Определение мошеннических звонков

Узнайте, как определить мошеннические звонки и как защититься от них.

1. Что такое мошеннические звонки и как они работают?

Мошеннические звонки похожи на фишинг. Цель этих звонков — выманить у вас персональные данные или предоставить кому-либо доступ к вашим финансовым счетам.

Если целью онлайн-фишинга может быть получение доступа к вашим учетным записям, то телефонные мошенники часто пытаются убедить вас сообщить им вашу финансовую информацию, чтобы оплатить фальшивый счет, или воспользоваться мнимой финансовой возможностью.

Вот некоторые приемы, которыми пользуются телефонные мошенники, чтобы вас обмануть:

- **Обманчивая срочность.** Телефонные мошенники часто оказывают на вас давление, чтобы выманить ваши данные. Они могут утверждать, что у вас есть задолженность или что вам делается «предложение с ограниченным сроком действия» по рефинансированию.
- **Запугивание.** Телефонные мошенники также часто пытаются вас запугать, чтобы выманить ваши данные. Например, они могут выдавать себя за сотрудников Налогового управления (IRS).
- **Заманчивая возможность.** Эти мошенники часто пытаются убедить вас, что вы что-то выиграли или что вы можете воспользоваться ограниченной или «специальной» возможностью.

- **Просьбы о пожертвовании.** Некоторые мошенники выдают себя за благотворительные организации и выманивают пожертвования на якобы добрые дела.

2. Каковы распространенные типы мошеннических звонков?

Телефонные мошенники часто пытаются заполучить ваши деньги. Вот несколько распространенных видов мошеннических звонков, с которыми вы можете столкнуться:

- **Рефинансирование задолженности.** Телефонные мошенники часто пытаются соблазнить вас предложениями по рефинансированию вашей задолженности, будь то кредит на обучение, рефинансирование ипотеки или задолженность по кредитной карте.
- **Помощь с выплатой кредитов.** Разновидность мошенничества, связанного с рефинансированием задолженности. Эти мошенники обманывают вас, предлагая помощь с выплатой ваших кредитов.
- **Медицинское страхование.** Эти мошенники пытаются обманом вынудить вас подписаться на фальшивый план медицинского страхования.
- **Звонки из Налогового управления.** Звонки якобы из Налогового управления (IRS) стали невероятно распространенными. Эти мошенники запугивают вас мнимой задолженностью перед Налоговым управлением и проблемами в случае отказа от немедленной выплаты.
- **Фальшивые предупреждения о мошенничестве.** Эти мошенники выдают себя за ваш банк или обслуживающую компанию и убеждают вас, что кто-то получил доступ к вашей учетной записи, чтобы выманить у вас данные.
- **Фальшивые благотворительные организации.** Эти мошенники выманивают пожертвования на якобы добрые дела.
- **Бесплатный круиз.** Еще один очень распространенный вид мошенничества. Эти мошенники пытаются заполучить ваши персональные данные, убедив вас в том, что вы выиграли бесплатный круиз.
- **Техническая поддержка.** Эти мошенники чаще всего задействуют электронную почту, но иногда бывают случаи телефонного мошенничества. Звонящий представляется

сотрудником службы технической поддержки и пытается заполучить данные вашей учетной записи.

3. Как определить мошеннические звонки и как защититься от них?

Попробуйте следующие способы:

- Относитесь с подозрением к звонкам с неизвестных номеров. Перенаправляйте такие звонки на голосовую почту для последующей проверки.
- Если вы ответили на звонок от неизвестного абонента и услышали робота или явную запись, это может быть признаком мошенничества.
- Сохраните на своем телефоне контакты компаний и сервисов, услугами которых вы пользуетесь, чтобы точно знать, кто вам звонит.
- Относитесь с подозрением к любым звонкам или голосовым сообщениям, если вас пытаются убедить или заставить предоставить персональные данные или финансовую информацию.
- Сократите количество получаемых спам-звонков, воспользовавшись настройками вашего телефона и средствами защиты от вашего оператора мобильной связи, чтобы блокировать спам и сообщать о нем. Найдите настройки для вашей модели телефона и вашего оператора мобильной связи.
- Воспользуйтесь сторонними приложениями, позволяющими контролировать и блокировать телефонный спам. Это такие приложения, как Robo-Killer, или приложения от операторов мобильной связи, например Call Filter от компании Verizon.
- Зарегистрируйтесь в реестре Do Not Call, чтобы перестать получать звонки от агентов по телефонным продажам.
- Будьте осторожны, сообщая свой номер телефона в Интернете.
- В случае получения подозрительного голосового сообщения или звонка поищите дополнительную информацию. Вы можете найти отзывы о подтвержденном мошенничестве.

- Наконец, вы сами можете сообщать о мошенничестве на такие ресурсы, как https://reportfraud.ftc.gov/#/.