МФЦ. А пока вы ходите в МФЦ, мошенники могут оформить на ВАС сим-карты, поставить на миграционный учет людей, оформить в НЕ очень известных банках (которым ой как очень нужны клиенты) банковские карты и счета, получить все необходимые выписки на ВАС, воспользоваться Вашим аккаунтом для подтверждения ВАШЕЙ личности при оформлении микрозаймов, открыть ООО-шку и многое другое!!

Как обезопасить: просто не ведитесь на такие звонки!!! А если сомневаетесь, позвоните в МТС-Билайн-Мегафон-Теле2 и т.д. завершив первоначальный звонок.

ВЗЛОМ - «Whatsapp» и «Telegram», проголосуй и займи!

Мошенник с **ранее уже взломанного аккаунта** «Whatsapp» и «Telegram», от имени Вашего друга, знакомого, коллеги по работе, присылают подготовленную ссылку, которая может быть одноразовой, В ОСНОВНОМ С ПРОСЬБОЙ ПРОГОЛОСОВАТЬ за дочь, сына, отца и святого духа) да хоть за кота сфотографированного спящим под забором, перейдя по которой вы попадаете на заранее подготовленный сайт, который как правило выглядит одной страницей, там вы находите кнопку, где написано проголосовать за этого кота), после чего у вас появляется окно с авторизацией с помощью «Whatsapp» или «Telegram», ЗНАЙТЕ, это окно авторизации ВАШЕГО аккаунта «Whatsapp» или «Telegram» через приложение, установленное на компьютере у злоумышленника! После чего, введя свой телефон, у вас появляется 6-значный уникальный код, который якобы нужно ввести в этом же окне! ВОТ И ВСЕ - Мошенник вводит у себя ваш телефон, после чего от Вас получает этот код и авторизовывается у себя на компьютере, находясь к примеру в Удмуртии. **После чего вы уже становитесь взломанным аккаунтом**. И уже от ВАШЕГО имени, т.к. злоумышленник видит вашу переписку абсолютно !!! полностью всю, начинает писать тем, с кем вы общались, коллегам, друзьям, родственникам, знакомым, с просьбой занять денег, возможно даже для достоверности в Фотошопе нарисуют Ваши имя и фамилию на банковской карте и ее скинут для перевода. И это минимальное!!, что могут с ВАМИ сделать… Хуже всего, если вдруг кто-то обменивался какими-нибудь конфиденциальными или компрометирующими материалами. У мошенников возникнет хороший повод для шантажа. Самое обидное,

что голод безразмерен, они все равно распространят ваши данные!!! Даже дойдя до сумм в сотни тысяч рублей.

Как обезопасить: ПРОСТО ПЕРЕЗВОНИТЕ человеку, от кого поступило сообщение с просьбой проголосовать, занять и т.д. Узнайте, так ли это… НИКОГДА, не сохраняйте в переписке конфиденциальные или компрометирующие материалы. СОВЕТ, лучше вообще ничего не отправляйте, т.к. даже если их удалите в переписке, как правило в 90% случаев у всех в настройках включено резервное копирование (лучше его отключить… да вы не сможете восстановить переписку если утопили телефон, продали его и купили новый, зато будете в безопасности).

Самое главное, установите двухэтапную защиту (аутентификацию) для каждого мессенджера. Они находятся в настройках. Придумайте пароль, используя ЗАГЛАВНЫЕ и *строчные буквы*, используйте цифровые символы, и по возможности иные символы и запомните, а лучше запишите его куда-нибудь. Без этого пароля, никто не сможет подключиться к вашему аккаунту в обоих мессенджерах, даже если вы всетаки передали коды, и вовремя опомнились. Также, при установке данной защиты, НЕ указывайте свою электронную почту, ее как ни странно тоже легко ломают!! ВАЖНО, если вы передали коды и пароль от дфухэтапной аутентификации, пишите письма!, доступ будет потерян навсегда, и его не восстановить!

Сообщения в мессенджере от руководителя, друга, знакомого и т.д. с просьбой оказать содействие сотрудникам ФСБ, и прочей безопасности..

Мошенник входит на сайт организации, а также страницу в социальных сетях «Вконтакте», «Одноклассники» в которой вы работаете, ознакамливается с ней, просматривая посты о том, что наихудший работник тысячелетия «Петров Петр Петрович», фото как «Сидорова Сидора Сидоровича» награждают похлопыванием по плечу, о том как все рады новому коттеджу руководителя «Иванова Ивана Ивановича» (информация утрирована))) путем несложных мысленных, логических манипуляций понимает, где руководитель «Иванов Иван Иванович», а где заместитель по непонятным вопросам «Сидоров Сидор Сидорович», и где простой работник «Петров Петр Петрович». Создает защищенный аккаунт в мессенджере, как правило «Telegram», дает ему имя «Иванов Иван Иванович», и вставляет полученное из общего доступа его улыбающееся фото, с которого начинает ВАМ писать. В сообщении как правило псевдо-Иванов просит сохранить анонимность переписки, в последующем утверждает Сидорову и Петрову, что им необходимо принять участие в безопасности организации, и что с ними свяжутся в последующем сотрудники различной безопасности (как правило сотрудники силовых структур). Последующие «сотрудники», под угрозой применения зачастую несоответствующих статей УК РФ, угрожая ответственностью за конфиденциальность общения, начинают утверждать, что Сидоров и Петров либо сливают различные данные в страны, с которыми в настоящий момент у нас натянутые международные отношения, либо что на имя Сидорова и Петрова пытаются взять кредит, и деньги отправить вновь этим же странам и т.д. и сообщают банки, где происходят данные операции. В последующем Сидорову и Петрову необходимо участие в поимке мошенников, которые работают в

банках. Для это необходимо якобы переоформить кредиты на себя, а деньги поместить в безопасные ячейки! А кредиты спишут. ВОТ И ВСЕ, деньги ушли. Так будет продолжаться, пока ВАС в 17-м по счету банке, каком-нибудь ООО «Банк памяти отсутствия урожая» не выдадут последний кредит. Когда ВЫ поймете, что ВАС обманули, ВАШ долг перед всеми банками уже будет составлять 65416843135465132465132643513213 4 рублей. И никакие кредиты не спишут! И сотрудник безопасности с псевдо-Ивановым- обманщики.

Как обезопасить: ПРОСТО ПЕРЕЗВОНИТЕ человеку, от кого поступило сообщение. Просмотрите аккаунт Иванова в мессенджере, ВЫ удивитесь, что их два – реальный и подложный.

СОВЕТ: Если вы всё-таки не уверены в себе, что можете противостоять в данной ситуации, в различных банках, которыми вы пользуетесь, есть возможность оформить страхование от мошеннических действий, ДА это стоит деньги, в большинстве случаев это помогает вернуть деньги. Звонок в банк, о том, что вы только что перевели деньги на карту определенного банка Вас не спасет. Банк не остановит эту операцию и не вернет деньги.

Безопасная сделка АВИТО и ЮЛА

Мошенник, создав, или же приобретя доступ к чьему-либо ранее взломанному аккаунту, торговой площадки «Авито» или «Юла», размещает объявление о продаже к примеру «Топора из дамасской стали». Вы в свою очередь, как обычный гражданин, работающий к примеру на вахте «Политехнического общежития», час назад разогнавшего пьяную толпу в комнате «12», находясь в состоянии «Брюса Ли» неожиданно задумались на сутках о приобретении в личное пользование «Топора из дамасской стали»). Решили на торговой платформе списаться с продавцом. Тот в свою очередь, якобы находясь в другом городе, предлагает оформить с Вами «Безопасную сделку». И скидывает скриншот, о правилах безопасной сделки. Там указано, что на ВАШЕЙ банковской карте должна находиться эквивалентная покупке сумма. Затем скидывает заранее подготовленную и зашифрованную ссылку, перейдя к которой, Вам необходимо внести реквизиты своей карты, в дальнейшем СМС – сообщение от вашего банка. И деньги спишутся. Но товар никакой не получите. А владелец объявления странным образом перестанет выходить на связь, или же просто заблокирует свой аккаунт.

Аналогично данной ситуации, мошенники пишут ВАМ, по ВАШЕМУ объявлению, только уже со стороны якобы покупателей, и предлагают также оформить «безопасную сделку». Соглашаясь с ним, вы также получаете ссылку для ввода реквизитов карты, якобы для зачисления его денежных средств ВАМ. Но по результату, денежные средства списывают у ВАС. Вы в свою очередь сообщаете ему свое недовольство. Мошенник же, утверждая, что произошла ошибка, вновь уговаривает ВАМ пройти по ссылке и внести карту. Но странным образом деньги вновь списывают у ВАС. И так будет происходить, пока не поймете, что ВАС обманывают.

Как обезопаситься: не переходите ни по каким ссылкам в ходе общения. В действительности, торговым платформам абсолютно без разницы, сколько у вас денег на карте. Если ВЫ покупатель, то Ваши денежные средства до момента

получения действительно спишут изначально, но совершенно иным способом. Деньги будут зарезервированы на торговой площадке. И только тогда, когда покупатель подтвердит получение товара, их спишут. Если вы продавец, то после совершения безопасной сделки, деньги должны поступить к ВАМ на карту, а не списываться у ВАС!!!. А лучше, приостановите общение, и зайдите на официальный сайт площадки, и ознакомьтесь с правилами безопасной сделки.

ВАШ Ребенок поиграл в игры, а деньги списали у вас.

Довольно простая ситуация, ребенок играет в игры на смартфоне, не важно, Вашем или нет. Любой ребенок – игроман, интересуется способами «упрощенного» прохождения игры. Способами ввода секретных кодов в игре, позволяющих «облегчение» игрового процесса. Для этого ребенок подписывается на блогеров, на различных видео-сервисах (Yuotube, Rutube, и т.д.). В т.ч. подписывается на различные каналы в мессенджерах (Viber, Telegram, Discord и т.д.) где после своей активности, в личных чатах получает сообщения, о различном выигрыше, бонусах, о способах легкого получения внутриигровой валюты и т.д. Ребенку сообщают, что одним из способов получить бонусы и выигрыши - получить их на карту. В дальнейшем под руководством, ребенок входит в приложение банка, как правило в Ваше отсутствие, и осуществляет операции, нажимая различные кнопки под диктовку, пока банк не заблокирует Вам все счета.

Как обезопасить: смените пароль от своего мобильного банка, чтобы его не знал ребенок. Установите лимиты по картам в банках, если эти карты находятся у ребенка. Ну и главное, общайтесь со своими детьми чаще, знайте что они делают и во что играют и с кем общаются. Это не запрещено.

ГЛАВНОЕ - Как обезопасить свои личные данные?

Запомните одну простую истину, какие-либо средства программно-технической безопасности не дают ВАМ 107% гарантию защищенности. В 99% процентах, совершаемых преступлений, присутствует человеческий и социальный фактор.

Во первых, никто не хочет терять свои денежные средства, на этом и делается упор при звонках мошенниками. Соблюдайте холодность мышления при таких звонках. Звонок - «Пытаются украсть деньги», завершите звонок, проверьте через горячую линию банка и не поддавайтесь волнению. Даже если Вам скажут в каком банке и назовут имя и фамилию, в т.ч. даже сколько денег на карте. Не передавайте никому какие-либо коды. Сотрудники банка, в телефонном режиме никогда не просят этого.

Во вторых, при совершении сделок, не поддавайтесь заманчивым предложениям о продаже «Заведомо удешевленного» товара, ознакомьтесь с правилами торговой площадки.

В третьих, не переходите ни по каким ссылкам, более того, отключите в настройках смартфона, автооткрытие ссылок. Достаточно будет в таком случае получить СМС – сообщение с ссылкой, которую смартфон просто откроет сам, в результате чего, на первый взгляд безобидная ссылка установит на ВАШ смартфон вредоносное программное обеспечение, предоставившее удаленный доступ, либо

содержащее микро-программу (скрипт), который внесет определенные изменения и совершит запланированные действия.

В четвертых, установите на смартфон оригинальное анти-вирусное программное обеспечение, скачайте или включите определитель номера, к примеру в браузере «Яндекс» (это бесплатно), при использовании "Getcontact", «NumBuster» удалите свои теги (сведения о том как вы подписаны у людей) не устанавливайте из сторонних источников приложения, браузеров и особенно из Телеграм-каналов, где приложения и игры взломаны для бесплатного пользования. Всегда обновляйте свой смартфон, системы безопасности и приложения на смартфоне.

В пятых, не используйте в общении конфиденциальные и компрометирующие данные. Помимо использования в целях мошенничества, не забывайте, что данные хранятся на серверах, к которым у организации, предоставляющей способ общения, имеется прямой доступ к вашим данным. В особенности у зарубежных.

В шестых, старайтесь не пользоваться различными «ботами» (программными роботами) в мессенджерах, зачастую перейдя на новый канал или чат, автоматически вы подключаетесь к различным ботам. Завершайте его работу и производите его дальнейшую блокировку вручную. Бот – это отдельная совершенно уникальная программа, находящаяся в мессенджере, какие возможности у бота, известно только создателю. Боты работают в автономном режиме, даже если Вы вышли из приложения. Последствием может быть несанкционированный доступ к Вашим личным данным, а также как результат - получение вредоносного программного обеспечения.

САМОЕ ГЛАВНОЕ!

Помните, что ежеминутно, скорее даже ежесекундно, по всему миру происходят вирусные атаки на различные сервисы, производятся взломы сайтов, взломы программного обеспечения с последующим сливом персональных данных, а также **логинов и паролей**, с целью дальнейшего их использования в корыстных целях. Потому, на различных сервисах, **используйте оригинальный, отличных от других пароль. Не используйте одинаковые пароли!**! Сольют логин и пароль от одного сервиса, «Мегамаркет», «Яндекс.Маркет», «ДНС», да что угодно… а пароль у Вас один от остального. В результате злоумышленнику не составит труда используя слитый пароль использовать его в попытках для входа в популярные сервисы, в т.ч. электронную почту, портал «Госуслуги» и т.д. Не используйте простые пароли, по принципу «четыре или пять клавиш подряд», такой как «12345», дату рождения, используйте пароли с верхним и нижним регистром (большие и малые буквы), по возможности используйте символы, а также цифровые обозначения. И заведите блокнот, где все эти пароли будут храниться на случай необходимости. Периодически меняйте пароли от важных сервисов.

Помните, Ваша безопасность и благополучие в Ваших руках.

ИТ отдел КПК