Информация для размещения

на сайтах администрации, в СМИ

11.10.2023 г.

**Распространенные виды мошенничества и методы защиты от них.**

Ранее мы обсуждали как вести себя, чтобы не стать жертвами мошенников? А чтобы научиться еще эффективнее противостоять злоумышленникам, давайте рассмотрим наиболее распространенные виды мошенничества и методы защиты от них.

1. **Если вам поступают неожиданные СМС – сообщения, электронные письма и звонки.**

- Вы получили сообщение якобы от родственника или друга, попавшего в беду, с просьбой о переводе денег. Свяжитесь с отправителем сообщения напрямую и уточните ситуацию.

- Вы получили сообщение или письмо от имени вашего банка с информацией о том, что ваша карта заблокирована или перевыпущена. Позвоните в свой банк по телефонному номеру, указанному на обратной стороне вашей карты, и выясните, все ли в порядке.

- Вам звонит «рассеянный человек», который говорит, что по ошибке указал при совершении интернет-платежа ваш номер телефона. Он просит сообщить ему код подтверждения, который придет (или только что пришел) на ваш телефон в SMS-сообщении. Игнорируйте этот звонок! В реальности ситуация, описанная этим «рассеянным человеком», невозможна.

- Вам поступает звонок якобы из клиентской службы или службы безопасности вашего банка.

При этом на вашем телефоне может отобразиться реальный телефон вашего банка, например, 900 для Сбербанка. В разговоре собеседник пытается заставить вас назвать секретные данные вашей банковской карты (PIN-код, CVC / CVV-код, одноразовые пароли из SMS-сообщений, кодовое слово карты).

Вам действительно могут позвонить из вашего банка, если совершенный вами платеж вызывает вопросы у сотрудников его службы безопасности. У вас могут спросить, действительно ли вы проводили эту операцию, попросить назвать время и способ совершения операции, но никогда не будут спрашивать у вас данные вашей карты, данные паспорта или кодовое слово. Вся необходимая информация у настоящих сотрудников банка уже есть.

**ВАЖНО ПОМНИТЬ!**

***- Злоумышленники могут говорить уверенным голосом, использовать психологическое давление, заявляя, что прямо сейчас по вашей карте проводятся подозрительные платежи на большие суммы денег, что к карте получили доступ мошенники и т. д. Кроме того, они могут обратиться к вам по фамилии, имени и отчеству, правильно назвать ваши паспортные данные и данные карты.***

***- Не поддавайтесь на провокации! Помните о том, что НИКТО и НИКОГДА не может требовать у вас назвать PIN-код карты, CVC / CVV-код или одноразовые пароли из SMS-сообщений. НИКОМУ, кроме злоумышленников, эта информация не может понадобиться!***

**Если вы стали жертвой мошенников:**

• обнаружив неожиданное списание денег со счета своей карты, немедленно позвоните в банк по телефону горячей линии (он указан на обороте карты);

• сообщите о случившемся и попросите заблокировать карту;

• затем обратитесь в отделение вашего банка и подайте заявление о несогласии с операцией;

• также обязательно обратитесь в правоохранительные органы с заявлением о хищении ваших

средств.

1. **Кибермошенничество.**

Это название носят действия злоумышленников, направленные на хищение личных данных граждан в сети Интернет. Одним из самых распространенных методов действия кибермошенников является фишинг – массовая рассылка электронных писем, сообщений в социальных сетях и мессенджерах.

- При получении сообщения, напоминающего фишинговое, имеет смысл связаться с компанией, от имени которой оно отправлено;

- Не используйте для связи телефоны из подозрительного сообщения;

- Не переходите ни по каким ссылкам и не загружайте вложенные файлы из подозрительных или неожиданных сообщений по электронной почте, в соцсетях и мессенджерах;

- Установите на компьютер надежный антивирус;

- Любые приложения и программы для компьютеров следует скачивать только с официальных сайтов разработчиков, а для смартфонов – в магазинах App Store и Google Play;

**ВАЖНО ПОМНИТЬ!**

***Даже если вы получили неожиданное сообщение со ссылкой или файлом от знакомого человека, лучше перезвонить ему и проверить, действительно ли именно он отправил вам это сообщение. Есть риск, что от имени вашего знакомого действуют злоумышленники.***

При подозрениях на фишинговую атаку немедленно смените пароли своих учетных записей на сервисах, которыми вы пользуетесь. При обнаружении кражи средств с банковских счетов действуйте в соответствии с не раз упомянутой выше схемой: звонок в банк, блокировка банковских карт, заявление о несогласии с операцией, обращение в полицию.

За получением дополнительной консультации Вы можете обращаться в отдел экспертиз в сфере защиты прав потребителей Южного Екатеринбургского филиала ФБУЗ «Центр гигиены и эпидемиологии в Свердловской области».

Контактная информация по территориям:

- г. Екатеринбург, телефон (343) 266-54-97;

- г. Арамиль, телефон (343) 385-32-81;

- г. Полевской, телефон (34350) 4-21-68;

- г. Сысерть, телефон (34374) 6-51-51.

Юрисконсульт отдела экспертиз в сфере защиты прав потребителей филиала ФБУЗ «Центр гигиены и эпидемиологии в Свердловской области в Чкаловском районе города Екатеринбурга, городе Полевской и Сысертском районе \_\_\_\_\_\_\_\_\_\_\_\_Попкова М.В.

|  |  |
| --- | --- |
| И.о. главного врача филиала Федерального бюджетного учреждения здравоохранения «Центр гигиены и эпидемиологии в Свердловской области в Чкаловском районе города Екатеринбурга, городе Полевской и Сысертском районе» | Поздеев А.В. |