Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Интернет-мошенники не дремлют | Les fraudeurs ne dorment pas

Author: Заррина Салимова, , 22.11.2023.

Фото: Dimitri Karastelev, Unsplash

В последнее время в Швейцарии активизировались злоумышленники, использующие мессенджеры и социальные сети. Что нужно знать, чтобы не попасть в ловушку?

|

Récemment, en Suisse, les cybercriminels utilisant les messageries et les réseaux sociaux sont devenus plus actifs. Que faut-il savoir pour ne pas tomber dans le piège?

Les fraudeurs ne dorment pas

Национальный центр кибербезопасности (NCSC) регистрирует все больше сообщений о мошенничестве, к которым относятся например, предложения о фиктивной работе. Швейцарские абоненты на протяжении уже нескольких недель получают бесчисленные звонки, а также сообщения через SMS, WhatsApp, Telegram и другие мессенджеры с предложением получить значительную прибыль за несложную работу. По сообщениям Le Temps, только в кантоне Во десяток жертв потеряли таким образом в общей сложности 130 000 франков, причем половину этой суммы заплатил злоумышленникам один человек.

Сообщения выглядят правдоподобно и приходят от неких Амелии, Беатрис или Люка, которые утверждают, что представляют швейцарские компании, например, PageGroup Switzerland или Stellenpartner AG Schweiz. Они пишут на английском, иногда – на немецком языке, отвечая с разницей в несколько часов или даже минут, что создает иллюзию, что с вами связываются реальные люди. «Работа» состоит в том, чтобы оценивать, например, отели на сайте Expedia и зарабатывать от 400 до 700 евро в день. Если собеседник проявляет интерес и отвечает, то рекрутер поручает ему оценить отели на онлайн-платформах. Виртуальный заработок отображается в криптовалютных кошельках и за четверть часа может быстро составить около тридцати франков, стремительно увеличиваясь. Правда, чтобы обналичить деньги, нужно... заплатить. В одном из случаев жертва была вынуждена внести более 19 тысяч франков, чтобы получить «зарплату» в размере 12 тысяч.

Мошенничество носит массовый характер: в NCSC в настоящее время еженедельно поступает более двух тысяч жалоб. Сколько именно людей уже стали жертвами киберпреступников, узнать невозможно, так как не все обращаются в полицию. Учитывая тот факт, что подобные кампании проводятся в больших масштабах, даже незначительный процент обманутых людей может принести злоумышленникам прибыль.

Логично, что многих интересует вопрос: каким образом преступники получили доступ к нашим телефонным номерам. Вариантов немало – украв персональные данные, купив уже украденную базу данных в даркнете, легально приобретя данные у провайдеров бесплатных услуг, которые таким образом зарабатывают деньги. Мы сами оставляем номера при регистрации на онлайн-платформах, в конкурсах или рекламных кампаниях – эта информация может быть передана или перепродана третьим лицам, причем мы нередко нажимаем на кнопку «принять условия», даже не читая их.

Иногда мошенники действуют более тонко: звонящие представляются сотрудниками информационного центра медицинского страхования и предлагают скидки на страховые взносы. Верить этим заманчивым предложениям не стоит. Не стоит верить и в том случае, если вам звонят представители полиции, таможни, Интерпола или Международного суда и говорят, что посылка с наркотиками перехвачена, а ордер на ваш арест уже выписан.

Как же реагировать на сообщения мошенников? Игнорировать и блокировать их, по возможности жалуясь на них с помощью специальной функции в приложении. Тем же, кто понес финансовые потери, стоит обратиться в полицию. Помните, что с помощью современных платформ можно подделать номер телефона любой страны: если на экране отображается швейцарский номер, то это еще не значит, что звонок сделан из Швейцарии. Немедленно кладите трубку, если вам позвонил «сотрудник Европола». Если вы предоставили данные кредитной карты, то свяжитесь с банком,

чтобы заблокировать ее. То же самое стоит сделать, если вы совершили платеж – в некоторых случаях транзакцию еще можно остановить. Не предоставляйте никому удаленный доступ к своему компьютеру или телефону.

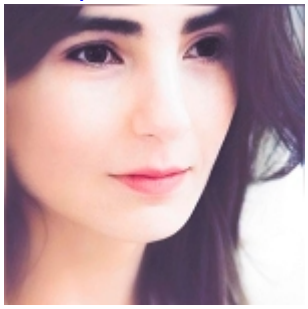
Осторожность стоит проявлять не только при получении сообщения от незнакомого лица, но и в том случае, если оно отправлено от одного из ваших контактов. Например, кто-то из ваших знакомых связывается с вами по WhatsApp и просит помочь в решении срочной проблемы. Все, что нужно сделать, – это отправить код, который пришел вам по SMS. В этот момент возникает соблазн оказать другу услугу, ведь простая передача кода ничего не стоит. Однако несколько мгновений спустя ваш собственный аккаунт WhatsApp будет заблокирован, и вы больше не сможете отправлять и получать сообщения.

Как поясняется в коммюнике NCSC, при таком виде мошенничества аккаунт связавшегося с вами человека уже взломан и контролируется хакером. Получив доступ к списку контактов жертвы, преступник может попытаться получить контроль над другими учетными записями. Для этого необходимо подтвердить, что именно он является владельцем номера, связанного с учетной записью, поэтому хакеру необходимо узнать и ввести шестизначный код, отправленный на устройство законного владельца номера. Каждая следующая скомпрометированная учетная запись приносит новые контакты, которые преступники пытаются обмануть. При этом они не могут прочитать разговоры, так как они записываются локально на устройствах отправителя и получателя сообщений.

Взломав учетную запись в WhatsApp, мошенники могут шантажировать жертву, требуя заплатить определенную сумму за возврат аккаунта; рассылать спам, в частности, со ссылками на фишинговые страницы или рекламу инвестиционных афер; использовать учетную запись в мошеннических объявлениях, что может оказаться удобным для преступников, действующих из-за рубежа и пытающихся выдать себя за швейцарцев.

Чтобы защитить себя, не передавайте полученные коды третьим лицам. В случае сомнений вы всегда можете позвонить запрашивающему код человку и выяснить причину. Всегда активируйте двухфакторную аутентификацию в WhatsApp. Установите шестизначный код, без которого в будущем невозможно будет перенести учетную запись WhatsApp на другое устройство. Эти же меры можно использовать и для защиты аккаунтов в Facebook или Instagram. Если кто-то уже взломал вашу учетную запись, то предупредите свои контакты о том, что от вашего имени им могут быть отправлены мошеннические сообщения.

мошенничество в интернете
интернет-мошенничество



Заррина Салимова
Zaryna Salimava

Статьи по теме
Внимание! Мошенничество с банковскими картами
Остерегайтесь онлайн-мошенников
Интернет-мошенники действуют под маской швейцарской таможни
Типичный профиль финансового мошенника
Вниманию мошенников
Все хотят использовать наши данные, но кто будет их защищать?
