Как сделать общение в соцсетях безопасным

Примеры мошеннических уловок:

- взламывание страниц: рассылка контактному списку сообщений с просьбой пополнить счет;
- рассылка от имени администраторов соцсети предупреждения об удалении страницы, в случае отсутствия подтверждения личности по смс;
- раскрутка якобы недавно созданного сайта, который после регистрации на нем позволит получать голоса, подарки.

Результат мошеннических действий:

- люди из вашего контакт-списка переводят «вам» денежные средства;
- снятие с вашего счета, привязанного к соцсети, дененежных средств.

Ваши правильные действия, или 6 советов омской полиции:

1. создайте сложный пароль для почтового ящика, на который вы будете регистрировать аккаунт соцсети;
2. общаясь в социальных сетях, не следует слепо доверять всем, кто захочет установить с вами контакт;
3. «освежите» секретные вопросы для восстановления паролей;
4. не привязывайте к аккаунту в соцсети кредитную карту или интернет-кошелёк;
5. не доверяйте предложениям относительно повышения рейтинга;
6. с большой осторожностью относитесь к установке приложений внутри соцсети.

УМВД России по Омской области

Телефоны:

«Горячей линии» - 79-33-04
Отделения по работе с обращениями граждан - 79-39-66
Дежурной части - 25-12-98

Телефоны городских отделов полиции:

Отдел полиции № 1 – 76-04-04
Отдел полиции № 2 – 71-03-04
Отдел полиции № 3 – 55-04-04
Отдел полиции № 4 – 40-04-04
Отдел полиции № 5 – 42-04-04
Отдел полиции №7 – 24-04-04
Отдел полиции № 8 – 63-04-04
Отдел полиции № 9 – 31-04-04
Отдел полиции № 10 – 20-04-04
Отдел полиции № 11 – 61-04-04
ПП «Октябрьский» – 79-34-02
ПП «Чкаловский» – 79-22-59
ПП «Крутая Горка» – 91-22-22

Веб-ресурсы омской полиции:

МВД55.рф
vk.com/55mvd
www.instagram.com/omsk_police/
twitter.com/omskpolice
www.youtube.com/user/omskpolice

Отпечатано при содействии Общественного совета при УМВД России по Омской области

УМВД России по Омской области

Безопасный он-лайн: рекомендации омской полиции

Как закрыть доступ виртуальным злоумышленникам к вашему кошельку

Примеры мошеннических уловок:
- смс-сообщение со ссылкой (например, выигрыш, отклик на ваше объявление);
- сообщение при просмотре интернет-страниц «Ваш flash player нужно обновить»;
- письмо на электронную почту с прикрепленным файлом формата «Имя.SCR», или файл-архив, внутри которого документ «Имя.SCR».

Это далеко не полный список! Каждый день злоумышленники придумывают новые способы обмана.

Результат мошеннических действий:
- если вы используете услугу «мобильного банка» либо производите электронные платежи с использованием банковских карт - злоумышленники списывают денежные средства с карты без вашего ведома. Даже если вы работаете с домашнего компьютера и не производите никаких платежей, рабочие документы, фотографии безвозвратно блокируются, а за их расшифровку потребуют заплатить.

Хищения денежных средств через «мобильный банк» происходит путем заражения вирусом мобильных устройств на операционной системе «Android». Сущность вируса – получение доступа к функциям отправки и отсылки смс-сообщений. В основе, как правило, лежит личное участие пользователя устройства.

Ваши правильные действия, или 7 советов омской полиции:
1. не переходить по ссылкам на неизвестные интернет-ресурсы;
2. установить антивирусные программы;
3. установить блокировщики рекламы;
4. на мобильных аппаратах на операционной системе «Android» отключить «мобильный банк», или приобрести для этой цели более простое мобильное устройство, с которого вы не будете выходить в Интернет;
5. использовать на смартфонах для перевода денег программы дистанционного банковского обслуживания типа «интернетбанк-клиент»;
6. отключить на смартфоне функцию «Установка из неизвестных источников»;
7. работать на ПК с правами доступа «Пользователь», а не «Администратор».

Как правильно совершать покупки в Интернете, чтобы они приносили радость

Признаки потенциально опасных интернет-магазинов:
- низкая цена;
- требование предоплаты;
- отсутствие возможности самовывоза;
- отсутствие контактной информации;
- отсутствие у продавца «истории»;
- неточности в описании товара;
- «продавцы» направляют изображение якобы своего паспорта с целью подкупить ваше доверие.

Результат мошеннических действий:
- перевод вами денежных средств на счет продавца, после чего последний перестает выходить на связь.

Ваши правильные действия, или 5 советов омской полиции:
1. сравните цену аналогичных товаров в других магазинах;
2. не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион»;
3. отдавайте предпочтение магазинам, в которых есть возможность забрать товар самостоятельно;
4. если указан адрес магазина, проверьте существует ли он;
5. с осторожностью совершайте покупки в только что открывшихся магазинах, изучите отзывы других покупателей.