Правила кибербезопасности:

По национальному проекту «Цифровая экономика» в России появилась программа информирования о рисках в интернете и способах их избежать. Особое внимание уделяется детям и подросткам

Shutterstock

В интернете мы работаем и общаемся с друзьями, оплачиваем счета и смотрим кино, оформляем документы и выбираем, куда поехать в отпуск, заказываем пищу и узнаем оценки ребенка. Проще сказать, активно делимся информацией о себе в сети - указываем имя, вводим номер телефона, данные паспорта или банковской карты, однако риск того, что сведения попадут в нечестные руки, велик.

Как и в реальной жизни, далеко не все знакомые и тем более незнакомые люди, встречающиеся нам в интернет-пространстве, приходят с добрыми намерениями. Однако если знать и соблюдать простые и эффективные правила кибербезопасности, проблем можно избежать. А познакомиться с этими правилами поможет Всероссийская программа кибергигиены, которую Минцифры России запустило по национальному проекту «Цифровая экономика». Программа рассчитана на три года и направлена на формирование у граждан безопасного поведения в интернете. Помимо образовательных блоков, она также включает проведение всероссийского мониторинга уровня грамотности граждан по вопросам информационной безопасности. Результаты исследования позволят определить, с какими цифровыми угрозами люди сталкиваются чаще всего в зависимости от их возраста и привычек. Эта информация ляжет в основу проектов, чтобы интернет-пользователи узнали о наиболее актуальных для них угрозах и научились противостоять им. Доступ к первым проектам программы уже открыт для участников по всей стране.

На портале госуслуг появился новый раздел «Кибербезопасность - это просто!». Здесь пользователи смогут пройти тест и узнать, насколько хорошо они умеют распознавать типичные уловки интернет-мошенников и защищать свои данные.

Минцифры России и «РТК-Солар» подготовили статьи с рекомендациями, как обезопасить себя от самых распространенных проблем - от взлома аккаунта до сообщений с просьбой перевести деньги. На портале также появились описания распространенных мошеннических схем - вместе с советами, как правильно себя вести, чтобы не потерять деньги или персональные данные.

В раздел по кибербезопасности на «Госуслугах» вошли и ответы на вопросы, которые часто задают службе поддержки. Например, «как проверить, не подали ли мошенники заявление с моей учетной записи?». Теперь можно сразу получить всю необходимую информацию: по каким признакам есть шанс определить, что аккаунт был взломан, и какие неотложные меры следует предпринять.

- На портале госуслуг данные пользователей надежно защищены. Однако безопасность определяется не только уровнем защиты портала, но и инструментами, которые может применить сам пользователь: надежный пароль, двухфакторная аутентификация, выявление мошеннических фишинговых писем. Соблюдение всего нескольких простых правил безопасного поведения в интернете позволит предотвратить большую часть атак и существенно снизит объем финансового ущерба как для каждого отдельного гражданина, так и государства в целом, - подчеркнул **директор Департамента обеспечения кибербезопасности Минцифры России Владимир Бенгин.**

- Мы планируем по-настоящему масштабную всероссийскую программу по борьбе с киберугрозами. Цифровых атак на граждан с каждым годом становится все больше, постоянно появляются новые сценарии мошенничества в интернете, поэтому очень важно давать людям практические инструменты защиты. Проект на «Госуслугах» - это не только эффективный способ донесения до граждан основных правил кибербезопасности, но и хороший пример для всех крупных организаций, работающих с финансовыми транзакциями и чувствительными данными граждан. Каждый интернет-ресурс с большой аудиторией должен иметь раздел с подробными правилами безопасного использования его сервисов. Это забота о пользователях и просто необходимая мера в современных реалиях, - считает **генеральный директор «РТК-Солар» Игорь Ляпунов.**

Сетевой ЗОЖ

В СЕТИ, КАК И В ПИТАНИИ, ОЧЕНЬ ВАЖНЫ ПОЛЕЗНЫЕ ПРИВЫЧКИ

Основная идея проекта «КиберЗОЖ» - побудить людей ознакомиться с правилами кибербезопасности и убедить их в том, что необходимо самим предпринимать действия для защиты в интернете.

Мы же чистим зубы каждое утро, несмотря на регулярные визиты к стоматологу? Точно так же и в интернете - антивирус, фильтры для спама и протоколы шифрования информации, безусловно, нужны. Но полезно и самим регулярно менять пароли и обращать внимание на странности в адресной строке сайта.

В рамках проекта создан сайт киберзож.рф, благодаря которому пользователи научатся основным правилам и привычкам цифрового ЗОЖа: как создавать надежные пароли, не попасться на фишинг и проверить сайт на безопасность.


Shutterstock

КОММЕНТАРИЙ ЭКСПЕРТА

Интернет-гигиену нужно изучать с детства

- На мой взгляд, кибербезопасности, правильному поведению в виртуальном пространстве, пониманию реальных рисков, которые возникают при столкновении с цифровым миром, нужно учить с детства, - считает **заведующий лабораторией медиакоммуникаций в образовании НИУ ВШЭ, автор курса «Основы безопасности в социальных сетях» Александр Милкус.** - Мы же, прежде чем сесть за руль, изучаем правила дорожного движения. Вот так и здесь - нужно обучение и для школьников, и для их родителей тому, как себя вести в сети, чтобы не накликать беду.

Это только на первый взгляд кажется, что виртуальный мир - картинка на твоем ноутбуке или смартфоне. На самом же деле мы знаем о тысячах трагедий, связанных с наивным ощущением безопасности цифрового мира. От сломанных судеб, когда человек опрометчиво выложил в сеть личную информацию, а потом его затравили (или просто злоумышленники взломали аккаунт), до потери всех накоплений из-за того, что с помощью фишинговой рассылки украли пароли. От принятия неправильных, ошибочных стратегических семейных решений, основанных на фейковой информации, до попадания под влияние, под манипуляции неких не самых, мягко говоря, законопослушных сообществ.

На самом деле виртуальному миру, которым мы активно пользуемся, не так много лет. Первые массовые смартфоны появились 15 лет назад. Но злоумышленники и всякого рода мошенники завелись во Всемирной паутине гораздо раньше. Жулики были уже в одной из первых социальных сетей - Classmates, а она была создана в 1995 году.

Поэтому, на мой взгляд, сегодня системное обучение цифровой гигиене, кибербезопасности - это важная социальная задача. И я бы подчеркнул, что задача перманентная, так как угрозы становятся все более изощренными, а мошенники - все более хитроумными.

Лилия СОКОЛЬНИКОВА.

ЦИФРЫ

65 млн россиян стали жертвами хакерских атак в 2022 году.

96% фишинговых атак идут через электронную почту.

80% угроз можно избежать, если соблюдать простые правила кибербезопасности.

57% россиян хотели бы узнать о том, как лучше защитить себя в интернете.

Дмитрий ГОЛУХИН/ Комсомольская правда

как вести себя в сети

КОНКРЕТНО

СОЗДАТЬ НАДЕЖНЫЙ ПАРОЛЬ

Создание надежных паролей для аккаунтов, электронной почты, мобильных приложений - одно из основных правил кибергигиены.

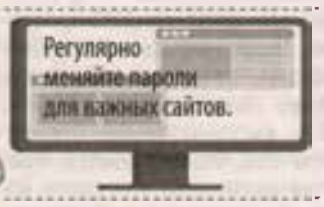
Да

Надежные пароли необязательно сложные для запоминания. Придумайте фразу, связанную с яркой и важной для вас историей или событием в жизни, привычкой или мечтой, и зашифруйте ее в виде пароля. Например, ОнаСказалаДА!15.02.12. Понятно только вам, а вы вряд ли забудете, когда сделали предложение руки и сердца.

Другие примеры паролей в этом стиле:
ГотовлюБорщ_на5+баллов!@
РекордПрохождения$
Цивилизации$-32часа _
Поеду1_вРио-де-Жанейро-
вБелыхШт@н@х

Длина пароля - 12 или более символов.

Используйте верхний и нижний регистры, числа и символы.



Храните пароли в специальных программах - менеджерах паролей.

Нет

Не подходят очевидные данные, которые легко узнать из ваших соцсетей: дата или место рождения, фамилия или имена детей.

Короткие пароли. Взломать любой пароль длиной до 6 символов хакеры смогут меньше чем за 2 секунды.

Не составляйте пароль из простых комбинаций букв и чисел, последовательных комбинаций клавиш, таких как qwe123.

Не используйте одинаковые пароли для всех своих аккаунтов и сайтов, особенно связанных с деньгами и большим количеством личной информации: соцсетей, госуслуг, интернет-банков. В этом случае злоумышленникам достаточно будет взломать пароль один раз, и они получат доступ ко всем вашим аккаунтам.

Не храните пароли на бумаге, в заметках на смартфоне, в электронной почте и браузерах.

Дмитрий ПОЛЯКИН/«Комсомольская правда»

Не делайте так!

123456 - самый популярный пароль среди пользователей Рунета. Также в списке очень часто используемых и абсолютно ненадежных - qwerty123, a11111, «пароль» и «любовь».

59% пользователей используют один и тот же пароль для всех аккаунтов.

Как не попасться на удочку фишинга

Фишинг - очень распространенный вид кибермошенничества, цель которого получить данные пользователя. В том числе пароли и номера банковских карт. Простые правила помогут не попасться на уловки.

1 Когда заходите на сайт, особенно по ссылке, проверьте написание адреса. Часто мошенники меняют всего одну букву. Например, https://www.gossuslugi.ru/ вместо https://www.gosuslugi.ru/ - мало кто обратит внимание на двойную «s». Или указывают другой домен - вместо .ru, например, .su или .org. А в остальном адрес правильный, поэтому легко не заметить подвоха. Надежнее всего вручную вводить название сайта в адресной строке.

2 В электронной почте обращайте внимание, с какого адреса пришло письмо. Увидели что-то вроде bank@mail.ru - тревога! Банки и другие организации не присылают письма с общедоступных почтовых сервисов, таких как @mail.ru, @gmail.com и другие. Злоумышленники нередко имитируют письма от админов социальных сетей и интернет-магазинов. В письме просят сменить пароль. При переходе по ссылке вы окажетесь на сайте, который оформлен как настоящий интернет-сервис. На странице предложат ввести старый пароль и придумать новый. Таким образом реальный пароль от вашего аккаунта окажется у мошенников. При необходимости меняйте пароли через личный кабинет, а не по ссылке из письма.

3 Фишинговыми могут быть также сообщения в мессенджерах, социальных сетях и СМС. Вы выиграли деньги, вам положена выплата от государства, срочно нужна ваша помощь - чаще всего заманивают подобными темами. При переходе по ссылке откроется фейковый сайт, где предложат ввести данные банковской карты. Мошенники получат доступ к вашей карте и могут списать с нее деньги. Уведомление из банка или от онлайн-магазина можно проверить, позвонив по телефону с официального сайта.

4 Не скачивайте файлы из непроверенных источников, в том числе приложения для смартфонов. Под видом бесплатных программ могут маскироваться вредоносные, нацеленные на кражу ваших данных, подписку на платные услуги, сбор информации в рекламных целях или доступ к корпоративной сети, если взламывают рабочий компьютер.

5 Минимизируйте использование открытого Wi-Fi. Особенно если вам предлагают зарегистрироваться через аккаунт социальных сетей или «Госуслуг». При подключении к публичным сетям включайте VPN-сервисы, благодаря им весь трафик будет передаваться в зашифрованном виде.

ВАЖНО

ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛИ ЖЕРТВОЙ ТРАВЛИ

- Тролли ждут, когда жертва начнет оправдываться, поэтому пытаться аргументированно общаться бесполезно. Лучше отвечать с юмором и даже абсурдной логикой. Или вообще игнорировать.
- Лучше не замыкаться, а рассказать друзьям, родителям, поговорить с психологом и обратиться в техподдержку соцсети.
- Обидчиков можно заблокировать или добавить в черный список.

КСТАТИ

Если в адресе в самом начале стоит https://, а не http:// - это хороший знак. Скорее всего, транзакции на таком сайте защищены криптографическим протоколом, который в идеале не может вскрыть даже администратор сайта или провайдер. Это называется SSL - Secure Sockets Layer. Подлинность SSL-сертификата и срок его действия легко проверить на специализированных сайтах. И лучше это сделать, прежде чем совершать покупку.

Опыт педагога

Первое, с чего мы начинаем обучение, - безопасность в сети

- Интернетом дети пользуются всегда, очень редкий школьник не сидит в телефоне на переменах. Они чувствуют себя неотделимыми от интернета и не всегда понимают, где граница между обыкновенной жизнью и жизнью в сети, - делится своим опытом **педагог дополнительного образования, куратор медиаклассов московской школы № 1517 Екатерина Ощепкова.** - Мы часто видим, как на детской площадке мама разговаривает по телефону, а рядом ребенок играет на планшете. Родители дают гаджеты детям для развлечения, не понимая, что так формируется образ жизни в интернете.

Уроки медиаграмотности и безопасности в интернете надо вводить с раннего детства. Первое, с чего мы начинаем обучение, - это безопасность в сети. Говорим о самых базовых темах: как защищать личные данные в интернете, как этично общаться и даже просто о том, что верить на слово в интернете никому нельзя. Личные данные дети сообщают очень легко, в большинстве случаев их даже не приходится спрашивать - они сами могут разместить данные о родителях и о себе в соцсетях.

По моему опыту, как минимум каждый второй подросток, у которого есть личные деньги и тем более своя банковская карта, попадал на мошенников. Чаще всего - на продажах и покупках в соцсетях: договариваются о каких-то брендовых вещах, переводят деньги, а дальше им никто не отвечает.

Надо показывать, как это работает, чтобы дети понимали, какая информация о них видна другим людям в интернете, как их можно вычислить через друзей по соцсетям и комментариям.

Может показаться, что это очевидные вещи, но на самом деле нет. О них обязательно нужно говорить, и делать это нужно в школе, так как редко в какой семье учат детей кибербезопасности. Обычно об этом рассказывают учителя информатики или педагоги дополнительного образования.

Для взрослых, конечно, тоже важны знания о безопасности в сети - их как раз и призваны дать новый раздел на «Госуслугах» и другие программы федерального проекта «Информационная безопасность».

- Взрослые люди в интернете - мигранты. А дети уже аборигены и иногда разбираются в нем лучше, - считает Екатерина Ощепкова. - Как-то я наблюдала, как пятиклассник подсказывал маме, чтобы она не вводила данные банковской карты, так как сайт небезопасный. Просвещение должно быть обязательно и для взрослых, и для пенсионеров в том числе - к сожалению, пожилые люди первыми попадаются на уловки мошенников.

Против буллинга

Кибербуллинг, или травля в интернете, - это оскорбления и угрозы в социальных сетях и мессенджерах. И проблема эта гораздо масштабнее, чем кажется. А последствия кибербуллинга для детей сравнимы с реальной травлей - вплоть до депрессии и проблем с учебой.

Основная идея проекта «Кибербуллинг» - объяснить детям и подросткам, что такое кибербуллинг и как правильно себя вести, если стали жертвой или свидетелем травли. Авторы проекта разработали специальные стикерпаки для оригинального ответа агрессору. А популярные блогеры рассказывают на своем примере, как справились с травлей в сети.

- Мы считаем очень важным запуск проекта по кибербуллингу и надеемся, что он позволит повысить грамотность подростков в цифровой среде и снизить эффективность травли с использованием цифровых технологий, - считает **проректор по цифровой трансформации Санкт-Петербургского государственного университета телекоммуникаций им. профессора М. А. Бонч-Бруевича Антон Зарубин.**

ВАЖНО!

- *55% подростков сталкивались с травлей в сети.*
- *46% буллеров ведут себя агрессивно ради развлечения.*

ТРИ САМЫХ ЧАСТЫХ ПОВОДА ДЛЯ БУЛЛИНГА В ИНТЕРНЕТЕ:

- ВНЕШНОСТЬ
- ЛИЧНЫЕ ОСОБЕННОСТИ
- НАЦИОНАЛЬНОСТЬ

Дмитрий ПОЛЯКИН/«Комсомольская правда»