

17 схем мошенничества с использованием телефона и интернета.

Уважаемые педагоги, обучающиеся, родители! Будьте бдительны, общаясь с незнакомцами по телефону, в интернете и лично. Читайте, какие схемы чаще всего используют сегодня мошенники.

Мошенничества с использованием мобильной и проводной связи

1. Самая популярная схема – просьбы о помощи от лица друзей или родственников с помощью sms примерно следующего содержания: «Привет. Это Саша. Положи мне, пожалуйста, 1000 рублей на телефон. Срочно!».

Как действовать, очевидно: ничего никому не класть!

2. Более сложная схема – вам звонит человек и представляется кем угодно вплоть до сотрудника правоохранительных органов. Такой «полицейский» сообщает, что кто-то из родственников попал в ДТП с последствиями и чтобы избежать уголовной ответственности, предлагает «решить ситуацию». *Не реагируйте, не паникуйте, просто посылайте такого «решалу» куда подальше!*

3. Звонок или сообщение на платные номера Вам звонят с неизвестного номера, но сбрасывают до того, как вы успеете взять трубку. Вы из любопытства перезваниваете и слышите либо автоответчик, либо длинные гудки. Фишка в том, что в обоих случаях звонок платный: деньги с вашего счёта переходят на счета мошенника. *Не любопытствуйте! Кому надо, ещё раз позвонят.*

4. Схема «Выгодное предложение»: вы получаете sms о том, что вы выиграли в лотерею (путёвку, машину и т. п.), и для получения информации о том, как забрать приз, вам надо отправить ответное sms либо перевести небольшую сумму на указанный счёт. Не менее опасно переходить по указанным в sms ссылкам. Вместо призов и «акций» можно попасть на сайт мошенников и получить вирус, крадущий с телефона деньги и информацию.

Бесплатный сыр бывает только в мышеловке!

5. Схема «Дайте позвонить»: мошенники обращаются к прохожим на улице с просьбой одолжить сотовый телефон, чтобы позвонить. После одного или нескольких звонков отзывчивый владелец мобильного обнаруживает, что баланс его стал почему-то значительно меньше.

Доброта она такая...

6. Схема «Платный код»: звонит «сотрудник службы технической поддержки оператора мобильной связи» и предлагает подключить новую эксклюзивную услугу или пройти перерегистрацию во избежание отключения связи из-за технического сбоя (или для улучшения качества связи). Якобы для этого абоненту надо набрать под диктовку некий код, который на самом деле является комбинацией для осуществления мобильного перевода денежных средств со счёта абонента на счёт мошенников.

Посылайте такого «сотрудника» в сад!

7. Схема «Штрафные санкции оператора»: злоумышленник представляется сотрудником службы техподдержки оператора мобильной связи и сообщает, что вы сменили тарифный план, а оператора об этом не оповестили (варианты: не внесли своевременно оплату, воспользовались роумингом без предупреждения) и теперь вам надо оплатить штраф определённого размера, купив карты экспресс-оплаты и сообщив их коды.

Никакие карты не покупайте!

8. Схема «Проблемы с банковской картой или счётом»: эти примитивные телефонные мошенничества рассчитаны на страх человека лишиться денег. Все они начинаются примерно одинаково: вам приходит sms «от банка», или звонят мошенники, выдавая себя за его сотрудников. Вам рассказывают «страшные вещи» о том, что заблокирована ваша банковская карта или вы задолжали по кредиту. В лучшем случае вам предлагают для

разъяснения ситуации позвонить «оператору банка». Если перезвоните – попадёте на платный номер и потеряете деньги со счёта телефона. Ещё хуже, если по просьбе «банка» вы сообщите мошенникам номер карты и её пин-код, пароль от «Личного кабинета» интернет-банка или персональные данные. При таком раскладе деньги с вашего счёта бесследно исчезнут.

МАТЕРИАЛЫ ПО ТЕМЕ

Налог на доверчивость

Мошенники ищут всё новые и новые способы выманивать деньги у доверчивых граждан.

Вот какой реальный случай произошёл в Бердске. Мужу потерпевшей пришло sms о том, что его банковская карта заблокирована. Напуганная женщина позвонила на указанный номер и попала на мужчину, назвавшегося сотрудником службы безопасности банка. Он спросил, знает ли она Полякова. Женщина ответила, что нет. «Сотрудник банка» поведал, что этот Поляков пытался снять деньги с банковской карты мужа, из-за чего служба безопасности заблокировала его карту. Чтобы разблокировать, необходимо назвать номер карты и цифры на обороте. Женщина всё это сообщила. После этого на её номер и номер её мужа стали приходить sms с кодами, которые она также сообщила «сотруднику банка». В итоге с карты мужа списано 10 тысяч рублей, с её карты – 22 тысячи рублей. Заведено уголовное дело.

На каждой банковской карте сверху указан номер телефона информационного центра вашего банка, по которому можно звонить круглосуточно. «Сотруднику» говорите «прощай» и звоните на этот номер с любыми вопросами.

9. Схема «Мобильный банк»: участились случаи мошенничеств с использованием услуги «Мобильный банк», позволяющей управлять счетами через мобильники. Услуга «привязывает» банковский счёт к номеру телефона клиента

банка. Следователь ГСУ ГУ МВД России возбудил уголовное дело по факту хищения денежных средств с банковской карты. Вот как развивались события: к банковской карте потерпевшего был подключен «Мобильный банк». Решив оплатить коммунальные услуги, мужчина вошёл в «Мобильный банк» по

ссылке, которой постоянно пользовался, но не заметил, что в строке, где пишется адрес входа, что-то поменялось. Ему пришло sms с одноразовым паролем для входа в «Мобильный банк». Он ввёл его, после чего на странице появилось «СПАСИБО» и больше страница не открывалась. Нажав повторно на ссылку, страница открылась, но с его счёта пропали 6 800 рублей.

Не распространяйте в интернете сведения о мобильных номерах с их привязкой к анкетным данным, не указывайте на страницах в соцсетях мобильные номера, свой адрес и другую личную информацию. Не используйте в интернете номера своих мобильных телефонов, к которым привязаны банковские карты и номера мобильных телефонов, которые вы используете в «Мобильном банке». Если с вашего телефона или банковской карты похитили деньги, немедленно обратитесь в банк, чтобы заблокировать счёт, запретить перевод денег с вашего счёта на другие счета или приостановить обслуживание счетов, на которые ушли ваши деньги. После ответа от банка идите в полицию.

Запомните! Банк никогда не запрашивает по телефону сведения о карте клиента, её номер, код на обратной стороне, ФИО владельца, срок её действия, а тем более пин-код! Если собеседник пытается получить от вас такую информацию, либо просит сообщить коды, которые пришли на ваш телефон от банка, просто прекращайте с ним разговор.

10. Схема «Вредоносная ссылка»: мошенники используют мобильный телефон для передачи сообщений через Viber или WhatsApp с вредоносной ссылкой. Например, «здесь ваши фото...», «ваш аккаунт, страница в «Одноклассниках» взломаны, пройдите регистрацию, «вы выиграли автомобиль, подробности ...» и т. д.

Не проходите по такой ссылке, очень высок риск заражения телефона вредоносной программой.

Кроме того, вы можете столкнуться с таким видом вредоносных программ, которые не требуют вашей активности и сами загружаются на

ваше мобильное устройство через уязвимости операционной системы. При заражении мобильного устройства происходит блокировка операционной системы, входящих sms, отправка искусственно сгенерированных мобильным устройством сообщений.

Заражённый мобильный телефон отключите, обратитесь к оператору за новой сим-картой, а телефон сдайте в сервисный центр. Если мошенникам удалось похитить денежные средства – бегом в полицию!

Мошенничества в интернете

1. Мошенничества при продаже товаров в интернете по предоплате: продавец отказывается встречаться лично и готов продать товар только посредством пересылки его по почте при условии полной или частичной предоплаты.

Пользуйтесь услугами уже проверенных магазинов!

2. Получение от интернет-магазина товара, не соответствующего заявленному.

До совершения покупки проверьте, давно ли создан сайт магазина, почитайте отзывы в интернете. Не делайте «слепые» покупки в соцсетях. Администрация соцсетей не несёт ответственность за совершаемые с использованием сети действия пользователей. При покупке железнодорожных и авиабилетов не приобретайте дешёвые билеты на сомнительных сайтах, расположенных в доменных зонах .com, .mobi, .org, .biz, .net, .info, .tv. и других, не связанных с российским интернет-пространством. Покупайте билеты на официальных сайтах перевозчиков.

3. Схема «Отклики на объявления»: вам приходит sms от имени сайта объявлений с предложением отправить текст на короткий номер в связи с тем, что вам поступили отклики по объявлению, или же ваш аккаунт

был заблокирован. Итог – с вашего счёта будут сняты деньги. Вернуть их невозможно.

Не отвечайте на подобные сообщения и обратитесь в службу поддержки или к оператору мобильной связи с жалобой.

4. Схема «Сами мы не местные»: мошенник под видом покупателя сообщает вам, что желает приобрести ваш товар, но живёт в другом городе и предлагает оплатить товар перечислением денег на вашу карту. Для этого он просит вас назвать номер карты, владельца, срок её действия, код на обратной стороне и сотовый номер, привязанный к карте, либо по умолчанию использует номер, указанный вами в объявлении. После этого мошенник использует данные о карте для оплаты покупок в интернете.

Недавний пример. Житель Новосибирской области разместил на одном из сайтов объявлений информацию о продаже дома в Республике Бурятия. Ему позвонил мужчина, который сказал, что хочет купить дом и готов перевести ему деньги на его банковскую карту в счёт предоплаты. После этого позвонила женщина, представилась бухгалтером и сказала, что готова внести предоплату за дом. Обрадованный продавец назвал ей номер своей карты, а после того, как пришли сообщения с кодами подтверждения, назвал и коды, не прочитав текст сообщений, в которых было сказано, что одноразовые коды нельзя сообщать никому, даже сотрудникам банка. В итоге с карты были списаны 63 000 рублей.

Запоминаем: одноразовые коды нельзя сообщать никому, даже сотрудникам банка.

5. Схема «Зарегистрируйся»: на некоторых сайтах можно зарегистрироваться, только указав свой номер телефона, на который якобы должен прийти код для регистрации. Но если код не приходит в течение 5 минут (а он и не придёт), вам самостоятельно необходимо отправить sms на определённый номер.

Не делайте этого! С вашего счёта спишут деньги!

6. Схема «Инвестирование»: на просторах интернета есть множество сайтов, которые предлагают вложить свои деньги под определённый процент. Но многие из этих ресурсов – обман.

7. Схема «Учим зарабатывать в интернете». Вам предлагают купить руководство по заработку в интернете (или иные методики), где даётся подробная инструкция, как можно заработать определённую, как правило, большую сумму денег. Чтобы разбогатеть, вам необходимо купить диск, оплатить пересылку и т.п. *Где бывает бесплатный сыр? На самом вы покупаете «пустышку».*

Если вы стали жертвой мошенника, незамедлительно обращайтесь в органы внутренних дел. Вовремя поступивший сигнал о деятельности преступников повышает шансы установить их личности «по горячим следам».