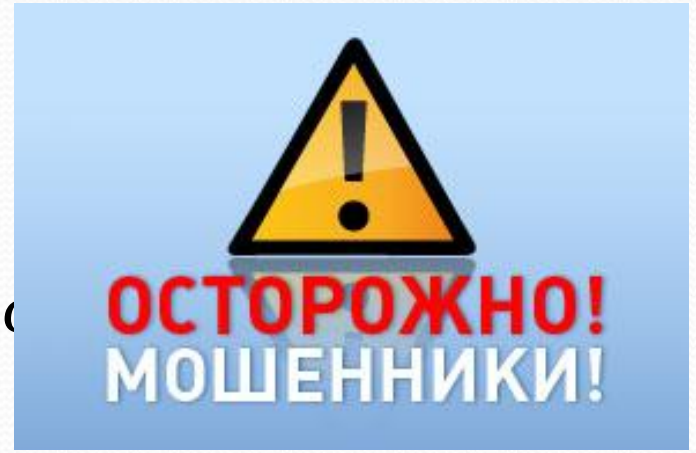
Безопасность в сети интернет

Вирусы

- **Рекомендации:**
- *Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.*
- *Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.*
- *Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).*
- *Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.*
- *Не подключать к своему компьютеру непроверенные съемные носители.*
- *Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.*

Мошеннические письма

- **Рекомендации:**
- *Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.*
- *Игнорировать такие письма.*

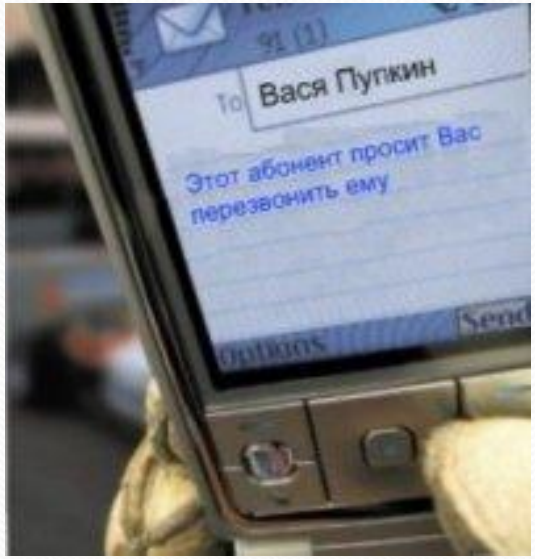


Получение доступа к аккаунтам в социальных сетях и других сервисах.

- **Рекомендации:**
- *Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).*
- *Никому не сообщать свой пароль.*
- *Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.*
- *Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).*
- *Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.*

Безопасность платежей в интернете.

Фиктивные звонки от платежных сервисов



- **Рекомендации:**
- *- Помнить, что банки и платежные сервисы никогда не просят сообщать –ни по почте, ни по телефону – пароль, пин-код или код из SMS.*
- *- Никому не сообщать пароли, пин-коды и коды из SMS от своего кошелька или банковской карты.*

Выманивание SMS-пароля незнакомцем

- **Рекомендации:**
- *- Никому не сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, а также мобильных операторов.*

Фальшивые письма от платежных сервисов

- **Рекомендации:**
- *- Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.*
- *- Не переходить по ссылкам из таких писем и не вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка, Яндекс.Денег или другого платежного сервиса.*
- *- Перед вводом своих платежных данных на каких-либо сайтах проверять название сайта в браузере. Например, вместо money.yandex.ru фальшивый сайт может называться money.yanex.ru*

Фальшивые выигрыши в лотереи

- **Признаки фальшивой лотереи:**
- Пользователь никогда не принимал участие в этой лотерее и вообще ничего о ней не знает;
- Пользователь никогда не оставлял своих личных данных на этом ресурсе или в этой организации, от имени которой приходит письмо;
- Сообщение составлено безграмотно, с орфографическими ошибками;
- Почтовый адрес отправителя – общедоступный почтовый сервис.
- Например, gmail.com, mail.ru, yandex.ru.

Фальшивые сайты авиабилетов

- **Рекомендации:**
- *- Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в интернете. Если не удается найти положительные отзывы или нет вообще никаких пользовательских сообщений об этом ресурсе, это должно насторожить. Сайт может быть создан за один день, а закрыться уже на следующий или даже сразу после того, как на нем будет совершено несколько покупок.*

Фальшивые квитанции

- **Рекомендации:**
- *- Проверять реквизиты, указанные в платежке. Если они не совпадают с прежними, не оплачивать по счету. Информацию о смене реквизитов можно проверить по официальным телефонам (на квитанции они могут быть неверные).*
- *- Проверять номер своего лицевого счета, указанный на платежке за ЖКУ. Он всегда один.*
- *- Обратить внимание на дату получения платежки. Как правило, мошенники приносят поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи.*
- *- Настроить онлайн-платежи на заранее проверенные реквизиты и платить только по ним через проверенные сайты (сервис «Городские платежи», интернет-банк «Сбербанк.Онлайн», Альфа-Банк и др.)*

Выпрашивание денег со взломанных аккаунтов в соцсетях или мессенджерах. Фальшивые SMS якобы от знакомого

- **Рекомендации:**
- *- Всегда лучше перезвонить знакомому и уточнить, правда ли он сейчас нуждается в деньгах.*
- *- Если возможности позвонить нет, можно задать какой-нибудь проверочный вопрос, ответ на который может знать только знакомый.*
- *- Связаться лично с пользователем, от имени которого прислано SMS, чтобы проверить информацию.*

Бесплатное скачивание файлов с подпиской

- **Рекомендации:**
- *- Не указывать свой мобильный номер на незнакомых сайтах.*
- *- Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.*

Безопасность при оплате картами

- *Не сообщайте номер карты другим людям*
- *Храните банковскую карту в надежном месте.*
- *Не держите записанные пароли и коды рядом с картой.*
- *Заведите отдельную карту для покупок в интернете.*
- *Используйте для покупок в интернете только личный компьютер.*
- *Регулярно обновляйте антивирусную защиту компьютера.*
- *Старайтесь делать покупки в известных и проверенных интернет-магазинах.*
- *Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.*
- *Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах.*
- *Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте.*
- *Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.*

Спасибо за внимание