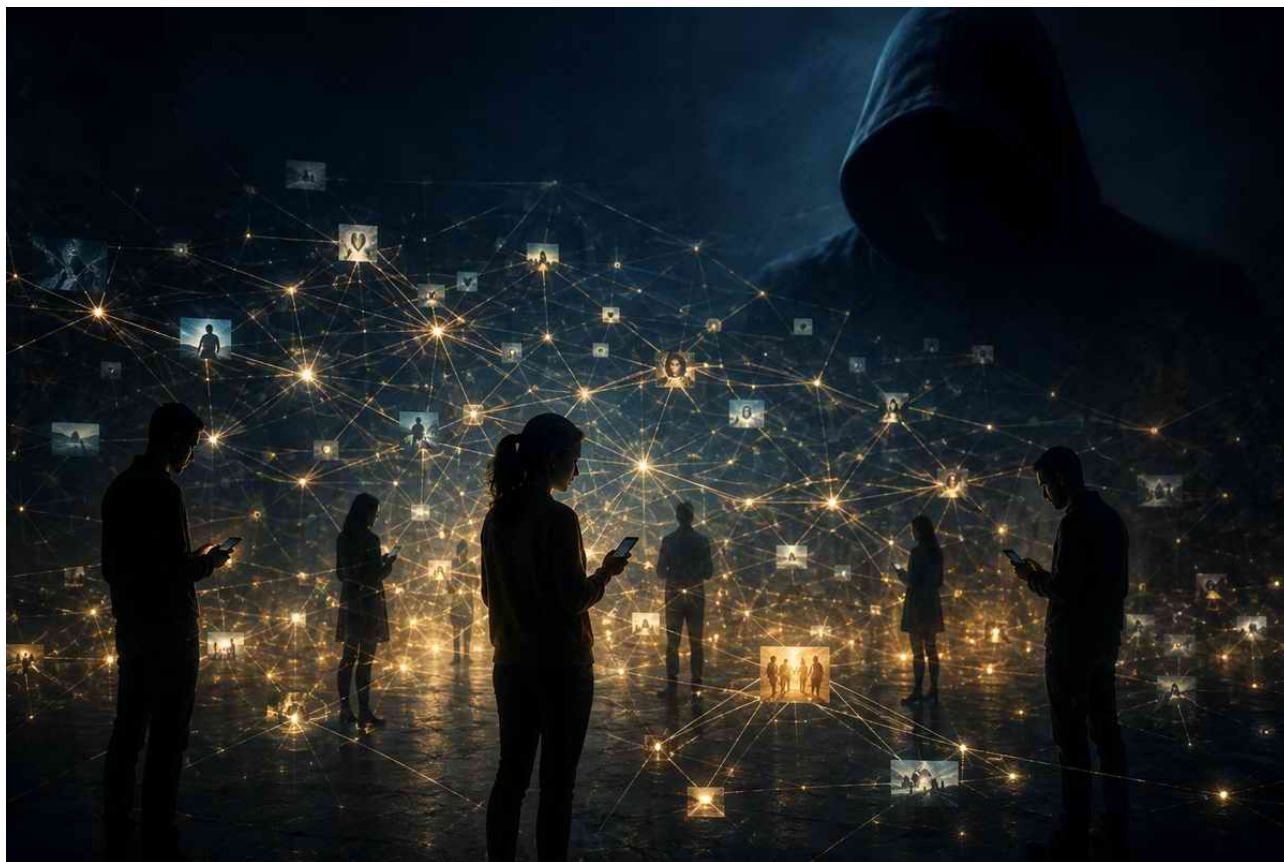


Даже длина онлайн-отзывов может раскрыть ваших друзей мошенникам



Дата публикации: 31.08.2026

Оставляя отзыв о ресторане, гостинице или интернет-магазине, человек вряд ли думает, что количество написанных им слов способно рассказать что-то о его друзьях. Имя можно скрыть, список контактов закрыть, профиль сделать почти анонимным, однако поведение пользователя тоже оставляет цифровые следы. Новое исследование показывает, что даже такой безобидный параметр, как длина онлайн-отзывов, позволяет с неожиданной точностью восстанавливать социальные связи между людьми.

Исследователи из Техасского университета в Остине и нескольких других университетов изучили проблему применительно к целевому фишингу. В отличие от массовых писем с очевидными обещаниями выигрыша, такая атака создается под конкретного человека. Мошенник может представиться знакомым, коллегой или родственником и попросить срочно перевести деньги, открыть документ, сообщить пароль или перейти на поддельную страницу.

Для подобной схемы особенно ценна информация о том, кому потенциальная

жертва доверяет. Социальные сети иногда позволяют скрыть список друзей, а на сайтах отзывов его может вообще не быть. Но это еще не означает, что связи невозможно восстановить косвенно. Исследователи предположили, что своеобразной картой отношений способно стать само поведение пользователей.

Для проверки гипотезы ученые проанализировали активность 4299 пользователей Yelp из Луизианы и Пенсильвании за 2020 год. Эта площадка оказалась удобной исследовательской моделью: доступны были как отзывы, так и реальные связи между пользователями. Сначала алгоритм пытался определить возможные знакомства только по поведению людей, а затем полученные результаты сравнивали с настоящими списками друзей.

Результат оказался достаточно высоким, чтобы обратить на него внимание специалистов по цифровой безопасности. Используя поведенческие признаки, можно было правильно определить около 49% социальных связей при 10% ошибочных совпадений. Если допустить увеличение доли ложных срабатываний до 20%, обнаруживалось уже до 63% реальных связей. Иными словами, даже без непосредственного доступа к контактам пользователя можно восстановить значительную часть его социального окружения.

Особенно неожиданным оказался один из наиболее информативных признаков — длина отзывов. У связанных между собой пользователей наблюдались характерные закономерности. Иногда один человек начинал писать более развернутые отзывы вслед за другом, словно перенимая его стиль поведения. В других случаях возникала противоположная модель: длинный отзыв одного пользователя сопровождался коротким дополнением другого.

Такой эффект вполне объясним с точки зрения социальной психологии. Люди постоянно влияют друг на друга, зачастую не замечая этого. Мы перенимаем выражения, способы общения, привычки, предпочтения и модели поведения. В реальной жизни подобная синхронизация помогает поддерживать отношения, однако в цифровой среде она превращается в измеримый сигнал. Компьютерному алгоритму необязательно понимать содержание текста, если достаточно сравнить его структуру и другие характеристики.

Для мошенника восстановленная сеть знакомств представляет гораздо большую ценность, чем набор случайных адресов электронной почты. Зная вероятную связь между двумя людьми, можно подготовить персонализированное сообщение: сослаться на знакомого, организацию, место или событие. Такая атака выглядит правдоподобнее обычного спама, а значит, вероятность того, что получатель откроет письмо или выполнит просьбу, возрастает.

Исследователи даже смоделировали экономику подобных атак. По данным

выборки из Пенсильвании, увеличение количества попыток позволяло резко повышать потенциальную отдачу злоумышленника. При масштабировании до тысяч сообщений возможность автоматически находить вероятные социальные связи становится особенно опасной: преступнику уже не требуется вручную изучать каждого человека.

Проблема выходит далеко за пределы сайтов с отзывами. Похожие поведенческие следы возникают на торговых площадках, в социальных сетях, сервисах путешествий и на платформах обмена медиаконтентом. Частота публикаций, время активности, оценки, объем текста и последовательность действий по отдельности могут выглядеть безобидно, но их сочетание способно раскрывать информацию, которую пользователь никогда напрямую не публиковал.

Именно здесь возникает новая проблема цифровой приватности. Традиционный подход предполагает защиту очевидных персональных данных: имени, адреса, телефона, списка контактов. Но современные методы анализа позволяют получать новые сведения путем сопоставления данных, которые сами по себе секретными не являются. Скрыть список друзей оказывается недостаточно, если алгоритм способен частично восстановить его по косвенным признакам.

Одним из возможных способов защиты исследователи называют добавление информационного шума. Платформа может слегка изменять публикуемые характеристики данных так, чтобы они оставались полезными для обычного пользователя, но хуже подходили для построения поведенческой модели. Теоретически можно, например, варьировать некоторые параметры текста без изменения его основного смысла.

Компьютерное моделирование показало, что такой подход способен уменьшать точность восстановления социальных связей и одновременно снижать экономическую привлекательность фишинговых атак. Однако слишком сильное искажение данных тоже нежелательно: платформам необходимо сохранять отзывы полезными для читателей, бизнеса и собственной аналитики. Поэтому защита превращается в поиск баланса между информативностью и приватностью.

Исследование напоминает о важной особенности современной цифровой среды: конфиденциальность определяется уже не только тем, какую информацию человек добровольно раскрыл. Не менее важно то, какие дополнительные сведения можно вычислить из совокупности его действий. Обычный отзыв о кафе кажется совершенно безопасным, но сотни подобных цифровых мелочей способны складываться в довольно подробный портрет

пользователя и его окружения.

Ссылка: «Когда поведенческие данные обманывают пользователей: диагностическая и защитная структура против утечки информации о социальном взаимодействии» [DOI: 10.1287/isre.2024.1469](https://doi.org/10.1287/isre.2024.1469).