В настоящее время киберпреступность растет с пугающей скоростью - так отмечают правоохранительные органы. Чтобы противостоять таким угрозам, в структуре МВД недавно было создано управление по борьбе с противоправным использованием информационно-телекоммуникационных технологий.

Сокращённо подразделение можно смело назвать киберполицией. Возглавил Управление генерал-майор полиции Филипп Немов.

Киберполицейские проанализировали все виды дистанционных хищений, которые преступники применяют в этом году, а также рассказали о некоторых актуальных мошеннических схемах.

Согласно схеме № 1 под названием «Ваш номер нужно подтвердить». Установлено, что это простейший обман, который чаще всего срабатывает. Поступает звонок якобы от оператора сотовой связи, мошенники пугают, что действующий договор на оказание услуг связи заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно седлать по телефону, уверяет собеседник, достаточно продиктовать код из смс. На самом деле цель одна - получить доступ к аккаунту человека на «Госуслугах».

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

Есть и другая цель, которую преследуют мошенники, представляясь оператором связи. Тот же звонок, но теперь с предложением по смене тарифного плана, подключением новых операций либо замены sim-карты. Чтобы это сделать, абонента просят продиктовать код из смс. С помощью этого кода злоумышленники получают доступ к личному кабинету пользователя на сайте оператора мобильной связи.

А после этого они настраивают переадресацию сообщений и звонков с номера жертвы на свой. Это делается для того, чтобы в дальнейшем подтверждать разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита.

Что в таком случае советуют делать киберполицейские. Вы можете обновить персональные данные, обратившись за услугой лично, в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из смс). Не называйте никаких данных незнакомым людям по телефону.

Схема № 2 «Предложения от лжеброкеров» заключается в следующем. Злоумышленники предлагают вам выгодно вложить свои средства, обещая процент гораздо выше, чем у банков. С потенциальными инвесторами они связываются через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний.

Предложение заманчивое: нужно лишь открыть «брокерский» счёт и инвестировать от 10000 рублей. Доход – не меньше миллиона. Для открытия такого счёта мошенники требуют установить приложение. Далее программа имитирует якобы рост доходов от инвестиций, в том числе в криптовалюте. Как

только у «инвесторов» возникает желание вывести деньги со счёта, начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счёт ещё раз на определённую сумму, оплатить «страховку». Или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства. В итоге инвестор теряет свои деньги, а заодно и надежду на будущие миллионы.

Вариант этой мошеннической схемы – участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают при помощи писем на электронную почту. Мошенники, оформляя сообщение, копируют визуальный стиль банка, для убедительности используя те же корпоративные цвета, логотип и другие элементы. Для участия в «выгодной» кампании предлагается перейти по ссылке.

После вам предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи, а также дадут доступ к специальному предложению. А уже там понадобится ввести данные своей банковской карты – с неё аферисты потом и спишут деньги.

Как отличить мошенников от реальных брокеров. Проверьте сайт инвесткомпании или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России. Откажитесь от услуг, если просят перевести деньги за услуги на карту физического лица либо через электронный кошелек.

Схема № 3 «Вам предлагают выгодную работу». Аферисты размещают лжевакансии на популярных сайтах объявлений типа «Авито». Зарплата привлекательная, условия заманчивые. Но нужно пройти собеседование с будущим работодателем, и вам предлагают сделать это онлайн по видеозвонку.

Во время онлайн-встречи мошенники пользуются растерянностью соискателей и крадут личные данные. Под видом будущего работодателя они проводят собеседование, где просят кандидата заполнить анкету прямо во время зума. Один из ее пунктов – номер карты и другие финансовые данные. Такая информация им нужна якобы для перечисления зарплаты в будущем. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия.

Понятно, что вместо пополнений с банковской карты соискателя в будущем происходят списания, а ни о какой работе, естественно, речи не идёт. Находясь в поиске работы, можно не только потерять деньги, но и нарушить закон, став дроппером.

Дропперы (от английского drop - бросать, капать) – подставные лица, которые заинтересованы в нелегальных схемах по выводу средств с банковских карт. Часто человек не осознаёт, что вовлечен в преступную схему. Ведь объявление о работе, на которую он устраивается, не выглядит подозрительно.

Чего необходиом делать при трудоустройстве онлайн. Внимательно изучайте предложения от будущего работодателя и отзывы о нём, следите за данными, доступ к которым предлагает предоставить работодатель.

Схема № 4 под названием «Друг просит о помощи» заключается в следующем. Происходит рассылка сообщений с просьбой одолжить денег

близким людям или друзьям. Порой в своих сценариях мошенники заходят дальше – играют на чувствах человека и сообщают, что его родственник попал в беду. Если раньше злоумышленникам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за всех это делает искусственный интеллект. Аферисты взламывают аккаунт пользователя, скачивают голосовые сообщения и на их основе генерируют диалог для дальнейшего обмана.

В таких случаях не переходите по неизвестным ссылкам, даже если получили их от знакомых. Договоритесь с родственником о секретном вопросе, который нужно задать, если разговор кажется подозрительным.