

В Сети оказалось более миллиона SMS с кодами двухфакторной аутентификации (2FA), которые были перехвачены исследователем информационной безопасности. Инсайдер сообщил об этом с целью привлечь внимание к несовершенству метода защиты аккаунтов от взлома.

Когда какой-либо сервис отправляет пользователю SMS с кодом для 2FA, то зачастую это осуществляется через посредников. В этом случае коды для 2FA рассылала малоизвестная швейцарская телеком-компания Fink Telecom Services, как оказалось, связанная с правительственными разведывательными агентствами и фирмами, занимающимися цифровой слежкой.

Исследователь предоставил более миллиона кодов 2FA, отправленных в июне 2023 года. Предполагается, что коды были перехвачены из-за проблем с безопасностью Fink Telecom Services и протокола передачи информации SMS.

Проблема с SMS-сообщениями заключается в их незашифрованности, что делает коды уязвимыми для перехвата. При этом утечка значительная, среди адресатов крупные компании, банки, приложения, крупная криптовалютная биржа и мессенджеры.

Получатели кодов находились в более чем 100 странах на пяти континентах.