Безопасный Интернет

БУДЬ В БЕЗОПАСНОСТИ:
КАК НЕ СТАТЬ ЖЕРТВОЙ IT-ПРЕСТУПЛЕНИЙ

ТОП-10 ПРАВИЛ

Появление в нашей повседневной жизни современных компьютерных устройств и программных сервисов делает нашу жизнь намного удобнее, но требует определённых навыков и знаний. Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие нас обмануть и присвоить наши денежные средства.

Чтобы не стать жертвой преступников, обезопасить себя и своих близких от посягательств на их персональные данные и личные сбережения, необходимо придерживаться соблюдения ключевых правил медиабезопасности.

Памятка «Будь в безопасности: как не стать жертвой IT-преступлений (ТОП-10 правил)» из серии «Безопасный Интернет» подготовлена на основе материалов Центра мониторинга социальных сетей и открытых Интернет-источников.

1

Не добавляйте незнакомых людей в друзья

Одно из ключевых правил безопасности гласит - никогда не говорите на улице с незнакомцами. Это же правило действует и в Интернете.

Только здесь притворяться другим человеком гораздо проще, чем в реальной жизни. Просто знайте, что за аватаркой симпатичной девушки может скрываться кто угодно – особенно если она отчаянно пытается узнать адрес или, например, модель компьютера.

2

Никому не сообщайте личную информацию

Никогда и ни при каких обстоятельствах нельзя сообщать информацию личного характера, в том числе свои персональные данные, к которым относятся: фамилия, имя, отчество, дата рождения, домашний адрес, номера телефона, банковских карточек, пароли.

Знакомясь и общаясь в Интернете, обращайте внимание на вопросы, которые вам задают новые друзья.

В случае подозрения виртуальных друзей в попытках обмана – немедленно прекращайте общение!

3

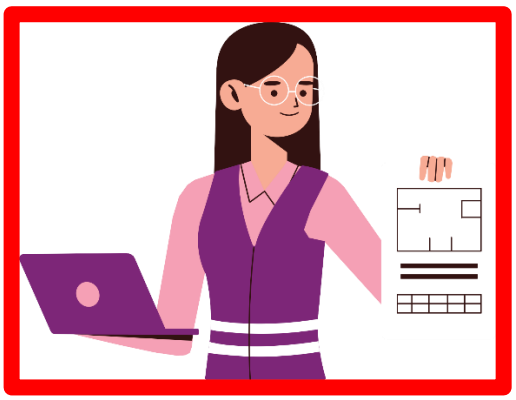
Не скачивайте программы с сомнительных сайтов

Используйте для загрузки приложений только официальные Интернет-ресурсы.

Скачав программу с первого попавшегося ресурса, можно легко поймать вирус, из-за которого не только сломается техника, но и у злоумышленников окажутся номера как ваших банковских карт, так и ваших родителей.

4

Не переходите по подозрительным ссылкам



Нельзя нажимать на подозрительные ссылки, которые приходят по электронной почте или в сообщениях.

Например: «Посмотри, что здесь о тебе говорят», «Ты стал обладателем нового iPhone – переходи по ссылке, чтобы забрать его». Нужно знать, что такие сообщения отправляют мошенники и при переходе по данной ссылке есть большой риск того, что на ваш компьютер или смартфон попадёт опасный вирус.

5

Не ставьте геометки под фото

По ним злоумышленники легко узнают, где вы живёте и учитесь. Конечно, нет ничего страшного в том, что вы проставите геометку на фотографии, например, со школьной экскурсии.

Но табу должны стать личный адрес, адрес вашего образовательного учреждения и работы близких друзей или родственников.

6

Перепроверяйте сообщения с просьбами о помощи от друзей и родственников

Иногда мошенники взламывают аккаунты в соцсетях и рассылают всем друзьям сообщения с просьбой перевести деньги.

Не торопитесь с помощью, свяжитесь по телефону с человеком, со странички которого пришло сообщение, чтобы самому узнать, нужны другу деньги или нет. Или посоветуйтесь с родителями.

7

Не переходите на подозрительные страницы для совершения онлайн-покупок

Мошенники любят совершать онлайн-покупки не меньше, чем вы, но у них на это есть свои причины. В виртуальном мире бдительность ослабевает, и игроки могут не заметить обмана. Покупателей заманивают низкими ценами и «уникальными акциями». И не стоит заблуждаться, в подобные ловушки могут попасть не только дети, но и взрослые.

Прежде чем вводить на странице сайта свои персональные данные, пароли, коды или реквизиты банковской карты для совершения покупки - удостоверьтесь, что это не мошеническая страница. Платежи в интернете нужно согласовывать со взрослыми. И лучше подключить уведомления о платежах!

8

Не надейтесь на быстрое обогащение!

Если вам не хватает карманных денег на модный телефон и терпения, чтобы на него накопить, мошенники с радостью вам «помогут»! Они размещают в интернете множество объявлений о быстром и легком заработке. Но зачастую в таких случаях внезапно разбогатеть удается только самим махинаторам.

Мошенники могут убедить вас вложить деньги в «сверхприбыльный проект» (спойлер – в финансовую пирамиду).

До выплат вкладчикам дело обычно не доходит. Собрав деньги с как можно большего числа людей, организаторы исчезают.

Порой обманщики предлагают «быстро заработать», просто зарегистрировавшись на сомнительном сайте. Надо только выполнять задания или делать букмекерские ставки. Для вывода «заработка» они просят оплатить комиссию. В итоге деньги вместе с данными карты оказываются в руках махинаторов.

9

Не верьте в легкие «выигрыши» в конкурсах

Нередко мошенники рассылают письма и сообщения, в которых обещают нежданный выигрыш или от имени популярных блогеров запускают рекламу «беспроигрышных лотерей». Но затем за доставку «приза» или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого надо пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь получает убытки.

Если организаторы конкурса просят что-либо оплатить, это повод насторожиться. Прежде чем пытать удачу в онлайн-розыгрышах, надо убедиться, что организаторы – не мошенники: почитать отзывы в интернете, новости (вдруг они уже замечены в скандалах).

Стоит проверить на официальной странице блогера, действительно ли он рекламирует этот конкурс, или он тоже стал жертвой мошенников.

10

Не используйте найденную на улице банковскую карту

Если вы нашли банковскую карту, то в соответствии со статьей 227 ГК РФ, Вы обязаны немедленно уведомить о находке лицо, потерявшее ее, и возвратить найденную вещь этому лицу. Если же владелец пластиковой карты вам не известен, вы должны заявить о находке в полицию или отделение банка.

При попытке оплатить что-нибудь в интернете, пароль придёт на номер телефона держателя. Почти везде предусмотрена двухфакторная аутентификация.

При попытке снять наличные вы попадёте на камеры видеонаблюдения, которыми оборудованы банкоматы.

За попытку взлома чужого счёта предусматривается штраф до 120 000 рублей, обязательные или исправительные работы либо лишение свободы до трех лет. Также уголовное дело может быть возбуждено за кражу.

10 советов по безопасности в Интернете от экспертов AV-Test

При использовании компьютера, планшета или смартфона, защищенное подключении к Интернету является необходимым условием безопасности. Следующие 10 советов от экспертов лаборатории AV-Test помогут легко избегать онлайн-угрозы, которые поджидают в Сети, а также позволят использовать интернет-сервисы и устройства без каких-либо проблем безопасности.

1. Используйте новейшую версию антивирусной программы.

Многие комплексные антивирусы предлагают эффективную защиту от троянов, вирусов и других вредоносных приложений. Сочетание антивирусной защиты, фаервола, спам-фильтра и других инструментов позволит защитить компьютеры, смартфоны и планшеты от дополнительных угроз из Интернета, например, от хакерских атак.

2. Своевременно устанавливайте обновления.

Онлайн атаки обычно нацелены на бреши в безопасности операционной системы, браузеров и популярных приложений. С помощью обновлений разработчики постоянно устраняют уязвимости в своих продуктах. Именно поэтому важно регулярно обновлять программы, в том числе и антивирусы. Защитные продукты постоянно получают информацию об обнаружениях вредоносных программ в Интернете. Обновления для Android, MacOS и Windows должны выполняться регулярно и своевременно.

3. Используйте безопасные пароли.

При выборе паролей, пользователи должны проявить свои творческие способности и должны создавать различные пароли для каждого аккаунта! Надежные пароль должен состоять минимум из 8 символов. Наиболее безопасная комбинация включает заглавные и строчные буквы, цифры и специальные символы. Легко запомнить пароли, состоящие из строки песни с добавлением года выхода композиции. Бесплатные менеджеры паролей также очень полезны при управлении большой коллекцией паролей. Естественно, никто не должен знать ваши пароли.

4. Зашифрованные подключения для безопасной передачи данных.

По возможности используйте зашифрованные подключения каждый раз при посещении Интернет-магазинов, Интернет-банкинга или почтового сервиса. Адрес зашифрованных подключений начинается с "https" вместо "http". Кроме того, браузеры показывают иконку замка при безопасных подключениях.

5. Соблюдайте меры предосторожности при использовании общественных сетей Wi-Fi.

Общественные сети Wi-Fi являются очень практичными, когда требуется зайти на сайт на короткое время или определить текущее местоположение с помощью смартфона. Тем не менее, они не подходят для Интернет-банкинга или передачи конфиденциальной информации. Пользователь не может знать, кто администрирует сеть и какие меры защиты предпринимаются. Именно поэтому рекомендуется совершать финансовые транзакции в защищенной домашней сети и по возможности избегать доступа к важным аккаунтам, если устройство подключено к публичной точке доступа. Если это сделать необходимо, то используйте виртуальные частные сети (VPN). В этом случае все передаваемые данные будут надежно зашифрованы.

6. Осторожно обращайтесь с личными данными.

Личная информация, которая предоставляется веб-сайтам и приложениям часто раскрывается и даже продается третьим лицам. Именно поэтому пользователи должны указывать как можно меньше личных данных, заполняя только требуемые поля. Обычно политика обработки данных указывается в общих условиях использования или в правилах соблюдения конфиденциальности онлайн сервисов, программ и приложений.

7. Остерегайтесь бесплатного.

При использовании бесплатных приложений и веб-сервисов пользователь должен всегда задавать себе вопрос, какую пользу указанная им информация может принести разработчикам. Очень часто пользователи «платят» за использование бесплатных приложений и сервисов своими личными данными, которые монетизируются поставщиками услуг. Например, пользователь может получать нежелательную рекламу на указанные номера телефонов и адреса электронной почты.

8. Используйте надежные источники.

Файлы, программы и приложения должны открываться или устанавливаться только если они загружены из достоверных источников. Новейшие версии браузеров и антивирусов предупреждают пользователя о посещении потенциально опасных ресурсов. Приложения лучше устанавливать из официальных магазинов приложений Google Play, App Store или из Магазина приложений Windows.

9. Регулярно создавайте резервные копии.

Всегда существует риск потери данных, даже если устройство не потеряно, не украдено или не уничтожено. В случае с троянами-вымогателями, резервные копии могут снизить риск вымогательства со стороны злоумышленников. Нужно регулярно создавать резервные копии важных данных на внешние диски с помощью специализированных программ. Некоторые программы для резервного копирования распространяются бесплатно.

10. Правильно удаляйте данные.

Прежде чем выбросить компьютер, телефон, жесткий диск или флешку, нужно надлежащим образом удалить все данные. Удаление данных с помощью собственных средств Windows, iOS и Android не является эффективной мерой, потому что в этом случае можно восстановить информацию. Безопасно удалить данные помогут специализированные программы, которые выполняют многократную перезапись случайным набором данных, что делает безуспешными попытки восстановления.