**Осторожно! Мошенничество в социальных сетях**

27.04.2020 ПРОФИЛАКТИКА

**Настало время снова поговорить о мошенниках. Их методы стары как мир, но все еще действенны, ведь обманщики пытаются нажиться на нашей главной слабости — на желании помочь ближнему.**

Итак, схема следующая: вам приходит сообщение с просьбой помочь от пользователя (чаще из списка ваших друзей). Это могут быть лучший друг, бывший одноклассник и даже девушка вашей мечты, которой вы все это время боялись написать. А тут такая удача — она написала сама, да еще и в помощи нуждается. Вы с готовностью спрашиваете, что же случилось, и как вы можете помочь?

**Дальше все просто: пользователь просит вас перевести ему некоторую сумму денег.** Цели могут быть разными: оплатить интернет, пополнить баланс телефона, просто перевести деньги с карты на карту и т.д. Объясняются эти просьбы тоже весьма разнообразно: внезапным ЧП, отсутствием своей карты, терминалов, денег (завтра точно верну!) — вариантов может быть множество.

Если вам приходит подобное сообщение, задайте другу вопрос, ответ на который можете знать только вы и он. Вопрос остался без ответа? Ваш друг взломан, а от его имени с вами общается мошенник. Смело помечайте сообщение с просьбой о переводе денег как спам и пытайтесь дозвониться до друга, чтобы сообщить ему о взломе аккаунта. Пусть он зайдет на сайт и восстановит доступ к странице, прогнав оттуда взломщиков сменой пароля и проверкой компьютера и телефона на вирусы.

**Есть и другой метод обмана: мошенники создают аккаунты-клоны**, которые один в один похожи на страницы ваших друзей. В этом случае стоит также отметить сообщение как спам и сообщить настоящему другу о поддельной странице.

Если ваш друг (или любой другой пользователь) вдруг **просит сообщить ваш номер телефона и код**, который на него придет — ни в коем случае ничего не отправляйте. Скорее всего, друг был взломан и от его лица к вам обращается мошенник. С помощью этого кода с вашего телефона могут сниматься деньги не только за разовую покупку голосов, но и за все последующие.

Желание купить что-то подешевле и в больших количествах глубоко заложено в человеческой природе. В итоге из-за собственной жадности люди частенько и страдают.

Голоса на сайте можно приобретать только одним способом — с помощью раздела «Баланс». Никаких других способов нет. Если кто-то присылает заманчивое предложение купить у него голоса оптом по весьма сладкой цене — остановитесь! Когда вы переведете «продавцу» деньги, он добавит вас в чёрный список, после чего продолжит поиск новых жертв.

Не надо жадничать и пытаться приобрести голоса подешевле, вы очень быстро нарветесь на мошенничество.

**Когда вам нежданно-негаданно друг без объяснений присылает ссылку, не торопитесь переходить по ней.**Она может вести на вредоносный сайт или программу. Обратите внимание на саму ссылку. Если видите незнакомый адрес или ссылка ведет на файлообменник — стоит насторожиться. Можете написать другу пару уточняющих вопросов, мол, что это ты мне прислал. Даже если вам придет ответ, все равно не спешите. Мошенники, взломавшие страницу, могут находиться на ней некоторое время и даже отвечать на сообщения. Если вам пишут злоумышленники, стиль ответов вас, скорее всего, насторожит. Они будут отвечать уклончиво и всячески торопить вас: «открой и увидишь», «это то самое фото», «не открывается? Я тебе другую ссылку сейчас пришлю», «нет времени объяснять — зайди и все увидишь» и т.д.

**Пометьте сообщение как спам и постарайтесь найти способ сообщить другу о взломе его страницы не через сайт.**

Представьте другую ситуацию. Вы находитесь вне дома, и вам на телефон **приходит сообщение «Ваша страница взломана, для активации страницы пришлите «ОK» на короткий номер...»** либо «На сайте ВКонтакте проходит проверка страниц. Все неактивированные страницы будут удалены. Для активации отправьте SMS на номер...». Не торопитесь! Когда вы окажетесь дома и зайдете на свою страницу, то увидите, что тревога была ложной. А если вы отправите ответное SMS «на всякий случай», то с вашего баланса моментально будет списано несколько десятков, а то и сотен рублей. Данный тип мошенничества довольно коварен. Злоумышленник может отослать десятки сообщений на любые произвольные номера, и с большой вероятностью многие из них окажутся привязанными к страницам. Но помните: ВКонтакте никогда не рассылает подобные SMS.

Многие знают, что в социальных сетях имеется своя валюта, в «Одноклассниках» это Оки, «Вконтакте» - это голоса. Действия злоумышленников в данной категории направлены на несовершеннолетних, которые играют в различные игры в социальных сетях. Так, **ребенку на страницу приходит сообщение от неизвестного ему лица, которое предлагает получить голоса «Вконтакте» бесплатно**, для этого необходимо предоставить абонентский номер. Ребенок естественно соглашается. После чего злоумышленник сообщает, что на телефон будут приходить сообщения, на которые необходимо отвечать «Да». Ребенок с радостью отвечает на смс-сообщения, при этом не обращает внимания на то, что в сообщении написано, что отправка платная и стоит в среднем 3,5 рубля. Тем самым на счету абонентского номера образовывается задолженность.

Призываем проявлять бдительность. Помнить самим и объяснять детям о возможности стать жертвой интернет-мошенников.