Кибермошенникам разрешили сесть

Журналистам «ОГ» рассказали о популярных способах обмана и борьбы с ними

Количество преступлений в сфере кибербезопасности на Среднем Урале снижается, однако сами схемы остаются устойчивыми и адаптируются под поведение людей. Мошенники не только изобретают новые механизмы, но и совершенствуют старые, используя психологическое давление и искусственный интеллект. О самых популярных схемах обмана и о том, как себя обезопасить, рассказал «ОГ» заместитель начальника управления по борьбе с киберпреступностью ГУ МВД России по Свердловской области Олег РУСИН.

ПАВЕЛ ВОРОЖЦОВ

Фишинговые ссылки и взлом аккаунтов

Наиболее заметное изменение последних лет – рост схем с использованием вредоносного программного обеспечения. В отличие от классических телефонных сценариев, здесь нет давления или угроз: всё начинается с обычного сообщения в мессенджере. Человеку пишет знакомый – с просьбой проголосовать, посмотреть фото или открыть ссылку. За счет того, что сообщение приходит от реального человека, оно не вызывает подозрений.

– Если жертва переходит по ссылке – злоумышленники получают доступ к его учетной записи. После этого от его имени начинается рассылка таких же сообщений другим людям, – говорит Олег Русин.

После клика по вредоносной ссылке на устройство попадает вирусная программа, которая работает в фоновом режиме и остается незаметной для пользователя. Основная задача такого ПО – перехват СМС-сообщений. Получив доступ к кодам подтверждения, злоумышленники заходят в банковские приложения и похищают деньги.

– В этом году мы фиксируем рост таких преступлений.

> Чаще всего жертвами становятся не пожилые люди, как раньше, а те, кто активно пользуется Интернетом и считает себя уверенным пользователем.

Если вам пришло сообщение в мессенджере или в соцсетях вроде «ты видел новость?» или «это ты на фото?», лучше просто позвонить и уточнить, что это. Как правило, человек сразу говорит, что его взломали. Доверять голосовым сообщениям, фото и видео уже нельзя – мошенники все чаще используют искусственный интеллект, чтобы генерировать их от имени взломанного аккаунта, – добавляет он.

И снова «безопасные» счета

О том, что «безопасных счетов» не существует, специалисты говорили не раз. Но на эту схему попадаются снова и снова. Если раньше киберпреступники брали своих жертв на испуг – звонили от имени «банков» и «ФСБ», то сейчас используют нейтральные бытовые поводы – доставка посылки или запись к врачу – и для этого просят назвать «код из СМС».

– Разговор начинается с нейтрального повода – доставка, запись, уточнение данных: «вам пришла посылка», «запись в поликлинику», «бесплатная замена домофона для пенсионеров». Человеку предлагают подтвердить личность – для этого сообщить код из «Госуслуг». Жертва диктует код, и ее аккаунт блокируется. Сразу после этого звонят «сотрудники безопасности» – теперь уже из «Госуслуг», ФСБ или Центробанка. Говорят: «Вы только что кому-то сообщили код? Проверьте, у вас «Госуслуги» заблокированы». Человек проверяет (действительно заблокированы) и начинает верить, – объясняет Олег Русин.

Жертве сообщают, что деньги пытались похитить, но «система успела вмешаться». При этом подчеркивают, что защита временная и ее нужно срочно усилить. При этом постоянно подгоняют и запугивают – кредитами, уголовной ответственностью, риском для родственников. В таком состоянии человек перестает критически оценивать ситуацию и действует по инструкции – снимает деньги, оформляет кредиты и переводит всё мошенникам.

> – Человеку говорят, что от его имени пытались перевести деньги на Украину, что он становится соучастником преступления,

а если расскажет кому-то – пострадают родственники. Требуют действовать быстро и запрещают рассказывать об этом кому-либо. Говорят, что нужно перевести деньги на «безопасный» или «резервный счет».

> Раньше требовали перевести деньги, но банки стали блокировать подозрительные операции, поэтому теперь за деньгами чаще приезжают дропы – курьеры мошенников.

Дальше средства через криптообменники уходят организаторам схемы. Информации о том, как не стать жертвой мошенников, сейчас много. Кажется, нет уже ни одного ресурса, где бы об этом не говорилось. Люди сами знают, что сотрудники МВД, ФСБ, Центробанка никогда не будут по телефону говорить, что нужно снять деньги и куда-то их отправить. Но тем не менее люди продолжают верить, – отмечает замначальника управления по борьбе с киберпреступностью.

Часто мошенники пытаются обмануть участников СВО, их родных и близких. Например, звонят родственникам погибшего военнослужащего и сообщают, что ему положен орден Мужества, но для его получения нужно «верифицироваться» – сообщить код из «Госуслуг». Дальше идет отработанная схема «безопасного счета».

«Инвестиции»: сказка о быстром богатстве

Еще одна популярная у мошенников схема – лжеинвестиции. Люди ищут в Интернете способы быстрого заработка, натыкаются на лжеброкеров. Первое время мошенники дают вывести небольшую прибыль, чтобы укрепить доверие.

– Например, человек вложил 50 тысяч, через неделю заработал 10 тысяч. Ему говорят: «Представьте, если бы вы вложили миллион». Жертва начинает верить, берет кредиты, продает квартиры и машины – и теряет всё. Платформы лжеброкеров находятся за границей, вне российской юрисдикции, поэтому вернуть деньги практически невозможно, – констатирует Олег Русин.