

«Безопасный интернет»



Интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избежать их.

Какие опасности могут поджидать в интернете

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут использовать самые разные инструменты и методы — например, вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах.

Как уберечь компьютер от заражения вирусом

Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.

Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

Не подключайте к своему компьютеру непроверенные съемные носители.

Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные от мошенников

Используйте сложные пароли (они 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 сообщайте свой пароль.

Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.

Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).

Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

Как избежать мошенничества при платежах

Во-первых, необходимо обеспечить безопасность своей банковской карты. Сделать это несложно, если придерживаться следующих рекомендаций:

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 адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.

Подключите в банке услугу sms-уведомлений, чтобы получать сведения о всех совершаемых платежах.

Сохраняйте документы об оплате и доставке товаров, полученные по электронной почте.

Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Не используйте общественный Wi-Fi при совершении покупок в интернете – данные банковских карт могут быть перехвачены мошенниками.

Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из sms.

Никому не сообщайте пароли, пин-коды и коды из sms от своего кошелька или банковской карты.

Фальшивые sms, якобы от знакомого

Мошенник может прислать родственникам пользователя sms с неизвестного номера, но якобы от имени пользователя. Например: «Мама, я попал в аварию, срочно нужны деньги, переведи их, пожалуйста, на этот номер телефона». «Папа, у меня проблемы, я в больнице, срочно нужны деньги, кинь их, пожалуйста, на этот кошелек. Маме не говори». Цель мошенника — выманить деньги у близких пользователя: они сами переведут их на указанный мобильный номер, электронный кошелек или банковскую карту (в зависимости от того, какой способ будет указан в sms).

Как не попасться на удочку sms-мошенников

Не отправляйте sms на незнакомые телефонные номера, за оправку таких sms могут взимать плату.

Переводите деньги только на известные телефонные номера.

Не вводите телефонный номер на незнакомых сайтах.

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.

Похищение данных при использовании бесплатных сетей Wi-Fi

Сейчас мы много общаемся через компьютер или смартфон и часто делаем это в общественных местах — подключившись к Wi-Fi-сети, которая не защищена паролем. Когда никто из окружающих не заглядывает в экран, создаётся ощущение приватности. На самом деле, передача данных через открытую Wi-Fi- точку – это в каком-то смысле разговор в полный голос в людном месте.

Злоумышленники создают сети с распространёнными названиями и просматривают всё, что подключившиеся к ней пользователи делают в интернете: читают и пишут личные сообщения в соцсетях, вводят пароли или данные банковских карт.

Как не пострадать при использовании бесплатных сетей Wi-Fi
Используйте мобильный интернет (EDGE, 3G, LTE).

Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

Старайтесь посещать только сайты с шифрованием данных (HTTPS – он обычно отмечен зелёным замочком в браузерах).

Используйте специальные средства защиты — браузеры со специальным безопасным режимом просмотра страниц или программы-защитники, которые разрабатывают антивирусные компании.

И еще один важный совет: **СЛЕДИТЕ ЗА ТЕМ, ГДЕ И КАК ПРОВОДЯТ ВРЕМЯ ВАШИ ДЕТИ, ОСОБЕННО В ИНТЕРНЕТЕ!** Установите ФУНКЦИЮ «Родительский контроль», ограничьте доступ к сайтам, которые могут навредить Вашим детям, Вам, спокойствию и здоровью Вашей семьи, нанести угрозу вашему финансовому положению!

Посетите сайты <http://kvestsetevichok.ru/index.php/edinyj-urok-po-bezopasnosti-v-seti-2015>, www.сетевичок.рф и следуйте рекомендациям специалистов по доступу к ресурсам Интернет.