Правила безопасности в социальных сетях

2 ГЛАВА

Социальные сети, блоги, публичные авторские каналы, мессенджеры — самые посещаемые интернет-ресурсы. Здесь размещается много личной информации, всегда есть возможность напрямую пообщаться с человеком. Поэтому их часто используют мошенники для кражи личных данных. Статистика показывает, что ежедневно в различных социальных сетях появляется до 750 тыс. злоумышленников. Чтобы обезопасить себя, нужно соблюдать простые правила.

Некоторые правила безопасности и примеры мошеннических схем можно найти в главе 3 «Как действуют мошенники в интернете, способы защиты» модуля 10 «Кибербезопасность».

Не размещайте на своей странице:

1. Номер домашнего, рабочего и мобильного телефона.
2. Точный адрес места жительства.
3. Паспортные данные.
4. Планы о поездках с указанием даты.
5. Электронные билеты на мероприятия.
6. Пароли и логины от своих личных страничек.
7. Данные банковских карт.
8. Информацию о ценных вещах, которые хранятся у вас дома.

Что интересует мошенников

В первую очередь — ваши личные данные. Любыми способами преступники стараются узнать данные вашей банковской карты (номер, ФИО владельца, срок действия, трехзначный CVV/CVC-код, который вводят для подтверждения платежа). Ценной информацией являются паспортные данные. Зная их, мошенник может действовать от вашего имени.

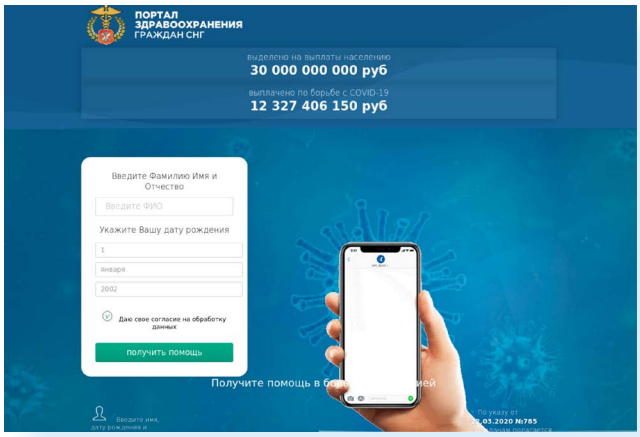
Чтобы получить нужную информацию, преступники могут звонить или писать пользователям, представляться работниками банка, социальной службы или оператора связи и просить подтвердить свои данные. При этом психологически главная задача — напугать и торопить пользователя (карта заблокирована, социальная выплата не будет оформлена, телефонная связь будет недоступна).

Кибермошенники могут присылать личные сообщения с просьбой перейти по ссылке. Зачастую это могут быть письма якобы от Социального фонда, банка или администрации социальной сети.

Чем чреват переход по такой ссылке? Либо вы активируете вирус в своем устройстве, который будет передавать нужную информацию мошеннику, либо попадете на фальшивый сайт, оформленный точно так же, как официальный сайт той или иной службы, где вам предложат ввести ваши личные данные. Есть вариант, что после ввода данных вас попросят подтвердить личность и перевести небольшую сумму на счет, куда вам якобы придет некая выплата.

Например, так работал мошеннический сайт «Портал здравоохранения граждан СНГ». Такого ресурса на самом деле не существует. А работал он следующим образом. Пользователь при переводе суммы на счет, во-первых, терял деньги, а во-вторых, введенные при оплате данные банковской карты тут же становились доступны мошеннику. Ниже — сайт мошенников, обещавший выплату гражданам 2.1.

2.1



Второй вариант — когда мошенники заставляют пользователя самого провести платеж. Как правило, преступники используют психологические приемы. Могут, например, прислать сообщения якобы от друзей или родственников, которые обращаются к вам за помощью. Ниже — один из таких примеров 2.2.

2.2

Может поступить сообщение или звонок от банка о том, что на вас оформлен кредит, и эту сумму срочно нужно заблокировать и перевести на специальный счет. В этом случае не предпринимайте никаких действий. Отключитесь от звонка и сами перезвоните в банк.

Киберворы часто охотятся за логинами и паролями от популярных страничек. Зачем им это? Чтобы завладеть страницей и от лица ее владельца делать рассылки. Это могут быть ссылки с вирусами или просьбы одолжить денег у друзей владельца странички. Надо сказать, что многие пользователи «ведутся» на такие просьбы давних знакомых. Им и в голову не приходит, что это пишете не вы — просто вашу страничку взломали.

В последнее время мошенники часто используют для звонков мессенджеры. Не отвечайте в мессенджерах на звонки с незнакомых номеров и не принимайте от них сообщения. Скорее всего, это реклама или мошенники.

Основные правила безопасной работы в сервисах общения

1. Не сообщайте о себе личную информацию: адрес места жительства, номера банковских карт, паспортные данные. Старайтесь не распространяться, с кем вы живете, когда уезжаете в путешествие. Лучше выкладывайте фото уже по возвращении из поездок.
2. Внимательно относитесь к ссылкам, которые вам присылает собеседник. В них может быть вирус или переход на поддельный сайт. Никогда не открывайте ссылки от незнакомых людей!
3. Если вам пишет знакомый с просьбой срочно перевести деньги, перезвоните ему лично или задайте уточняющий вопрос, имеющий отношение к вашему знакомству. Страничка вашего друга может быть взломана, и от его имени такие сообщения присылают мошенники.
4. Осторожно относитесь к предложениям от частных лиц что-то купить или продать. Как минимум, созвонитесь с этим человеком. Если это аккаунт какой-то компании, перейдите на ее сайт в интернете, свяжитесь с ее представителем. Почитайте отзывы.
5. От мошенников могут поступать предложения заработать. Не оплачивайте доступы к базам данных или какие-то услуги, которые якобы помогут вам найти хорошую работу — это 100% обман! Читайте отзывы об агентствах или компаниях, которые вдруг написали вам в личные сообщения с предложениями о работе.
6. Точно также внимательно отнеситесь к сообщениям о вашем внезапном выигрыше или полагающейся вам социальной выплате. Не переходите по ссылкам в сообщении. Почитайте отзывы о компании, предлагающей выигрыш в интернете. Информацию о социальных выплатах вы можете уточнить на Портале госуслуг.

На что еще обратить внимание?

Никогда не переходите на сайт по ссылкам, которые вдруг появляются на экране вашего компьютера и информируют о том, что ваша страничка в «Одноклассниках» или «ВКонтакте» взломана — это уловка мошенников!

Старайтесь не заходить с чужих компьютеров на свою страничку в соцсетях. А если возникла такая необходимость, то делайте это в браузере в режиме «Инкогнито». Тогда на компьютере не сохранятся ваши данные.

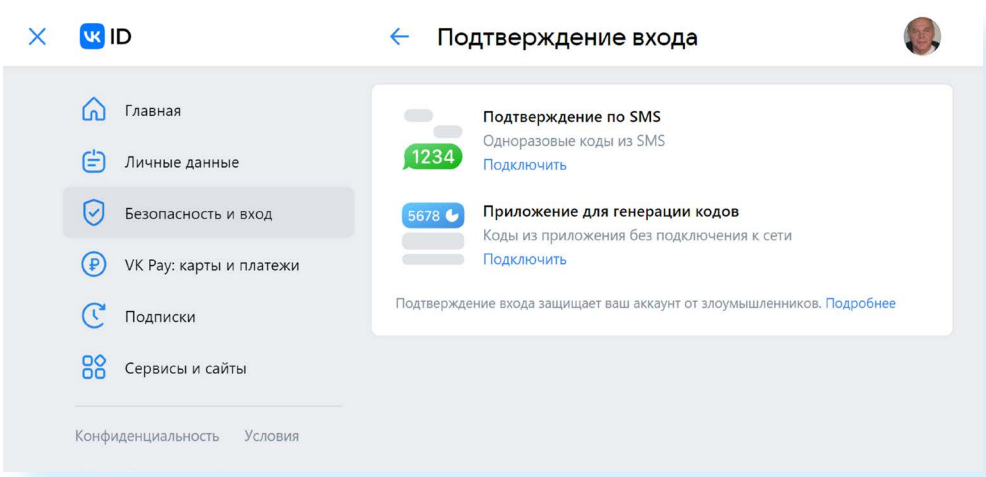
Внимательно относитесь к добавлению друзей. Старайтесь не добавлять незнакомцев.

Используйте настройки безопасности для своей странички. Например, включите двухфакторную аутентификацию или дополнительное подтверждение входа по СМС. Это метод идентификации пользователя. Сначала система вас распознает по введенному логину и паролю, а затем просит дополнительное подтверждение, что это именно вы, и, например, вышлет код в СМС-сообщении на привязанный к страничке номер телефона. Вы должны будете ввести код в обозначенное поле, и система пропустит вас на страничку.

Например, во «ВКонтакте», чтобы настроить такую дополнительную проверку, нужно:

1. Вверху справа нажать на значок аккаунта.
2. Выбрать «Настройки».
3. Далее выбрать раздел «Безопасность».
4. Затем кликнуть надпись «Перейти в VK ID».
5. В блоке «Подтверждение по СМС» нажать «Подключить».
6. Далее нажать «Начать настройку».
7. На следующей странице указать текущий пароль от профиля «ВКонтакте».
8. Подтвердить, что вы — владелец аккаунта и следовать инструкциям на экране 2.3.

2.3



Здесь же в разделе «Безопасность» можно посмотреть историю активности, когда и с какого браузера был выполнен вход на вашу страничку.

Как правило, если в ваш аккаунт попытаются зайти с другого, система предупредит вас. Если заподозрили, что кто-то вошел в ваш аккаунт, вы можете удаленно выйти со своей странички на всех устройствах, кликнув «Завершить все сеансы».

Стоит настроить видимость на вашей страничке. «ВКонтакте» для этого нужно перейти в «Настройках» в раздел «Приватность». Вы можете настроить свою страничку так, что отдельная информация будет видна только вам, или вам и вашим друзьям. Например, можно свою страничку сделать закрытой, принимать сообщения и комментарии только от друзей.

Но если вы ищете людей, с которыми потеряли связь, или ведете публичную страничку своего проекта, взаимодействовать пользователям с вами будет труднее. Но вы всегда можете регулировать и менять настройки доступности данных на вашей странице в зависимости от ситуации и обстоятельств.

Однако никогда не стоит терять бдительность. Перепроверяйте информацию и не делитесь личными данными!

О правилах безопасной работы в интернете — в главе 6 «Безопасная работа в Сети интернет».

Контрольные вопросы

1. Почему в социальных сетях нужно особенно внимательно соблюдать правила безопасности?
2. На какие настройки своей публичной страницы стоит обратить внимание?
3. Какую личную информацию в целях безопасности не нужно размещать на своей странице в социальных сетях или блоге?
4. Ваш знакомый прислал вам странную ссылку сообщением в социальных сетях. Ваши действия?
5. Почему не стоит делать покупки у частных пользователей в социальных сетях?
6. Как могут действовать мошенники в сервисах общения?