Памятка по основам кибербезопасности для клиентов
ООО ПКО «АБК»

1. Используйте надежное Интернет-соединение.

Мы не рекомендуем использовать публичные сети Wi-Fi. Выходя в интернет через общественную сеть Wi-Fi, вы не контролируете ее безопасность, а значит, легко можете стать целью для злоумышленника. В этих случаях рекомендуется избегать выполнения операций с использованием персональных данных – в частности, пользоваться услугами интернет банка и совершать покупки онлайн.

2. Используйте надежные пароли.

Пароли – одно из самых слабых мест в системе кибербезопасности. Пользователи часто создают пароли, которые легко запомнить и злоумышленникам не составляет труда подобрать их с помощью специальных программ. Используя один и тот же пароль для нескольких учетных записей, вы подвергаете свои данные еще большему риску, ведь, получив учетные данные от одного сайта, злоумышленники смогут войти и в другие ваши аккаунты.

Выбирайте надежные пароли, которые сложно подобрать.

Надежный пароль обладает следующими свойствами:

• Длинный: минимум 12 символов, в идеале даже больше.

• Сложный: содержит заглавные и строчные буквы, а также специальные символы и цифры.

• Не очевидный: в пароле не используются последовательные цифры (1234) и личная информация, которую легко узнать или найти в интернете (ваш день рождения, имя домашнего животного и так далее).

• Случайный: не содержит запоминающихся сочетаний клавиш.

В этом случае может быть полезным использование менеджера паролей. Менеджеры паролей помогают создавать надежные пароли, хранить их в цифровом хранилище, защищенном единым мастер-паролем, и автоматически подставлять их при входе в учетные записи.

Мы рекомендуем менять пароль не реже чем один раз в 3 месяца.

3. По возможности включите многофакторную аутентификацию.

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используются два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация:

• Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или адрес электронной почты.

• Ответы на личные вопросы безопасности.

• Отпечаток пальца или другая биометрическая информация, например, голосовые данные или распознавание лица.

Многофакторная аутентификация снижает вероятность успеха кибератаки.

Чтобы защитить онлайн-аккаунты, мы рекомендуется возможности использовать многофакторную аутентификацию.

4. Обновляйте программное обеспечение и операционную систему.

Разработчики постоянно работают над безопасностью продуктов, отслеживая последние угрозы и выпуская исправления безопасности в случае обнаружения уязвимостей в приложениях. Используйте последние версии операционных систем и приложений, чтобы не пропускать свежие обновления безопасности. Это особенно важно для приложений, содержащих платежные данные, сведения о состоянии здоровья и прочую конфиденциальную информацию пользователя.

5. Убедитесь в надежности сайта.

Надежность – важный атрибут всех посещаемых веб-сайтов, особенно тех, на которых осуществляются транзакции. В частности, сайтов электронной коммерции. При переходе на неизвестный сайт проверьте, защищен ли он SSL-сертификатом. Адреса таких сайтов начинаются с HTTPS вместо HTTP (буква S означает «безопасный»), а в адресной строке отображается значок замка. Другие признаки надежности сайта включают:

• Грамматически правильный текст без орфографических и пунктуационных ошибок. Авторитетные бренды прикладывают значительные усилия для обеспечения надлежащего качества своих веб-сайтов.

• Качественные изображения, соответствующие ширине экрана.

• Объявления, органично вписанные в структуру сайта и не перегружающие его.

• Единообразное цветовое оформление и выдержанная тема. Едва заметные изменения цветовой гаммы или стиля страницы, на которую вы возвращаетесь после перехода по ссылке, могут быть признаком мошеннического сайта.

• Согласно отраслевым требованиям, все онлайн-транзакции по кредитным и дебетовым картам должны проходить через платежный шлюз. Если вам предлагают перечислить деньги иным способом, вероятно, это мошенники.

6. Проверьте настройки приватности и ознакомьтесь с политиками конфиденциальности.

Маркетологи, как и злоумышленники, хотят знать о вас все. Они могут получить эту информацию из истории поисковых запросов и социальных сетей. Но вы можете контролировать доступную им информацию. В веб-браузерах и мобильных операционных системах предусмотрены параметры

для обеспечения конфиденциальности в интернете. На сайтах социальных сетей предусмотрены параметры обеспечения конфиденциальности, которыми вы можете управлять. Мы рекомендуем разобраться с параметрами конфиденциальности и настроить учетные записи так, как вам комфортно.

Многие принимают условия политики конфиденциальности, не читая, однако огромное количество данных обрабатывается в маркетинговых, рекламных, а также преступных целях, поэтому рекомендуется ознакомиться с политиками конфиденциальности используемых веб-сайтов и приложений и понять, как осуществляется сбор и анализ данных. Но даже если вы закрыли посторонним доступ к своим данным, не следует забывать, что обеспечить полную конфиденциальность в интернете практически невозможно, но это определенно снизит риски получения злоумышленниками ваших данных.

7. Следите, по каким ссылкам вы переходите.

Один неосторожный переход по ссылке - и ваши личные данные могут попасть к злоумышленникам или устройство может заразиться вредоносной программой. Поэтому важно следить за тем, по каким ссылкам вы переходите, и избегать определенных типов контента: ссылок из ненадежных источников, спам-сообщений, онлайн-викторин, кликбейтных заголовков, «бесплатных» предложений и нежелательной рекламы.

При получении электронного письма, в подлинности которого вы сомневаетесь, не переходите по содержащимся в нем ссылкам и не открывайте вложения.

Если вы не уверены в подлинности электронного письма, обратитесь непосредственно к отправителю. Например, при получении подозрительного письма якобы из вашего банка позвоните в банк и спросите, действительно ли письмо пришло от них.

При просмотре сайта убедитесь, что переход по ссылкам осуществляется на страницы со связанным или ожидаемым содержимым. Например, если вы переходите по ссылке на описание сафари в Африке, но вместо этого попадаете на кликбейтную страницу о том, как похудели знаменитости, или на статью с заголовком «Где они сейчас?», немедленно покиньте эту страницу и не вводите никакие свои данные.

8. Убедитесь, что ваши устройства защищены.

Около 60% пользователей используют мобильные устройства для совершения покупок и поиска информации в интернете гораздо чаще, чем компьютеры, и такие устройства должны быть надежно защищены. Рекомендуется использовать пароли, секретные коды и другие средства безопасности, такие как считывание отпечатков пальцев или технологию распознавания лица на всех устройствах: телефонах, компьютерах, планшетах, умных часах, умных телевизорах и других устройствах. Эти меры безопасности снизят вероятность кибератаки или кражи ваших личных данных.

9. Регулярно выполняйте резервное копирование.

Следует иметь резервные копии важной личной информации на внешних жестких дисках и регулярно создавать новые резервные копии. Программы-вымогатели – это тип вредоносных программ, блокирующих компьютер и не позволяющих получить доступ к важным файлам. Резервное копирование данных помогает минимизировать негативные последствия атак программ-вымогателей, а специальное ПО для защиты повысит уровень вашей безопасности. Есть и другие типы вредоносных программ, которые блокируют доступ к персональным данным, создавая чрезмерную нагрузку на систему, или просто удаляют файлы.

10. Удалите неиспользуемые учетные записи.

У многих есть учетные записи, которые давно не используются. Их наличие может стать источником уязвимостей при использовании интернета. Старые учетные записи часто имеют более слабые пароли, а сайты, на которых они использовались, могут иметь ненадежную политику защиты данных. Кроме того, по данным в старых профилях социальных сетей злоумышленники могут собрать о вас различные данные, например, дату рождения и местонахождение, и использовать их для последующей кибератаки.

11. Будьте осторожны с загрузками.

Цель злоумышленников - заставить вас скачать вредоносную программу, которая откроет им доступ к вашему устройству. Вредоносные программы могут быть замаскированы под любое ПО, начиная с популярных игр и заканчивая приложениями для проверки погоды или наличия пробок на дороге. Кроме того, они могут быть скрыты на созданных злоумышленниками веб-сайтах, которые пытаются установить вредоносные программы на ваше устройство.

Вредоносные программы наносят ущерб: нарушают работу устройства, крадут личные данные, предоставляют несанкционированный доступ к компьютеру. Обычно для загрузки вредоносных программ требуется ряд действий со стороны пользователя, но встречается также заражение путем скрытой загрузки, когда веб-сайт пытается установить вредоносные программы на компьютер, не спрашивая предварительного разрешения. Будьте осторожны при переходе на неизвестный сайт и при загрузке объектов на устройство, загружайте контент только из надежных или официальных источников. Регулярно проверяйте папки загрузки и немедленно удаляйте неизвестные файлы – они могли попасть на ваше устройство в результате скрытой загрузки.

12. Будьте осторожны с публикациями.

В интернете нет возможности удаления опубликованной информации. Все опубликованные комментарии и изображения могут навсегда остаться в

Сети, поскольку при удалении оригинала вы не удаляете копии, которые могли сделать другие пользователи. После публикации комментария уже нет возможности «взять свои слова обратно», также невозможно удалить опубликованное компрометирующее изображение.

И будьте осторожны, публикуя личную информацию в интернете: не указывайте номер социального страхования, адрес и дату рождения в профилях социальных сетей. В реальной жизни вы бы не стали сообщать личные данные незнакомцам, и точно так же не следует публиковать их в интернете и делать доступными миллионам пользователей.

Соблюдайте осторожность при предоставлении адреса электронной почты. Полезно иметь дополнительную временную учетную запись электронной почты, используемую исключительно для регистрации и подписки. Она должна отличаться от рабочей и от используемой для переписки с друзьями и близкими.

13. Перепроверяйте информацию, найденную в интернете.

К сожалению, в интернете присутствует большое количество поддельных новостей и ложных сведений. В потоке получаемой ежедневно информации легко потеряться. Если вы сомневаетесь в достоверности прочитанной информации, проведите собственное исследование и установите реальные факты. На надежных веб-сайтах, как правило, приводятся ссылки на первоисточники. а на подозрительных страницах вообще не приведено никаких ссылок.

14. Используйте хороший антивирус и регулярно обновляйте его.

Помимо соблюдения рекомендаций по обеспечению безопасности в интернете, важно использовать надежное антивирусное решение. Программное обеспечение для безопасности в интернете защищает устройства и данные и блокирует не только распространенные угрозы, такие как вирусы и вредоносные программы, но и комплексные атаки с использованием приложений-шпионов, шифровальщиков и межсайтового скриптинга. Как и в случае с операционными системами и приложениями, антивирус необходимо регулярно обновлять, чтобы получать защиту от новейших киберугроз.