Звонок от "начальника" и другие новые способы телефонного мошенничества

Мошенники придумывают все новые способы обмана граждан по телефону.

❗ Наряду с общеизвестным способом, таким как звонки от имени родных, которые якобы попали в беду и нуждаются в денежных средствах, сейчас широко распространены случаи направления сообщений от лица руководителя предприятия, учреждения, где трудится гражданин:

- о необходимости сбора средств на различные общественные нужды,

- о перечислении средств в целях временной помощи организации с обещанием последующего возврата денег с вознаграждением,

- об утечке персональных данных работников и необходимости помещения своих денег на "безопасные" счета.

Нередко мошенники, представившись директором, ссылаются на проходящую в организации проверку со стороны правоохранительных органов. При этом далее гражданину начинают поступать звонки от "сотрудников" таких органов с информацией о проблемах в фирме или у самого работника.

❓ Что делать в случае, если вам поступил подобный звонок или сообщение от руководителя?

Имейте ввиду, что в настоящее время мошенники ведут серьезную подготовительную работу, они могут точно знать ваше имя, должность, имена других работников организации, использовать в качестве аватара реальную фотографию вашего начальника. Не доверяйте собеседнику только на том основании, что ему известны сведения про вас!

👆При первой же возможности лично обратитесь к руководителю, от чьего имени ведется общение либо к вашему непосредственному начальнику. При отсутствии такой возможности лично пообщайтесь с коллегами, даже если собеседник запрещает кому-либо рассказывать об этом!

Не бойтесь прервать разговор, чтобы прояснить ситуацию. В первую очередь вас должно насторожить именно требование никому ничего не рассказывать и быстро принять решение.

‼️Другие признаки, что вам звонят или пишут мошенники от лица вашего руководителя и (или) сотрудников правоохранительных органов:

а) Начальник связался с вами не тем способом, как вы обычно общаетесь, ведет беседу в несвойственном ему стиле.

б) С вас требуют снять деньги в банкомате.

в) Вас заставляют взять кредит в банке и при этом в случае звонка службы безопасности банка сказать, что кредит вы берете на личные нужды.

г) Вам приказывают сотрудничать и угрожают привлечением к ответственности.

👆Запомните! Работники правоохранительных органов никогда не будут предлагать вам перевести куда-либо ваши деньги или предъявлять обвинения по телефону без вручения официальных документов!

❗ Другие новые способы мошенничества в информационной сфере:

1. Мошенники под видом запроса Росфинмониторинга рассылают требования о необходимости совершить платеж или заплатить комиссию за денежные переводы.

2. Поступает звонок с указанием на необходимость обновления банковского приложения на смартфоне, поскольку предыдущее устарело или лишилось поддержки. Затем в СМС-сообщении направляется ссылка на сайт, с которого якобы можно скачать обновление для приложения.

3. Создание точных копий официальных сайтов, на которых предлагается ввести персональные данные, данные банковских карт.
Обращайте внимание на адресную строку сайта. Домен фишингового ресурса может иметь отличие от домена оригинального сайта всего в одну букву!

4. Направление электронных писем от имени популярных маркетплейсов. В этих письмах говорится о том, что пользователю якобы отправлен подарок от известного онлайн-магазина, который можно получить, перейдя по конкретной ссылке. Если перейти по этой ссылке, то откроется веб-страница, оформленная в стиле известного маркетплейса, где будет предложено ввести персональные, платежные и другие конфиденциальные данные для получения выгодного промокода, бесплатного товара или какого-то другого вознаграждения.

5. Злоумышленники, представляясь по телефону сотрудниками правоохранительных органов либо представителями техподдержки портала «Госуслуги», сообщают о взломе аккаунта на данном портале и попытке мошенников оформить кредит.

6. Рассылка электронных писем от имени Федеральной налоговой службы о выявлении подозрительных транзакций и активности налогоплательщиков. С целью подтверждения указанных действий могут быть запрошены копии каких-либо платежных либо личных документов.

7. Злоумышленники звонят с информацией о том, что ваш тарифный план или договор оказания услуг связи закончился и необходимо их продлить, указав паспортные данные либо перейдя в личный кабинет пользователя сотового оператора.

8. Злоумышленники от имени управляющих и ресурсоснабжающих организаций рассылают информацию о перерасчете платы за коммунальные услуги по итогам года либо оплате с выгодной скидкой. В рассылке указана ссылка на сайт, при оплате через который якобы будет предоставлена скидка. В действительности жертва попадает на поддельный сайт, при вводе персональных данных и данных банковских карт они попадают к злоумышленникам.

👆Будьте внимательны в информационном пространстве!