**Топ-3 мошенничеств летом:**

**под видом диспансеризации, дешевых путешествий и бесплатных фотосессий**

«Запись на диспансеризацию»

Мошенничество начинается с звонка по телефону. К человеку обращаются по имени-отчеству, представляются работником регистратуры поликлиники и приглашают на диспансеризацию. «Записаться на удобное время и пройти несколько обследований можно в один день», — уверяют аферисты. За вами закрепляют дату посещения и для ее подтверждения нужно продиктовать код из СМС, который поступит во время звонка.

Если человек будет внимательным, то заметит, что код пришел вовсе не для записи в поликлинику, а для подтверждения входа в личный кабинет на портале Госуслуги. Если его назвать, то мошенники получают доступ к аккаунту человека и впоследствии могут оформить на него онлайн-займы.

«Аферисты нередко используют в схемах обмана тему медицины и здоровья. Они могут называть фамилии реальных врачей, адрес местной поликлиники, к которой прикреплен человек. Такие сведения они находят в открытых источниках или в краденных базах данных. Иногда мошенники убеждают установить на телефон приложение для записи к врачу, а по факту это программа-вирус, из-за которой человек потеряет доступ к своему устройству. И под угрозой оказываются все приложения с персональными и платежными данными, в том числе банковские», — отметил эксперт по кибербезопасности владимирского отделения Банка России Евгений Гаврилюк.

«Отдых со скидкой»

Мошенники присылают по электронной почте или через мессенджеры предложение отдохнуть по удивительно низкой цене. Такое объявление также может попасться в соцсетях или выпасть в поисковике. Скидки за раннее бронирование и на горящие туры действительно бывают, но не стоит спешить переходить по рекламной ссылке и оплачивать поездку. Страница, на которую вы попадете, может оказаться фишинговой (поддельной).

Оплачивая гостиницы и апартаменты через сервисы бронирования, можно попасть на отели-призраки, которых на самом деле нет. Если человек переведет деньги за такую гостиницу, то сервис будет обязан вернуть их или подобрать отель, так как не уследил и допустил публикацию мошеннического предложения. Стоит насторожиться, если «представитель отеля» уговаривает уйти с официального сайта или сервиса бронирования в мессенджер, присылает ссылку для оплаты или просит перевести деньги ему лично по номеру телефона. В этом случае существует риск потери денег, так как пользователь покидает безопасный сервис бронирования.

«Когда вы увидели рекламу гостиницы и решили забронировать ее напрямую, важно быть уверенными как минимум в двух моментах. Первое — перед вами жилье, которое действительно существует. Второе — вы попали на настоящий сайт этого отеля. Российские отели, пансионаты и дома отдыха легко проверить в реестре Ростуризма — там собраны только настоящие объекты. Если перейдете на их сайты прямо из реестра, можете не сомневаться, что перед вами реальные описания, а формы для оплаты не фишинговые», — пояснил Евгений Гаврилюк.

«Красивые фото бесплатно»

Аферисты выбирают аккаунты симпатичных девушек, делают им комплименты и зазывают на «бесплатные» съемки. Мнимые фотографы просят перевести им деньги на электронный кошелек или карту только за аренду студии. Иногда для большей правдоподобности предлагают провести оплату на странице самой «площадки». Правда, для этого присылают ссылку на поддельный сайт, где выкладывают фотографии чужих локаций.

«Чтобы не потерять деньги, тщательно изучите предложение. Когда фотограф присылает примеры своих работ, проверьте их в поисковике через сервисы «поиска по картинке». Не исключено, что фотографии принадлежат совершенно другим людям. Внимательно изучите сайт фотостудии. Если нет никаких контактов, кроме аккаунта в мессенджере — это тревожный знак. Студия должна сказать вам свой адрес. В идеале стоит заранее туда съездить и посмотреть залы для съемки. Будьте крайне осторожны при переводе денег за аренду. Если сайт студии окажется фишинговым, мошенники могут опустошить ваши счета», — предупредил эксперт по кибербезопасности.