БЕЗОПАСНОСТЬ

Сеть и золотые горы

Около 20% жителей Тверской области, которые пытаются заработать в интернете, становятся жертвами мошенников в первые дни поиска работы

Работа уходит в интернет

Различные исследования говорят о том, что скоро почти каждый пятый россиянин будет работать удаленно. Но пока точное число работников, трудящихся вне офиса, посчитать невозможно. В России просто не существует подобных систем учета. Зато есть статистика других стран. Совместное исследование Всемирной организации труда и Европейского фонда по улучшению условий жизни и труда показало, что в развитых странах в среднем 17% сотрудников работают дистанционно. Лидеры по этим показателям с 40% являются Япония и США. Отметим, что в эту статистику входят как сотрудники, постоянно работающие удаленно, так и те, кто трудится вне основного рабочего места время от времени.

Большинство удаленных сотрудников — консультанты и менеджеры различного уровня. Более 60% удаленных сотрудников работают дома, остальные на рабочих местах, организованных самостоятельно или работодателем. Отметим, что в эту статистику не входят различные фрилансеры, поэтому процент людей, работающих удаленно, может быть даже выше, чем по данным исследования.

Многие компании в России тоже используют практику удаленной работы, но их число неизвестно. Рынок удаленной работы в России только формируется.

Кто становится жертвой мошенников

Просторы Рунета пестрят различными привлекательными объявлениями: от традиционных до экзотических. Различные компании постоянно ищут себе на удаленную работу или подработку копирайтеров, дизайнеров, видеографов, наборщиков текстов, программистов и других фрилансеров. Во Всемирной паутине можно встретить огромное количество предложений заработать с помощью нетрадиционных и с виду очень выгодных способов. Речь идет об играх на бирже, криптовалютах и различных схемах бизнеса, которые якобы не требуют или почти не требуют никаких первоначальных вложений и усилий.

Федеральный проект «Кибердружина», штаб-квартира которого находится в Твери, помогает полиции расследовать киберпреступления и уже более двух лет проводит для школьников, студентов и взрослых людей мастер-классы по информационной безопасности. По данным проекта, еще два года назад только 10% жителей Тверской области знали основы информационной гигиены. Постепенно их число растет, однако многие до сих пор попадаются в сети мошенников.

— По нашим данным, 20% жителей региона становятся жертвами мошенников в первые три дня поиска работы в Сети, — рассказывает руководитель «Кибердружины» Григорий Пащенко. — Большинство из них теряют большие суммы денег, данные своих паспортов и банковских карточек.

Практика показывает, что в первую очередь жертвами мошенников становятся школьники и студенты, которые ищут подработку на биржах фрилансеров и различных сервисах объявлений. Сотрудники «Кибердружины», проводя анализ сотни ресурсов, пришли к выводу, что доверять можно только трем из них. Речь идет о самых известных в стране биржах фрилансеров www.freelance.ru и www.fl.ru, а также о сайте для поиска работы hh.ru.

Но даже на этих ресурсах есть мошенники. Чтобы не стать их жертвами, Григорий Пащенко рекомендует пользоваться услугой «Гарант-сервис». За небольшой процент от сделки администрация ресурса выступит посредником между заказчиком и исполнителем, а также поможет решить все возможные спорные моменты.

Те, кто предпочитает напрямую общаться с заказчиками, может стать жертвами мошенников. В данный момент «Кибердружина» расследует случай мошенничества, который произошел с молодым жителем Тверской области. Он отозвался на предложение о подработке на сайте www.fl.ru. Заказчик предложил ему совершить сделку на стороннем ресурсе. Далее молодого человека убедили в том, что если он купит платную подписку, то получит доступ к большему числу предложений. Он перевел деньги, но доступа не получил. Вскоре сайт прекратил работу, а мошенники перестали отвечать на письма. Молодой человек обратился в полицию и в «Кибердружину».

К слову, на www.fl.ru и www.freelance.ru тоже есть платная подписка, но за нее пользователь получает различные дополнительные сервисы. Брать заказы на этих биржах можно и совершенно бесплатно.

— Сами биржи фриланса не могут ничего поделать со случаями мошенничества. Администрации ресурсов готовы заблокировать аккаунты злоумышленников, но этого недостаточно, — рассказывает Григорий Пащенко. — Мошенники скрывают свои ip-адреса через VPN и сеть TOR. Есть шанс найти их через транзакции платежей, которые совершаются через разные системы. Распутать цепочку перевода денег можно, но, во-первых, это трудоемкий процесс, во-вторых, не все платежные организации готовы тратить время на обработку запросов о предоставлении данных.

Но все более искусными становятся не только мошенники, но и те, кто их ловит. «Кибердружина» использует автоматическую систему «Zeus». Она работает по принципу нейросетей, поэтому постоянно развивается. Так, сейчас с помощью этой системы можно отследить цифровой отпечаток мошенника. При его формировании учитываются не только IP-адреса и другие открытые данные, но даже стилистика написания его сообщений. Например, одного мошенника поймали потому, что он случайно оставил свой IP-адрес на форуме, который не имел отношения к его деятельности по обману людей. Система, проведя анализ, увидела, что стиль письма мошенника соответствует стилю написания сообщений пользователя форума. Далее по IP-адресу человек был легко и быстро найден.

— Многие жертвы мошенников не обращаются в полицию, потому что боятся волокиты и не верят, что это даст результат. Я же по опыту знаю, что на подачу заявления в полицию не уходит много времени. Главное — грамотно подготовиться: указать время и даты, когда мошенники выходили с вами на связь, распечатать переписку с ними, указать, с каких устройств вы выходили в Сеть, куда и с каких счетов перечисляли деньги, — говорит Григорий Пащенко. — Тогда правоохранительные органы смогут составить полную картину преступления.

В полиции у пострадавшего могут попросить на экспертизу технику, но не стоит этого бояться. Опасаться стоит только тем, кто хранит на своих компьютерах противоправный контент или сам занимается мошеннической деятельностью, следы которой остались на его цифровых устройствах.

Как себя обезопасить

Для того, чтобы не стать жертвой мошенников, нужно не только заключать безопасные сделки, но и как можно меньше оставлять в Сети открытых данных. Расследуя вышеописанный случай мошенничества, сотрудники «Кибердружины» выяснили, что злоумышленники предварительно анализировали своих жертв. Например, они проверяли, являются ли их аккаунты в социальных сетях настоящими, а затем проводили их анализ. Все это происходит в автоматическом режиме и занимает совсем немного времени. Составив психологический портрет человека, мошенники подбирают к нему ключи.

В прошлом году произошел взлом крупнейших в России вещевых интернет-магазинов. Их базы данных и сейчас можно найти в Сети. В них есть телефон, электронная почта, адрес проживания человека и номер его заказа. Такие базы служат мошенникам подспорьем для составления психологического портрета человека.

Часто в Сети можно найти и паспортные данные граждан России. Купить их можно всего за 300 рублей. Григорий Пащенко рассказывает о том, что большая часть утечек происходит в микрофинансовых организациях. Сотрудники МФО, выдавая займ, сканируют паспорт, а затем продают его данные на черный рынок всего за 200 рублей.

Паспортные данные мошенники могут использовать как ключ для получения доступа к жизни человека. Например, они обращаются в администрацию социальных сетей и заявляют об утрате доступа к якобы своей страничке. Когда он получен, мошенники забирают из нее все документы, фотографии и даже личную переписку.

На паспорт человека также могут зарегистрировать какую-нибудь компанию или ИП, получить кредит и совершить другие действия, о которых человек даже не будет догадываться.

Также не стоит оставлять в Сети свой основной номер телефона и даже не пользоваться бесплатным Wi-Fi. Данные о сайтах, которые вы просмотрели, например, за чашкой чая в кафе, могут уже вечером быть проданы. Так, однажды на телефон маленькой девочки позвонила туристическая компания с предложением купить путевку в Египет для всей семьи. Выяснилось, что за два дня до этого с данного телефона мама девочки, сидя в кафе, искала путевки в Египет. Конечно, она использовала бесплатный Wi-Fi.

Еще один способ себя обезопасить — повысить уровень своих знаний. «Кибердружина» и ресурсный центр ассамблеи народов России проводят бесплатное и платное обучение для иностранцев и жителей России, которые хотят повысить свою информационную грамотность.

Руководитель института межнационального единения и разработки комплексных алгоритмов безопасности IT-пространства Елена Машетова рассказала нашему еженедельнику о том, что иностранцы, которые приехали в Тверь, тоже часто становятся жертвами мошенников. Покупаясь на красивые условия в различных объявлениях, они теряют время и деньги и даже невольно становятся закладчиками наркотиков. Такие случаи в нашем городе уже были.

Блокчейн поможет заработать

Григорий Пащенко считает, что зарабатывать в интернете можно. Главное, быть бдительным и всесторонне проверять потенциального работодателя. И, конечно, если возникает подозрение или уже случаи мошенничества — обращаться в «Кибердружину» и в правоохранительные органы. Чем больше общество обращает внимание на этот вопрос, тем лучше. Появятся необходимые механизмы защиты и действенное законодательство в этой сфере.

А уже в ближайшем будущем честно заработать поможет технология блокчейн, о которой мы писали в прошлом номере. Напомним: ее суть в том, что все открытые данные видят все участники определенной системы. База данных хранится не в одном месте, а сразу на всех устройствах.

С помощью этой технологии на некоторых ресурсах уже сейчас можно заключать безопасные сделки — смарт-контракты. Когда контракт заключен, ни одна из сторон не сможет его изменить. При этом все участники системы будут видеть суть этого контракта. Обмануть просто не получится.

Главное, чтобы государство ввело эти сделки в законодательное поле. К слову, это может произойти уже совсем скоро. Законопроект, в котором будут дано определение смарт-контрактам, уже внесен в Государственную Думу. Ожидается, что он будет принят к июлю.

В данный момент тестируется множество систем, созданных на технологии блокчейн. Разумеется, они охватят и такую важную сферу, как удаленная работа, сделав ее более безопасной как для исполнителя, так и для заказчика.

Андрей САБЫНИН