Почему полагаться на двухфакторную аутентификацию – не лучшая идея?

В наши дни двухфакторная Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, которая проводится с помощью криптографической обработки, позволяющей защитить передаваемые данные от злоумышленников.

 Система аутентификации включает в себя несколько элементов: субъект (лицо, которое проходит процедуру аутентификации), характеристика субъекта (отличительная черта), человек, несущий ответственность и контролирующий работу системы аутентификации, механизм аутентификации, а также механизм, который предоставляет или лишает субъекта определенных прав доступа. Одним из способов аутентификации является ввод учетных данных (логина и пароля) пользователя. Эталонные учетные данные хранятся в специальной базе данных. Вводимый субъектом пароль может передаваться по сети двумя способами: в незашифрованном виде, на основе протокола парольной аутентификации, а также с использованием шифрования или однонаправленных хэш-функций." data-html="true" data-original-title="Аутентификация" >аутентификация (2FA, или двухфакторная аутентификация, — это метод дополнительной защиты аккаунта, который помимо пароля требует ввод дополнительного кода или подтверждения при входе. Это может быть код, отправленный на мобильный телефон или электронную почту, или код, полученный с помощью мобильного приложения-аутентификатора. Это добавляет дополнительный слой безопасности, поскольку для входа нужно иметь не только пароль, но и устройство или доступ к электронной почте или мобильному телефону.
 Метод позволяет защитить аккаунт от несанкционированного доступа, даже если кто-то узнает ваш пароль." data-html="true" data-original-title="2FA" >2FA) стала стандартом безопасности для большинства веб-сайтов и онлайн-сервисов. Некоторые страны даже приняли законы, обязывающие определенные организации защищать учетные записи пользователей с помощью 2FA. Однако популярность этой меры привела к развитию множества методов ее взлома или обхода, постоянно эволюционирующих и адаптирующихся к современным реалиям.

Согласно новым данным, злоумышленники все чаще используют так называемые OTP-боты для кражи кодов 2FA. Эти нехитрые программы представляют серьезную угрозу как для пользователей, так и для онлайн-сервисов.

OTP-бот — это программное обеспечение, предназначенное для перехвата одноразовых паролей с помощью социальной инженерии. Функциональность ботов варьируется от простых сценариев для определенных организаций до высоко настраиваемых конфигураций с широким набором сценариев на разных языках и с различными голосами.

Типичная схема мошенничества с использованием OTP-бота включает следующие шаги: злоумышленник получает учетные данные жертвы и пытается войти в ее аккаунт, жертва получает одноразовый пароль на телефон, OTP-бот звонит жертве и, следуя заранее подготовленному скрипту, убеждает ее поделиться кодом. Жертва вводит код верификации, не прерывая звонок, а злоумышленник получает этот код через специальную панель управления или Telegram-бота и использует его для входа в учетную запись.

Разработчики ботов стараются сделать их максимально привлекательными для злоумышленников. Например, один OTP-бот предлагает более дюжины функций, включая круглосуточную техническую поддержку, скрипты на различных языках, возможность выбора женского или мужского голоса, а также подмену номера звонящего.

Для большей убедительности некоторые OTP-боты могут демонстрировать на экране телефона жертвы официальный номер организации, от имени которой они звонят. Боты также способны определять, если звонок переадресован на голосовую почту, и завершать вызов. Разработчики ботов конкурируют, стараясь включить максимум функций по привлекательной цене — стоимость подписки может достигать 420 долларов в неделю.

Помимо OTP-ботов, мошенники также используют многоцелевые фишинговые наборы для перехвата одноразовых паролей в реальном времени. Эти наборы имитируют веб-сайты банков, платежных систем, онлайн-магазинов, облачных сервисов, служб доставки, криптобирж и почтовых сервисов, запрашивая у жертв личные данные, включая логины, пароли, коды 2FA, номера банковских карт, CVV-коды и даже даты рождения.

В ходе многоэтапной фишинговой атаки жертва сначала вводит свои учетные данные на поддельном сайте, а затем, когда требуется ввести одноразовый пароль для дополнительной верификации, на этом же сайте появляется форма для ввода кода. После получения OTP злоумышленники могут запрашивать у жертвы еще больше конфиденциальных сведений под предлогом подтверждения личных данных.

Некоторые боты позволяют заранее отправить жертве СМС с предупреждением о предстоящем звонке от сотрудника какой-либо компании. Это психологический трюк, призванный завоевать доверие человека — сначала обещание, а потом его исполнение. Тревожное сообщение также может заставить в напряжении ждать звонка.

Статистика Лаборатории Касперского показывает, что в мае 2024 года их инструменты предотвратили 69 984 попытки посетить сайты, созданные с помощью фишинговых наборов, нацеленных на банки. Также было обнаружено 1262 фишинговые страницы, сгенерированные 10 многоцелевыми наборами для перехвата OTP.

Пик активности фишинговых страниц пришелся на первую неделю мая и совпал с всплеском деятельности одного из наборов. Эксперты отмечают, что мошенники могут получать исходные данные жертв, такие как логины, пароли, номера телефонов из утечек в интернете, на темном рынке или с помощью фишинговых сайтов.

Для защиты своих учетных записей от мошенников эксперты рекомендуют:

Не открывать подозрительные ссылки напрямую — вводить адреса веб-сайтов вручную или использовать закладки;

Проверять корректность адреса сайта перед вводом учетных данных и использовать Whois для проверки даты регистрации;

Не произносить и не вводить одноразовые пароли во время телефонных звонков;

Использовать надежные антивирусные решения, блокирующие фишинговые страницы.