

Технологии развиваются. Нужно быть ГОТОВЫМ КО ВСЕМУ

Защита граждан от кибермошенников – приоритет работы полиции

Михаил БАТУРИН

В прошлом году доверчивые свердловчане отдали мошенникам в общей сложности более 2,7 миллиарда рублей. За десять месяцев 2024 года сумма обманом украденных у наших земляков средств составляет уже 3,5 миллиарда. Злоумышленники придумывают все новые схемы для выманивания «наших кровных», используя для этого самые изощренные психологические уловки и современные технологии. Правоохранительные органы держат вопрос на особом контроле. В Главном управлении МВД РФ по Свердловской области противодействием преступлениям в киберсфере занимается специальное подразделение – Управление по борьбе с противоправным использованием информационно-коммуникационных технологий. Его руководитель полковник полиции Евгений ПОЛУПАНОВ стал гостем редакции «Областной газеты» и ответил на вопросы журналистов и читателей, позвонивших по прямой линии.



БОРИС ЯРКОВ

Вопросы «ОГ»:

? Евгений Владимирович, насколько помним, раньше преступления в сфере компьютерных технологий занимался отдел «К».

– Отдел «К» – подразделение по борьбе с киберпреступлениями, с преступлениями в сфере информационных технологий – существовал до 30 сентября 2022 года, когда по Указу Президента РФ Владимира Путина на его основе было создано управление по противодействию преступлениям в сфере информационных технологий. Сегодня такие подразделения есть во всех региональных управлениях МВД России, в том числе в Свердловской области. В их задачи входит выявление, раскрытие и предупреждение преступлений в IT-сфере.

Фронт работы у нас большой. Это и неизвестное всем дистанционное мошенничество, и кражи с использованием средств коммуникаций, и преступления в сфере половой неприкосновенности несовершеннолетних в сети Интернет, и противодействие деструктивной информации.

? Если смотреть по процентам: каких преступлений больше?

– Сначала года в Свердловской области зарегистрировано порядка 50 тысяч преступлений. Треть

из них – преступления в сфере информационных технологий. Из этой трети преступлений, связанных с неправомерным доступом к информации (статья 272 УК РФ), с созданием и использованием вредоносного программного обеспечения (статья 273 УК РФ), около 6%. А преступлений против собственности (самый массовый сегмент) – мошенничества и кражи, совершенные дистанционным способом, – более половины (7 800 преступлений). Это небольшое количество.

Активный рост по дистанционным мошенничествам и кражам мы начали фиксировать с 2016 года. Полагаю, что на протяжении последних лет все получали подобного рода звонки от мошенников.

? Вы тоже?

– Ну, конечно. Вообще схем, конечно, очень много. Как и раньше, до сих пор являются «рабочими схемами» обмана для злоумышленников звонки от якобы сотрудников служб безопасности банков, Центрального банка, ФСБ, правоохранительных органов.

В числе наиболее часто используемых мошеннических схем этого года – звонки от работников «Энергосбыта», якобы с целью бесплатной заме-

ны электросчетчиков, или недопущения отключения электричества. Для этого они предлагают установить на телефоне некое приложение, ссылку на которое посылают через мессенджер. Приложение, причем, визуально внушает доверие, может называться «Энергосбыт.арк», «Энерго +.арк» или еще как-то похоже. Но на самом деле это вредоносное программное обеспечение. После того, как человек под воздействием мошенника произведет набор определенных действий по установке, все-таки преступники закупают доступ к его устройству. Экран мобильного телефона гаснет, при этом мошенник уверяет: это нормально, что сейчас все будет настроено и заработает как надо. Реально же благодаря этому вредоносному приложению мошенники получают доступ ко всем данным потерпевшего, и через какое-то время с его банковских счетов начинают выводиться денежные средства.

Еще одна популярная мошенническая схема – звонок из поликлиники. Предлагают пройти бесплатную диспансеризацию, флюорографию, получить результаты обследования, поменять медицинский полис и т. п. И для этого опять-таки нужно установить особое мобильное приложение «ЕМИАС.арк». В результате итог аналогичен –

злоумышленник заведает доступом к мобильному устройству и приложениям, включая банковские.

Также злоумышленники могут представляться, например, оператором сотовой связи с требованием срочно продлить договор, иначе вас прямо сейчас отключат от связи или вы потеряете свой телефонный номер, или перейдете на невыгодный тариф. Цель звонка одна – получить от вас информацию о коде доступа из СМС-сообщения к личным кабинетам на различных Интернет-ресурсах. Например, к личному кабинету портала «Госуслуги». Для этого преступники предлагают продиктовать код сообщения, который приходит на абонентский номер. И потерпевшие, несмотря на то, что в самой эсэмэске написано «никому не сообщайте данные», тут же их сообщают.

Далее доступ к «Госуслугам» у потерпевшего блокируется. Он идет в МФЦ восстанавливает его. Но злоумышленники за это время уже, как правило, выгружают все личную информацию, связанную с пенсионными отчислениями, данные трудовой книжки и другую информацию, которую потом могут использовать в разговоре с потерпевшим.

И тут начинается вторая часть обмана потерпевшего – производится второй звонок. По

ту сторону трубки представляется службой безопасности «Госуслуг», говорят, что до этого звонили мошенники, что данные украдены и обещают решить все проблемы: «Мы работаем совместно с ФСБ, с Росфинмониторингом, сейчас оттуда позвонят и нужно беспрекословно выполнять все инструкции». Потерпевший, конечно, уже понял, что стал жертвой обмана и готов на все, чтобы исправить ситуацию.

Наступает следующая часть многоходовки. Новый позвонивший мошенник уже представляется сотрудником ФСБ или Росфинмониторинга. Он уверяет, что все контролирует, что звонившие изначально мошенники, воспользовавшись данными с «Госуслуг», намерены получить кредиты во всех банках, каких только возможно, и увести денежные средства на свои преступные счета либо на финансирование вооруженных формирований Украины. Так что потерпевший, по их словам, еще и станет пособником террористической деятельности или преступного режима. А то и вообще на него уголовное дело заведут.

Все это происходит в режиме мощнейшего прессинга, морально-психологического давления. Это один из методов социальной инженерии, позволяющий вывести человека из стабильного состояния. Звучит ключевая фра-