Как вести себя в киберпространстве

Вам сегодня звонили с неизвестного номера? Как часто вы сталкиваетесь с нежелательными контактами, которые могут негативно отразиться на вашем настроении, финансовом благополучии и безопасности? Навязчивые спам-звонки от рекламных компаний отнимают время, вызывают злость и раздражение? Это, увы, реалии наших дней, обратная сторона комфорта, даруемого Интернетом и сотовой связью. О манипуляциях в цифровом пространстве беседуем со специалистом Координационного центра ЯрГУ им. П.Г. Демидова Ольгой Рудкиной (на фото).

■ Сергей НИКИФОРОВ

Ох уж эти звонки...

– Ольга Геннадьевна, сначала в нескольких словах поясните читателям «Городских новостей», чем занимается Координационный центр?

– У нас довольно обширный круг задач, работа нацелена и на формирование у молодежи активной гражданской позиции, и на предупреждение межнациональных и межконфессиональных конфликтов, и на противодействие идеологии терроризма, и на профилактику экстремизма. Одним из важных направлений деятельности Координационного центра является информационное сопровождение, в рамках которого мы ведем мониторинг сети Интернет по выявлению незаконного контента и в случае выявления инициируем его блокировку. Проводим встречи для различных категорий граждан по теме информационной безопасности, обеспечиваем сопровождение движения киберволонтеров.

– Итак, навязчивые звонки мешают сосредоточиться на важных делах, отвлекают от работы, забирают время. Но ведь это еще полбеды, нередко после общения со звонившим с неизвестного номера люди лишаются куда большего...

– Звонки мошенников, которые выдают себя за представителей банков, правоохранительных органов или медицинских учреждений, могут привести к серьезным потерям денежных средств и потере персональных данных, которые включают адрес места жительства, семейное положение, образование, профессию, доходы, номер счета, историю болезни. Зачастую этими схемами пользуются колл-центры, осуществляющие свою деятельность на территории других стран, а собранные средства используют в преступных целях, для финансирования террористических актов, направленных в том числе и против нашей страны.

Всегда что-то новенькое

– Что нового придумали мастера обмана в 2024 году?

– Мошенники пытаются завладеть доступом к аккаунтам на портале «Госуслуги». Цифровые пираты звонят потенциальной жертве, утверждая, что у нее подходит к концу текущий договор с оператором сотовой связи и требуют продления, в противном случае номер будет передан другому абоненту. Мошенники убеждают выполнить все необходимые действия по телефону, требуя предоставить код из SMS. Если человек выполняет все указания звонящего, то у мошенников появляется доступ к его личному кабинету на госуслугах. Отсюда сразу различные негативные последствия, самые нежелательные из которых – микрозаймы и кредиты на имя жертвы.

Важно помнить, что все обновления персональных данных следует производить лично – обратившись в офис оператора связи или через личный кабинет на его официальном портале, но ни в коем случае не по ссылке из SMS. Не предоставляйте никакие данные по телефону незнакомцам. В случае сомнений лучше позвонить оператору связи по номеру, указанному на его официальном сайте.

– Часто приходится слышать, что интернет-злоумышленники звонят или пишут человеку якобы от лица сотрудников ФСБ, Росфинмониторинга, ФНС, Социального фонда России...

– Самая распространенная уловка – предложение получить какую-либо государственную выплату. Схема классическая: вы нам данные карты, мы вам – деньги. Есть и другой сценарий. Например, звонок от представителей следственных органов или Росфинмониторинга с угрозой блокировки счета, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф. Для убедительности они могут даже прислать квитанцию на официальном бланке ведомства.

Чтобы не попасться на эту уловку, нужно знать, что подобные ведомства не наделены полномочиями по аресту денежных средств, не оказывают платных услуг по оформлению документов, а также не рассылают подобные письма и не звонят по телефону или в мессенджерах. Если вы получили подобные сообщения, проигнорируйте их и обратитесь напрямую в государственную организацию.

Существует и другой «безобидный» сценарий – предложить проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

«Чтобы не привлекать к себе внимание мошенников в Интернете, необходимо:
- не размещать на личных страницах социальных сетей и аккаунтах мессенджеров информацию о месте жительства, работе, учебе, свои личные данные и данные родственников;
- ограничить доступ к личным фотографиям, записям, оставив доступ только кругу хорошо знакомых людей;
- не вступать в переписку с незнакомыми людьми, особенно настороженно относиться к тем, кто проявляет чрезмерную активность и интерес, а также предлагает легкий и быстрый способ заработка за короткое время;
- на любое предложение о легком заработке, решении проблем отвечать отрицательно и прервать дальнейшую переписку;
- не отправлять фото документов, удостоверяющих личность (паспорт, ИНН, водительские права);
- не передавать третьим лицам данные банковских карт, счетов, сведений из личного кабинета налогоплательщика на портале госуслуг.

Если вы столкнулись с чем-то подобным, то не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых. Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным. Такой шаг поможет раскусить намерения мошенника.

Но не только аферисты могут поджидать вас в Интернет-пространстве, но и фейковая – ложная или вводящая в заблуждение информация, выдаваемая за реальные новости.

То ли правда, то ли ложь...

– Как же отличить правду от вымысла и не поддаться на провокации?

– Обратите внимание на заголовок. Иногда сама новость может быть в целом правдивой, но, чтобы побудить пользователя открыть ее, используется сенсационный заход, не соответствующий содержанию. Как, например, – «Ванга предсказала России катастрофу!», «Ты не сможешь удержаться от смеха!», «Чтобы через год купить себе квартиру, нужно всего лишь каждый день...» А вот еще один: «Через два года смартфоны вымрут!».

Проверяй «горячую сенсацию» на информационных ресурсах. Увидев строки: «В таком-то городе нашей страны произошло непостижимое», найдите авторитетный первоисточник или перейдите на ресурсы ведущих средств массовой информации. Если там об этом ни слова, то скорее всего вы столкнулись с ложной, беспокоящей информацией.

Тревожным индикатором неправдивой новости является большое содержание эмоций. Самые скандальные и быстро распространяемые фейки носят панический характер или обращаются к несуществующим теориям заговоров. По сути, это развод и спекуляция на темах, которые близки каждому, – деньги, отношения, семья, здоровье.

Еще одним звоночком служит однобокость излагаемой информации. Когда материал поддерживает определенную позицию, содержит призывы или стереотипные высказывания, то скорее всего автор манипулирует аудиторией и стремится влиться в доверие к потребителям информации.

Но и это еще не все, что может поджидать вас на просторах Интернета. В связи с проводимой нашей страной специальной военной операцией (СВО) в последнее время участились случаи вербовки граждан РФ специальными службами враждебных государств.

Не общайтесь с незнакомцами

– По каким же признакам вы можете распознать вербовщика?

– Вербовщики действуют в основном через социальные сети и мессенджеры WhatsApp, Telegram, Viber, используют даже сайты знакомств. Схема, как правило, стандартная. Первым делом новый знакомый пытается войти в доверие к собеседнику, начинает активно интересоваться личной жизнью, увлечениями, проблемами, заботами, финансовым положением. Это необходимо, чтобы найти нужную «кнопку» и в будущем знать, на что надавить.

Затем, выяснив, чего или кого собеседнику не хватает, вербовщик старается занять пустующую нишу в его жизни. Он стремится стать другом, любовником, соратником, учителем, спасителем и проч. Старается помочь решить проблемы собеседника, даже если его об этом не просили, чтобы в дальнейшем тот чувствовал себя обязанным. Вот фразы, которые должны насторожить потенциальных жертв, – «я хочу тебе помочь», «ты себе даже не представляешь, как тебе сейчас нужна помощь».

Вербовщик будет стараться изменить привычную жизнь человека, советовать «порвать с людьми, которые тебя не ценят», «обрести новых друзей», «игнорировать родителей и родственников, которые не понимают твоей уникальности или таланта». Он будет рекомендовать читать книги или статьи, которые «изменят твою жизнь и представления об окружающем мире». В ходе переписки будет манипулировать эмоциональным состоянием для того, чтобы запрограммировать на определенное поведение.

Главная задача вербовщика – сделать человека беззащитным перед манипуляцией, заставить его усомниться в своем мировоззрении, в своих жизненных принципах, идеях. Затем он пообещает решить все проблемы разом, но при условии выполнения определенного задания. В качестве теста может попросить о любой, самой простой услуге. Если собеседник соглашается, то он попал к вербовщику на крючок.

– Как противостоять технологиям вербовки?

– Общаясь с новыми людьми, особенно онлайн, соблюдайте три главных правила. Во-первых, подумайте, что с вами происходит сейчас. Вырабатывайте навык наблюдателя, научитесь задавать вопросы и задавайте их по существу, например: «Зачем Вы мне это говорите?», «Для чего вам это нужно?» Во-вторых, перепроверяйте любую информацию, исследуя предмет полностью, начиная с отзывов в Интернете и заканчивая сводками МВД. И в-третьих, найдите глобальную цель в жизни, продумайте путь ее достижения. И тогда ни одна секта, ни одна мысль или идея не смогут сдвинуть вас с пути, по которому вы идете для достижения намеченных планов.

Вербовкой занимаются специально обученные, хорошо подготовленные люди, владеющие психологическими приемами, – техникой манипуляций, внушением. Поэтому противостоять им довольно сложно, необходимо вовремя распознать вербовщика и минимизировать общение с ним. ■