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

Уловки мошенников в Twint | Les astuces des fraudeurs dans Twint

Auteur: Заррина Салимова, Берн , 19.12.2023.

Фото: Jonas Leupe, Unsplash

В преддверии праздников пользователям популярного швейцарского платежного приложения не стоит терять бдительность.

|

À l’approche des fêtes de fin, les utilisateurs de la populaire application de paiement suisse doivent rester vigilants.

Les astuces des fraudeurs dans Twint

Денежные переводы, покупки, оплата парковки – около пяти миллионов жителей Швейцарии регулярно используют для этих целей Twint. Учитывая популярность, простоту и удобство этого приложения, не приходиться удивляться тому, что мошенники пытаются ввести пользователей в заблуждение с помощью все более изощренных трюков.

На одну из получивших распространение в последнее время мошеннических схем обратило внимание издание Le Temps. Речь идет об электронных письмах от отправителя «Twint-Community». «Мы хотели бы сообщить, что все функции были заблокированы и что ваша учетная запись больше не активна. Если вы хотите продолжать пользоваться нашими услугами, мы просим вас пройти процедуру верификации, чтобы мы могли снять блокировку с вашего аккаунта. В противном случае ваш аккаунт будет заблокирован навсегда», - говорится в сообщении, к которому для достоверности прикреплен логотип платежного сервиса. Нажав на ссылку, пользователь попадает на страницу, где ему будет предложено выбрать банк, а затем ввести личные данные. Сделав это, пользователь передаст мошенникам данные своей карты и счета. Как правило, веб-браузеры предупреждают о том, что это может быть попыткой мошенничества.

В других письмах мошенники просят получателя предоставить платежные данные для проверки счета. Иногда подобные ссылки работают только на мобильных телефонах – таким способом злоумышленники надеются обойти анализ и блокировку фишинговой страницы.

Киберпреступники могут действовать и с помощью QR-кодов. Мошенники, например, заказывают подарочные сертификаты на определенную сумму у легального онлайн-продавца, выбирая Twint в качестве способа оплаты. Одновременно они публикуют на какой-нибудь популярной онлайн-платформе объявление о продаже товара на ту же сумму. Получив от продавца QR-код или шестизначный код для оплаты, мошенник передает его жертве, откликнувшейся на объявление. Таким образом, жертва напрямую оплачивает заказанный злоумышленником подарочный сертификат, думая при этом, что оплачивает свою покупку.

В кантоне Во мошенники выдают себя за представителей власти, требуя оплатить через приложение штраф в размере 500 франков.

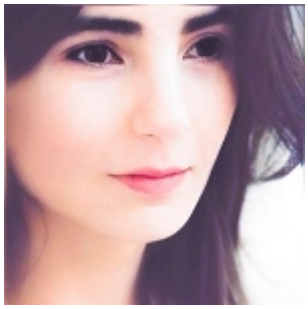
Фальшивые сообщения распространяются и в социальных сетях. В одном из «конкурсов» пользователям предлагалось просто напечатать слово «Twint» в комментариях под постом, после чего они получали сообщение через приложение Messenger в Facebook о призе в размере одной тысячи франков. Затем нужно было открыть Twint и ввести код – и со счета невнимательной жертвы списывалась сумма. Некоторые также могут отправлять случайные запросы на оплату непосредственно через Twint, поэтому следует внимательно изучать каждый запрос.

Денежные операции через Twint выполняются очень быстро – в этом заключается преимущество приложения. Но в этом же и его недостаток: секундная невнимательность может привести к ошибке или к отправке слишком большой суммы денег. Согласно Twint, заполнив специальную форму на сайте, можно получить деньги обратно от банка-получателя. Но, как сообщает издание 24 heures, это не всегда просто, так как банки и Twint предусматривают исключения. В возмещении, например, может быть отказано, если клиент подтвердил платеж по неосторожности.

Добавим, что Национальный центр кибербезопасности регистрирует рост случаев использования искусственного интеллекта для фишинга и попыток мошенничества. Преступники могут загрузить снимки из открытого профиля жертвы в социальных сетях и сгенерировать на этой основе изображения и видеоматериалы, которые очень трудно отличить от настоящих. Фальшивка может использоваться для монтирования секс-видео и последующего шантажа. С помощью ИИ можно подделать даже голос человека. Голосовые сообщения применяются, например, для шоковых звонков: вам якобы звонит сотрудник полиции и объясняет, что сын или дочь попали в аварию, а вам нужно внести залог. В качестве доказательства проигрывается сфабрикованная запись.

Эксперты напоминают, что не стоит переходить по ссылкам в электронных письмах или текстовых сообщениях. Если вы перешли по такой ссылке, то не вводите пароли, коды или данные кредитных карт. Если вам сообщают, что кто-то из членов семьи попал в беду, повесьте трубку и свяжитесь с человеком напрямую по другому каналу. Обратитесь в полицию, если вас шантажируют компрометирующими фотографиями. Будьте осторожны с фото и видеозаписями, которые вы публикуете для всеобщего обозрения. В общем, дорогие читатели, оставайтесь начеку!

мошенничество в интернете
мошенники в швейцарии



Заррина Салимова
Zaryna Salimava

Статьи по теме
Интернет-мошенники не дремлют
Вниманию мошенников
Внимание! Мошенничество с банковскими картами
Интернет-мошенники действуют под маской швейцарской таможни
Apple Pay, Twint и швейцарские пользователи
Как не стать жертвой обмана, покупая в интернете?

Source URL: *http://www.nashagazeta.ch/news/economie/ulovki-moshennikov-v-twint*