

СМС - сообщение с «сюрпризом»

В последнее время, все чаще на мобильные номера жителей нашего города приходят СМС – сообщения следующего характера:

«Привет! Я нашел твои фото: (ссылка). Не благодари!». Когда получатель данного сообщения переходит по указанной ссылке, на его телефон устанавливает вирусная программа, которая открывает полный доступ, как к самому телефону, так и к банковской карте.

Чтобы избежать такой ситуации, настоятельно рекомендуется установить антивирусную программу на свой смартфон, а так же не переходить по сомнительным ссылкам, направленных даже с якобы известных Вам номеров.



Взлом страницы

Мошенники взламывают страницу Вашего друга в Социальных сетях и посылают Вам сообщение:

«Привет. Не одолжишь тысячу рублей до субботы? Очень срочно, поэтому лучше на карту».

В результате деньги получают именно мошенники, а не Ваш знакомый.

Помните, получив просьбу дать в долг, положить деньги на телефон, заплатить за Интернет... перезвоните и уточните, действительно ли знакомый нуждается в деньгах.

Если у вас нет его номера, подумайте, стал бы этот человек просить у вас денег?



Памятка для граждан

Как не стать
жертвой мошенников



Мошенничество как отдельный вид преступной деятельности постоянно меняется и развивается пропорционально процессам, происходящим в стране и в обществе, затрагивая интересы различных слоев населения.



Будьте бдительны! Предупредите своих родственников и знакомых, не поддавайтесь на уловки мошенников! Не перечисляйте деньги на счета неизвестных вам номеров сотовых телефонов, не отправляйте денежные средства на имя неизвестных лиц! Кроме того, ни под каким предлогом нельзя сообщать посторонним лицам номер карты, цифры, размещенные на ее обратной стороне, а также пин-код. Помните, что банковские служащие такие данные не запрашивают!

Часто мошенникам удавалось обмануть жителей нашего города используя социальные сети «ВКонтакте» и «Одноклассники». Граждане вступали в переписку с якобы продавцами интересующего их товара, затем по договоренности перечисляли денежные средства, когда же товар не приходил в установленный день, они узнавали что «продавец» перестает выходить на связь и добавляет их в черный список;



Еще одним из наиболее распространенных видов мошенничества, является мобильный банкинг, суть его заключается в том, что гражданин привязывает свой абонентский номер сотового телефона к зарплатой или кредитной карте какого-либо банка. По истечении времени абонент прекращает использовать абонентский номером или отказывается от него, однако услугу смс – оповещение не отключает. Спустя некоторое время компанией сотовой связи указанный абонентский номер выдается другому лицу, которое с помощью подключенной услуги похищает денежные средства.

Работа по предоплате

Преступники размещают объявление о вакансии, обещающие большую заработную плату, в газетах или на интернет-сайтах. Соискателя приглашают на собеседования и просят взять документы и пластиковые банковские карты. После чего просят сообщить последние три цифры номера, указанного на обратной стороне пластиковой карты, якобы для перечисления ему будущей заработной платы. После чего со счета гражданина списываются все активы.

Встречи

Нередко мошенники регистрируются в соцсетях под видом бывших одноклассников или сослуживцев других пользователей, предлагают организовать встречу. По одному из распространенных сценариев мошенник на сайте «Одноклассники» берет первую попавшуюся школу и начинает поиск «одноклассников». Люди, естественно, пишут, что не припоминают такого человека, но он убеждает их в обратном, приводит аргумент, что учился с ними лишь короткое время. Затем злоумышленник говорит жертвам, что желает организовать встречу выпускников и на это ему потребуются денежные средства, он уже выбрал ресторан, где можно «хорошо посидеть», весело провести время. Одноклассники дружно отправляют деньги на счет, на этом встреча и заканчивается.

Вашу личную страницу удалят

Еще одна уловка, которой не пренебрегают злоумышленники: они рассылают пользователям от имени администрации сайта требование подтвердить, что они реально существующие люди. Предлагают сделать это посредством отправки смс на указанный номер. Затем предупреждают, что удалят страницу безвозвратно. При отправке сообщения на данный номер, Вы рискуете потерять все денежные средства, которые находятся на счету.



Чтобы не попасться на мошенничество «ВКонтакте» или на «Одноклассниках», желательно следовать нескольким простым правилам:

- уточните у адресата, от которого пришло странное сообщение, отправлял ли он вам его.
- Если он ничего не отправлял, не выполняйте никаких указаний из письма;
- старайтесь не добавлять «в друзья» незнакомых людей;
- не используйте очень простой пароль для входа на вашу страничку или сайт.