Внимание!

Современные мошенники активно используют социальную инженерию – психологические приемы, вынуждающие жертву сделать именно то, что нужно мошеннику, например перейти по ссылке, скачать вредоносный файл или сообщить код из СМС. По данным ВЦИОМ, 9% россиян теряли деньги в результате действий Интернет-мошенников, а 6% заявляли о краже крупных сумм.

За чем же охотятся цифровые мошенники?

- **Деньги;**
- **Персональные данные;**
- **Логины и пароли.**

Надо запомнить!

1. Для современных мошенников персональные данные являются не менее ценными, чем денежные средства, а иногда они даже полезнее. Именно с помощью персональных данных преступники отнимают у жертвы денежные средства, входя к ней в доверие. Кроме того, персональные данные сами по себе имеют ценность, ведь мошенники могут продавать их другим преступникам.
2. Кроме онлайн-мошенников существует другая, не менее опасная группа – телефонные мошенники. Они могут представиться кем угодно: сотрудником банка, полиции, прислать СМС от имени родственника. Они также используют социальную инженерию, пытаясь украсть данные. Иногда мошенники специально охотятся за голосом человека, например, задавая навязчивые вопросы. Их интересует то, как абонент назовет свои ФИО, а также скажет: «Да». В дальнейшем мошенники могут использовать записи голоса для входа в банковский аккаунт жертвы, голосом подтверждая банковские операции.
3. Еще одна опасность в Интернете – скрытые платные подписки. Многие мошенники или недобросовестные организации провоцируют пользователей на оформление подписок таким образом, что пользователь узнает об этом только тогда, когда обнаружит регулярное списание денег со своего счета. Такую скрытую подписку можно случайно оформить при переходе на сайт с пиратским контентом, при скачивании файла или приложения или при оплате какой-либо услуги в Интернете. Так, например, однократно купив что-либо или пожертвовав деньги, можно не заметить галочку, которая подтверждает ваше согласие на подписку. Иногда создатели сайта специально делают эту галочку едва различимой или даже вовсе скрытой с экрана. Будьте бдительны!

Полезные советы

Как защитить ребенка от мошенничества в Интернете?

1. В первую очередь следует научить ребенка перепроверять информацию. В случае с сайтами следует обращать внимание на адресную строку – нет ли в адресе сайта каких-либо изменений или неточностей. Если адрес отличается от настоящего даже на один символ – это явный признак подделки. Если входящий звонок поступает от представителя банка или другой структуры, следует самостоятельно перезвонить в эту организацию и задать им вопрос, есть ли у них такой сотрудник и мог ли он вам сейчас звонить. Чаще всего банки не осуществляют операции по звонкам. Однако следует учитывать, что мошенники могут целиком скопировать даже настоящий номер и представиться настоящим именем сотрудника.
2. Объясните ребенку, что не следует принимать поспешных решений. Мошенники могут требовать от жертвы принять решение в текущий момент. Они рассчитывают на то, что в спешке, панике или страхе человек утратит бдительность и охотнее согласится на перевод денег. В таком случае можно ответить: «Сейчас я все проверю и перезвоню вам», или «перезвоните мне через 5-10 минут, мне нужно время, чтобы подумать». Обычно этого времени хватает человеку, чтобы распознать мошенников, проверить информацию и не допустить ошибки.

3. Ребенка следует приучить беречь свои персональные данные с раннего возраста. Ребенок должен знать, что именно относится к персональным данным и что их нельзя размещать в Интернете без необходимости. Опасность представляют как сами данные, так и фотографии документов. Даже простое размещение номера телефона в социальной сети может привести к нежелательным звонкам, спаму, угрозам или шантажу.
4. Если у ребенка уже есть банковская карта, не следует хранить на ней много денег. Лучше всего класть деньги на карту тогда, когда он собирается что-то потратить или хранить на ней небольшое количество денег, которое не страшно будет потерять.
5. Не привязывайте телефон ребенка к банковским картам, счетам, платежным системам. Все платежи за ребенка лучше проводить самостоятельно.
6. Ограничивайте установку приложений на телефон ребенка. Наличие на телефоне антивируса и родительского контроля позволит защитить телефон от спама и вредоносных программ.
7. Установите ограничения и контроль на мобильном счете ребенка. Лимит расходов, можно установить в личном кабинете мобильного оператора. Там же можно отключить возможность оформления платных подписок и изменения тарифа.
8. Научите ребенка опасаться звонков с незнакомых номеров и не перезванивать на них. К любому звонку с неизвестного номера следует относиться с осторожностью. Если перезвонить на такой номер, вас могут перевести на линию, где за каждую минуту разговора с вашего счета будут списываться огромные деньги.
9. Объясните ребенку, что нельзя переходить по ссылкам из СМС и загружать файлы, которые пришли с неизвестного номера. Такой файл или ссылка могут установить на устройство вирус или отправить все данные владельца телефона прямо в руки к мошенникам.
10. Подключите ребенку защиту от нежелательных звонков. Такая функция есть у смартфонов на системах Android и iOS. Она позволит отфильтровать спам, звонки с опасных и нежелательных номеров.
11. Если ребенок уже стал жертвой мошенников, следует немедленно обратиться в полицию. Не забудьте сохранить все доказательства мошеннической деятельности – скриншоты сайтов, переписок, квитанций онлайн-платежей.

Личный пример

Установите на смартфоне ребенка надежный пароль, который он должен знать наизусть и ни с кем не делиться. Это обезопасит устройство при попадании в руки чужих людей, в том числе других детей.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ: необходимые средства защиты

Процветающий бизнес на каждом из нас

Современные технические средства очень сильно изменили виды мошенничества, которые используются злоумышленниками. Они могут, например, подделывать сайты, создать страницу абсолютно идентичную странице Интернет-магазина с нужным вам товаром, но при оплате деньги отправятся напрямую к мошенникам.

Самым распространенным способом мошенничества в Интернете является «фишинг». С его помощью мошенники выуживают у пользователя данные и потом используют их в своих целях. В Интернете существует огромное множество фишинговых сайтов. Они могут копировать страницу, например, известной соцсети. При попытке войти в свой профиль на таком сайте мошенники получат полный доступ к вашему аккаунту.

Они с лёгкостью подделывают любой номер телефона и не только его цифры, но даже могут сделать так, что при звонке ребёнок увидит надпись, например, «полиция», «мама», «брат» и т.п. Более половины россиян регулярно получают звонки от мошенников (по данным ВЦИОМ). Страшно? Есть способы остановить злоумышленников!

Ключевой вопрос

Как противостоять преступным действиям мошенников?