Муниципальное автономное дошкольное образовательное учреждение «Синеглазка»

Муниципального образования город Ноябрьск

# Памятка «Безопасность в интернете»

Подготовила: воспитатель гр.12 Пилюгина И.В.

Люди просто безудержно делятся личной информацией, доверяют сохранение паролей браузерам и ошибочно полагают, что Интернет — это нечто белое и пушистое. Интернет сегодня – это гораздо больше, чем просто общение с друзьями, социальные сети, игры, онлайн-покупки. Это открытая система информации, и если кажется, что вам нечего скрывать или ваша информация никому не нужна, вы глубоко заблуждаетесь. Любая информация о вас может быть использована не теми, кому она предназначалась.

Гораздо страшнее то, что абсолютно любая информация, которой мы ежедневно делимся с друзьями и близкими, может в любой момент оказаться у злоумышленников. Это не паранойя, это суровая реальность или скорее дань Интернету, и однажды она может обойтись слишком дорого.

Чтобы обезопасить себя от многих ненужных проблем, я предлагаю соблюдать хотя бы основные правила безопасности в Интернете, своеобразный кодекс.

**Контроль за личной информацией**

Старайтесь как можно меньше рассказывать о себе. Особенно это касается социальных сетей. Везде, где вы зарегистрированы, измените свои настройки конфиденциальности. Ваш профиль должен быть виден только вашим друзьям.

Каков главный девиз всех социальных сетей в принципе? «Неважно, что мы хотим узнать от вас, главное, что вы сами хотите рассказать о себе».

Главная опасность социальных сетей заключается в непринужденной публикации различной информации о себе.

**Надежный пароль**

Придумывайте сложные пароли, состоящие не только из букв и цифр, но и из символов. Хорошо, если ваш пароль содержит такие буквы как «Х» и «Ъ»: они плохо распознаются системой и редко используются при переборке паролей.

Не используйте один пароль на всех аккаунтах, лучше используйте вариацию пароля.

Старайтесь не переходить по ссылкам из личных сообщений. Скопируйте присланную ссылку и откройте ее в новой вкладке. Будьте бдительней, особенно если приложение просит полный доступ к вашей странице.

Везде, где это можно, старайтесь не указывать свои реальные данные, и не нужно заполнять поля, не являющиеся обязательными для регистрации.

**Электронная почта — ключ к безопасности**

Это очень важный пункт в борьбе за вашу безопасность. Более того, именно взломанный почтовый ящик — это ключ к несанкционированному доступу к разным сайтам от вашего имени. Будьте очень аккуратны с вашим паролем!

Если ваш почтовый ящик будет взломан, злоумышленник в считанные секунды изменит пароль ко всем вашим сервисам, где данный адрес использовался для регистрации.

Помните о важности сложного пароля и старайтесь как можно чаще менять пароль. Не разрешайте браузеру сохранять ваш пароль от почты!

**Безопасность в интернете**

- Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.
- Если заходите в соцсеть или почту с чужого компьютера, не забудьте разлогиниться.
- Выключайте Wi-Fi, когда им не пользуетесь. И себя защитите, и заряд батареи сэкономите. Обязательно отключите функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.
- Не доверяйте непроверенным Wi-Fi-соединениям, которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей.
- Не заходите в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице. Воспользуйтесь мобильным интернетом.
- Помните: банки, сервисы и магазины никогда не рассылают писем с просьбой перейти по ссылке, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные!
- Отключите Сири на айфоне. Скорее всего, вы ей не пользуетесь, а вот мошенники уже научились выводить деньги через интернет-банк голосовыми командами.
- Заведите несколько адресов электронной почты: личная, рабочая и развлекательная (для подписок и сервисов).
- Придумайте сложный пароль, для каждого ящика разный.
- Везде, где это возможно, включите двухфакторную аутентификацию.
- Регулярно меняйте пароли, обновляйте браузер и спам-фильтры.
- Установите и обновляйте антивирусные программы. Устаревшие версии не могут гарантировать защиту от вредоносного ПО. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.
- Кликать по ссылкам, пришедшим в сообщениях от незнакомых людей — верный способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного знакомого, поэтому лучше уточните, что такое он вам прислал и нужно ли это открывать.
- Не запускайте неизвестные файлы, особенно с расширением .exe
- Внимательно проверяйте адреса ссылок, логотипы, текст и отправителя сообщений.
- Никогда не отвечайте на спам.
- Если вам в мессенджер пришла просьба от знакомого с просьбой срочно выслать денег, ничего не отправляйте! Сначала перезвоните ему и удостоверьтесь, что аккаунт не был взломан злоумышленниками.
- Чтобы никогда не терять деньги на незаметных платежах, не покупать дополнительных услуг по ошибке и точно заплатить за нужные, всегда читайте правила перед тем, как поставить галочку напротив чекбокса «согласен» и перейти к оплате.

- Если в секретном вопросе вы указали девичью фамилию матери, которая сейчас есть в открытом доступе на ее страницах в соц.сетях, обязательно поменяйте секретный вопрос.
- Установите безопасный режим для ребенка. Для этого создайте отдельную учетную запись на сайте выбранной вами поисковой системы или используйте детские поисковики: Гогуль или Спутник.дети.
- Совет для пользователей Google Chrome, Firefox и Opera: если вы часто путешествуете и выходите в сеть с ноутбука в общественных местах, установите специальное расширение для браузера для безопасного выхода в интернет. Рекомендуем HTTPS Everywhere от Electronic Frontier Foundation (EFF). По умолчанию этот плагин обеспечивает безопасное соединение для Yahoo, eBay, Amazon и некоторых других веб-ресурсов. Вы также можете добавить сайты по вашему выбору.
- Постарайтесь ничего не покупать в социальных сетях, особенно с предоплатой. Мы вообще не рекомендуем переводить деньги на карту физических лиц (то есть, когда кто-то просто дает вам номер или реквизиты своей карты).
- Покупая в интернет-магазинах, сохраняйте здоровый скептицизм. Помните: цена не может быть слишком низкой, тем более, если вы рассчитываете приобрести оригинальную продукцию бренда.
- Изучите историю магазина в сети, проверьте наличие контактов, выясните, можно ли туда приехать и познакомиться вживую. Читая отзывы, обратите внимание, чтобы они были разными. Заказные отзывы пишут люди, которым приходится делать это много раз в день, поэтому такие тексты будто написаны по шаблону.
- Посмотрите, как на отзывы реагируют продавцы. Обратите особое внимание на
- негативные: если их отрабатывают, это хороший знак (причем ситуация должна быть конкретная, содержать номер заказа и т.п.).
- Заведите отдельную (можно виртуальную) карту для платежей в интернете.
- Если для оплаты в интернете вы пользуетесь своей обычной картой, не храните на ней крупные суммы денег.
- Подключите в своем банке СМС-информирование о всех операциях по картам и счетам. Так вы сможете быстро заметить, если ваша карта будет скомпрометирована, и заблокировать ее.
- Страницы ввода конфиденциальной информации любого серьезного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета.
- Куда обращаться, если что-то пошло не так? Деятельность интернет-магазинов контролируется теми же организациями, что и обычных: Роспотребнадзором, Обществом защиты прав потребителей. Обязательно напишите на Горячую линию Рунета: www.hotline.rocit.ru
- Будьте осторожны при общении в сети с незнакомыми, они могут оказаться не теми, за кого себя выдают.
- Не делайте репостов жалостливых объявлений про милого котика, который срочно ищет дом (а в посте — телефон владельца или номер карты, куда можно перечислить деньги на содержание животного). Велика вероятность, что это мошенники, решившие заработать на сердобольных и доверчивых гражданах.
- Логотип известного благотворительного фонда еще не означает, что деньги пойдут туда — реквизиты счета могут быть подделаны. Если хотите помогать людям, делайте это только для лично знакомых или, например, с проектом dobro.mail.ru.
- Не покупайте авиабилеты на незнакомых сайтах, особенно если они стоят гораздо дешевле, чем на всех остальных. Зайдите на настоящий билет.рф и удостоверьтесь

в подлинности ресурса. Также не лишним будет посетить сайт авиакомпании, которой вы хотите улететь, и сравнить цену билета на нужное направление.

- Обращайте внимание на адрес страницы, где вы оказались: если он отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), введите его вручную самостоятельно.
- Если на смартфоне появилась надпись «Вставьте сим-карту», срочно зайдите в ближайший офис вашего мобильного оператора или позвоните ему с другого телефона и выясните, в чем проблема. Возможно, кто-то получил дубликат вашей симки и ее нужно срочно заблокировать.
- По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт. Злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.
- Потеряли телефон, к которому привязана банковская карта? Срочно блокируйте и симку, и карту.
- Лучше не пользоваться торрентами: если вы скачиваете нелегальный контент, вы не только обкрадываете любимого автора, но и можете загрузить зараженный вирусом файл.
- Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть или скачать приглянувшийся фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.
- Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего вы должны самостоятельно отключить услугу. Если вы этого не сделаете, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.
- Всегда блокируйте экран компьютера, даже если отходите «всего на минуточку».

Подготовила: Пилюгина И.В.