28 января

Международный день защиты персональных данных. Как защититься от мошенничества

С развитием интернета появляются новые и развиваются уже известные схемы мошенничества через сеть. Не попадайтесь на уловки преступников, и помните о защите персональных данных. Какие способы чаще всего используют мошенники и как им противостоять — читайте в этом материале.

1. Звонок из банка

Этот вид мошенничества наиболее популярен в последнее время, только за первое полугодие 2020 года количество таких звонков увеличилось на 30%. По оценкам экспертов, ежегодно мошенники, представляясь сотрудниками банков, воруют миллиарды рублей, большая часть средств уходит в следственные изоляторы, тюрьмы, колонии.

Опасайтесь мошенников! Рисунок: depositphotos, Margorita

Как это происходит

Потенциальной жертве звонят, представляясь службой безопасности банка. Довольно часто обращаются по имени. Возможно несколько вариантов диалога:

- *С вашей карточки происходит подозрительное списание средств;*
- *У нас произошел технический сбой и нам надо восстановить ваши данные.*

Схема действий варьируется: жертву вынуждают назвать не только номер карты, но и ПИН- или CVV-код, СМС-пароли банка, логин и пароль для входа в онлайн-банк, контрольную информацию (кодовое слово). Иногда призывают подойти к ближайшему банкомату и совершить определенные действия.

Звонок поступает с номера, похожего на номер банка или даже с номера банка. Дело в том, что существуют программы, позволяющие менять номер, этой программой часто пользуются пранкеры, телефонные хулиганы, разговаривающие от имени другого лица.

Разговор имитирует диалог с банковскими сотрудниками, «клиента» переключают на «специалиста» или «сотрудника правоохранительных органов», который сообщает, что проводится операция по задержанию мошенников, а сопротивление оперативной работе может расцениваться как правонарушение. При этом жертве не дают времени, не дают возможности отключиться, все это притупляет внимание, отключает способность критического мышления, вызывает страх.

Как противостоять?

Многие просто не отвечают на звонки с неизвестных номеров, но если вы ответили, помните, сотрудники банка не будут интересоваться вашими секретными данными, не будут просить сообщать код СМС. Если вам не дают возможности отключиться и перезвонить позже – с вами разговаривают мошенники.

Никогда не переходите по ссылкам в СМС, электронных письмах или размещенных на рекламных баннерах.

В августе Альфа-банк провел своеобразное тестирование. Он разместил в соцсетях рекламный баннер, где обещал 2020 рублей всем, кто перейдет по ссылке. За 3 дня перешли на сомнительный сайт 20 тысяч человек.

2. Доступ к персональным данным при поиске работы

Набирающий популярность способ получить доступ к вашим персональным данным. Вы ищете работу и получаете заманчивое предложение, но для доступа к контактам или документам, вам необходимо скачать приложение, которое размещено в официальном магазине. Приложение заражено вирусом, открывающим доступ к управлению вашего компьютера, а это значит и доступ к электронным кошелькам, мобильным банкам и прочим данным.

При этом приложение может быть размещено в магазине PlayMarket, куда одно из них, зараженное вирусом, предварительно загрузили мошенники.

Это новый вид мошенничества, так как зараженная программа устанавливается с официальных магазинов. Эксперты оценивают высокую вероятность риска того, что эта схема в ближайшее время станет массовой, ведь потенциальные жертвы — люди, нуждающиеся в работе.

Google уверяет, что во всех Android-смартфонах работает система безопасности «Google Play Защита», которая проверяет приложения во время установки.

3. Продажа на интернет-площадках

Вы выставили на продажу вещь на «Авито», «Юле» или подобной площадке. Покупатель предлагает вам отправить товар с таксистом, а деньги за покупку он готов перевести на вашу карту. При этом он спрашивает не только номер карты, но и дату выдачи, фамилию и имя владельца, код CVC. Иногда требует и код SMS. Объясняет тем, что оплата идет с расчетного счета предприятия, а данные нужны для отчетности.

> *Никогда не сообщайте дополнительных сведений, для перевода на карту нужен только ее номер. Вас может насторожить, что покупатель мало интересуется приобретаемой вещью, а несколько дополнительных вопросов продемонстрируют полную незаинтересованность и некомпетентность «покупателя».*

4. Взлом аккаунтов в мессенджерах и соцсетях

Если в личку соцсети или мессенджера пришло сообщение от друга с просьбой денег, какими бы обстоятельствами это ни объяснялось — не спешите сразу же на помощь. Свяжитесь с другом по телефону, через аккаунт в другой соцсети или любым другим доступным вам способом.

На этой системе построены целые мошеннические корпорации. Письма пишут так, что сразу и не заподозрить, что это другой человек — он использует привычные вам обороты слов и общается в привычном вам сценарии, т.к. вся предыдущая переписка была изучена, и на ее основании составляется схема вымогания денег. И так распишут ситуацию, что сразу хочется броситься на

помощь. Конечно, бывают у них и «проколы». Однажды в скайпе «ожил» аккаунт недавно погибшей коллеги. От ее лица мошенники начали вести диалог со всеми, до кого смогли дотянуться...

Как противостоять?

Если вы не уверены, что это мошенники, и хочется помочь другу, но нет возможности связаться иным способом — задайте несколько тестовых вопросов, на которые посторонний человек ответов знать не будет. Про общих друзей, родственников, про место нахождения. Скажите, что наберете его вечером или попросите связаться с вами другим способом.

Самозащита в таких вопросах — это техника собственной финансовой безопасности. Помните, что мошеннические схемы выстроены хитрым образом, и полиция едва ли сможет разобраться. И если вы попались — с деньгами придется попрощаться.

Елена Гвозденко
Специально для Журнала Calend.ru
