**Дистанционное мошенничество, что это такое и как с ним бороться.**

67 процентов россиян получили за последние полгода звонки от мошенников. Киберпреступность с каждым годом растет не только в целом по стране, но и в нашем районе. Только за истекший период 2024 зарегистрировано 10 таких преступлений и их число продолжает расти.

 Для того, чтобы уберечься от таких мошенников, не лишиться своих денег, имущества и не попасть в долговую яму, хочу привести самые актуальные схемы, которые используются недобросовестными гражданами для получения «легких» денег.

 **Схема № 1.**

 **«Ваш номер нужно подтвердить»**

Простейший обман, который чаще всего срабатывает. Вам поступает звонок якобы от оператора сотовой связи. Мошенники утверждают, что действующий с Вами договор на оказание услуг связи заканчивается и его необходимо продлить, иначе Ваш номер передадут другому абоненту, но идти никуда не нужно, все можно сделать по телефону, уверяет вас собеседник. Достаточно продиктовать код из СМС. На самом делу мошенника цель одна - получить доступ к аккаунту человека на портале «Госуслуги».

Следующий шаг – перейти по присланной ссылке, где нужно ввести еще один код. Таким образом, человек не продлевает договор, который на самом деле является бессрочным, а предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая там хранится.

Есть и другая цель, тот же звонок, но уже с предложением по смене тарифного плана, подключением новых опций и т.д. Чтобы это сделать, абонента просят продиктовать код из СМС, с помощью которого 0злоумышленник получает доступ к личному кабинету пользователя на сайте оператора мобильной связи. А уже там он настраивает переадресацию сообщений и звонков с номера жертвы на свой для того, чтобы в дальнейшем подтверждать разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита.

Если это уже произошло, Вам необходимо обновить персональные данные, обратившись в офис оператора связи или в личном кабинете на его официальном портале. А чтобы этого не случилось – не называйте никаких данных незнакомым по телефону!

**Схема 2.**

**«Предложения от лжеброкеров»**

Аферисты предлагают Вам выгодно вложить деньги, обещая проценты выше, чем у банков. С гражданами они связываются, как правило, через «социальные сети». Предложение выглядит заманчиво: нужно лишь открыть «брокерский» счет и инвестировать от 10 тысяч рублей. Доход – не меньше миллиона.. Для открытия такого счета мошенники требуют установить приложение. Далее программа имитирует якобы рост доходов от инвестиций, в том числе в криптовалюте. Как только у Вас возникает желание «вывести» деньги со счета, начинаются проблемы; пополнить счет еще раз, заплатить «страховку», либо найти поручителя и т.д. В результате гражданин теряет свои деньги, а с ним уходит и надежда быстрого обогащения.

**Схема № 3**

**«Вам предлагают выгодную работу».**

Афферисты размещая лжевакансии на популярных сайтах типа «Авито» с вакансиями, приличной зарплатой и шикарными условиями работы. Но нужно пройти собеседование с будущим работодателем и вам предлагаю это сделать онлайн по видеозвонку.

Во время онлайн встречи мошенники крадут ваши личные данные Они, проводя собеседование просят заполнить анкету, одним из пунктов которой - номер карты или иные финансовые данные, которые нужны, якобы, для перечисления заработной платы в будущем.

Понятно, что вместо пополнений с банковской карты соискателя в будущем происходит списания, а ни о какой работе, естественно, речи не идет.

Поэтому, внимательно изучайте предложения от будущих работодателей и отзывы о нем. Не видитесь на обещания легкого заработка с минимальными затратами.

**Схема 4**

**«Друг прости о помощи»**

Еще одна тактика мошенников – рассылка сообщений с просьбой одолжить денег близким или друзьям. Зачастую мошенники играют на чувствах человека и сообщают, что его родственник попал в беду И если раньше аферистам приходилось разыгрывать «спектакль» подделывать голос, то теперь за них это делает искусственный интеллект. Аферисты взламывают аккаунт пользователя, скачивают голосовые сообщения и на их основе генерируют монолог для дальнейшего обмана.

Как же понять, что родственник то «фальшивый», не переходите по неизвестным ссылкам, даже если получили их от знакомых. Договоритесь с родственниками о пароле или секретном вопросе, если разговор Вам кажется подозрительным

Разъясняет заместитель прокурора Пристенского района Жданова С.Л.