Мошенничество в сети Интернет. Мобильное мошенничество.

Актуальность темы обусловлена тем, что интернет прочно вошел в нашу жизнь. Им пользуются все, начиная от детей и заканчивая стариками.

Одни просто ищут информацию, другие являются более активными пользователями, которые применяют возможности глобальной сети для приобретения товаров, оплаты коммунальных счетов, проверки состояния банковского счета, пополнения мобильного телефона и т.д. То есть производят операции с денежными средствами через интернет. Кроме того многие заводят аккаунты в социальных сетях, вводят при регистрации личные данные. И это норма нашей жизни.

Но что для одних стало нормой, для более «предприимчивых» является возможностью нажиться. Если вы относитесь к активным пользователям Всемирной паутины, то рекомендуем прочитать эту статью очень внимательно. Мы собрали крайне полезную информацию о том, как обманывают в интернете, как не попасться на крючок к мошенникам.

Все виды и способы вряд ли удастся перечислить, настолько они разнообразны. Тем не менее, мы попробуем уберечь наших читателей от самых распространенных схем мошенничества.

1. В социальных сетях.

1.1 Мошенники взламывают аккаунты пользователей и от имени того, кого взломали, пишут сообщения всем друзьям из списка с просьбой одолжить денег. Вы соглашаетесь, так как это ваш друг или родственник и переводите свои деньги, может и небольшие мошенникам на карту.

Совет: в таких случаях, задайте ему проверочный вопрос. Если уходит от ответа или отвечает не правильно, его взломали.

1.2 Конкурсы за репост. Когда участника просто разводят на деньги, под предлогом оплатить доставку за выигранный приз.

Совет: если вы получили сообщение о выигрыше, уточните когда он проходил и есть ли видео подтверждающее что выиграли именно вы и самое главное не платите за доставку.

1.3 Если в группе по тематике «отдам даром» закрыты комментарии и отсутствует подпись в объявлениях, им не стоит доверять, поскольку в настоящих группах участники общаются и задают вопросы о товаре.

2. Через СМС.

Чтобы избежать обмана и не стать жертвой мошенников соблюдайте основные правила:

1. Проверьте и убедитесь в достоверности информации, которую Вам сообщили в СМС

2. Не торопитесь выполнять действия, которые от Вас требует неизвестные.

3. Не отправляйте СМС на короткие номера, указанные в СМС сообщении

4. Не открывайте файлы и ссылки, пришедшие в СМС сообщениях с неизвестных номеров

3. Электронная почта.

Один из самых распространенных сейчас способов взлома электронной почты - это рассылка электронных писем со встроенными в них вирусами. Обычно такие письма имеют вложенные файлы в виде картинок или архивов, которые вам предлагается скачать и открыть на своем компьютере.

Часто пароль мошенникам раскрывает сам владелец почты. Происходит это так: на ваш электронный ящик приходит письмо, подписанное службой поддержки, где сказано, что по таким-то причинам вы должны сообщить свой пароль службе поддержки, иначе возникнут проблемы с доступом к вашему ящику.

Что бы обезопасить свою электронную почту соблюдайте основные правила:

1. Пароль должен быть сложным, то есть состоять минимум из 8 знаков, часть из которых должны быть цифрами — таким образом, вы усложните процесс подбора пароля. Не используйте пароли типа: 123456, qwerty, qwerty123, super, dimon и т.д и т.п.

2. Ответ на контрольный вопрос должен быть необычным, знать его должны только вы.

3. Хотя бы раз в полгода меняйте пароль, так как устаревший пароль является источником опасности и повышает шансы на взлом вашей почты.

4. Не используйте один и тот же пароль в разных сервисах (например, для входа в почтовый ящик и для электронных денег).

5. Никому не сообщайте ваш пароль.

6. Не разрешайте компьютеру хранить ваши данные, держите пароль в голове.

7. Будьте осторожны при общении с незнакомыми людьми в Сети.