



Практически ежедневно в правоохранительные органы, и в том числе в Следственный комитет, поступает информация о новых фактах телефонного мошенничества. Результаты анализа сообщений о мошеннических действиях неизвестных лиц, совершаемых по телефону, позволяют сделать вывод, что злоумышленники становятся все изощреннее и изобретательнее. Для реализации преступного умысла они зачастую используют IT-технологии и программное обеспечение, а также поддельные документы с реквизитами различных государственных органов и банковских организаций.

Еще раз напоминаем гражданам о необходимости проявлять бдительность. Следственный комитет обращает внимание на следующую распространенную схему, которую используют мошенники, а также предлагает возможный алгоритм действий для тех, кто столкнулся с подобной ситуацией:

*- использование мошенниками системы автоматизированной подмены номеров, при этом нередко дозвон осуществляется несколько раз подряд с разных номеров.*

То есть на абонентской станции (на телефонном аппарате) отображается номер телефона, не соответствующий реальному номеру абонента, осуществляющего дозвон. Для этих целей используются специальные программные средства, в которых имеется поле для указания желаемого номера для отображения у конечного абонента – таким образом можно ввести абсолютно любой номер телефона.

**Важно !** Не следует перезванивать по входящим номерам, поскольку они отображаются некорректно – с подменой телефонного номера. Для получения информации и разъяснений необходимо вручную набрать телефонные номера, указанные на официальных сайтах государственных структур и банков.

*- требование в ходе телефонного разговора о явке по называемым адресам и убеждение в необходимости перевода денежных средств под различными предложениями на указанные звонящим лицом счета.*

Следователи СК России и сотрудники других правоохранительных органов, на которых возложены обязанности по проведению предварительного следствия, производят вызов граждан в порядке, установленном законодательством. Лица вызываются повесткой. При этом должностное лицо никогда не требует по телефону предоставления персональных данных и банковских реквизитов, информации по счетам и пластиковым картам.

**Важно !** Ни по телефону, ни в ходе очной беседы сотрудники правоохранительных органов (СК России, ФСБ России, МВД России, Росгвардии и другие) не заявляют требований о переводе денежных средств на какие-либо счета. Это незаконно. Любые

предложения о содействии правоохранительным органам, например, в поимке преступников путем перечисления денежных средств на указанные «собеседником» счета, либо с целью обезопасить сбережения от противоправных действий третьих лиц – это явный признак мошенничества, о чем необходимо сообщить в правоохранительные органы.

*- предоставление электронными и иными средствами связи поддельных документов, подтверждающих вымышленную мошенниками информацию для завладения денежными средствами.*

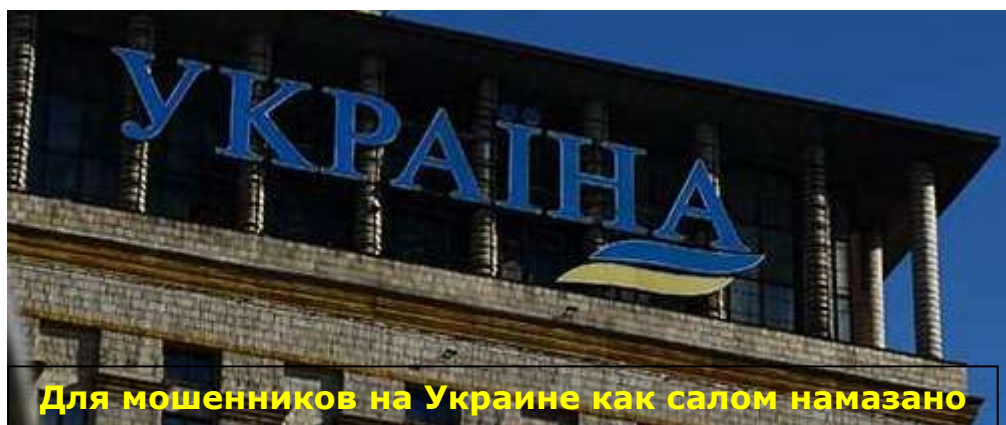
Мошенники, представляющие следователями и другими сотрудниками госорганов, в подтверждение своих слов предупреждают и реально направляют фальшивые «документы», и вновь просят перевести денежные средства под каким-либо предлогом. Как правило, используется адрес собеседника, который есть в открытом доступе.

**Важно !** В случае таких требований со ссылкой на отправленные документы стоит позвонить по номерам телефонов государственных органов или финансово-кредитных организаций, указанных на их официальных сайтах, и проверить подлинность полученного документа и достоверность сведений. При этом следует уточнять совокупность всех сведений.

Следует помнить, что в случае, когда потерпевший сообщает злоумышленнику о том, что сам перезвонит в государственные органы и финансовые организации для уточнения всей информации по данному вопросу, он может натолкнуться на провокации. Мошенники зачастую путем угроз и недостоверной информации пытаются убедить абонента не делать этого, поскольку якобы может произойти «разглашение определенных сведений, за что действующим законодательством предусмотрена ответственность». Данные заявления не являются правомерными и рассчитаны на запугивание абонента, который может растеряться и отказаться проверить поступившую информацию и достоверность документов.

Еще раз обращаем внимание граждан: не поддавайтесь уговорам, угрозам и влиянию телефонных мошенников и не переводите денежные средства на указанные ими счета. Сообщайте о таких фактах в органы полиции.

Если звонящий представился сотрудником правоохранительного органа – проверяйте озвученную им информацию по телефонам «горячих линий» соответствующего госоргана.



95% мошеннических звонков россиянам, по оценкам экспертов, поступает с территории Украины. Сегодня там работают 800–900 таких call-центров. Настоящей «столицей» телефонного мошенничества специалисты называют город Днепропетровск (Днепр). В том, почему Украина привлекает аферистов и как защититься от действий этих преступников, разбирались «Известия».

О том, что Украина стала главным центром, откуда телефонные мошенники звонят россиянам, заявил зампред Сбербанка Станислав Кузнецов, выступая на уральском форуме «Кибербезопасность в финансах».

**«Более 92–95% звонков в формате телефонного мошенничества совершается с территории Украины, — сообщил он. — Всего на Украине мы фиксируем 800–900 call-центров по всей территории».**

Кузнецов также добавил, что столицей телефонного мошенничества по-прежнему остается город Днепр - там работало более 1100 call-центров, а сейчас осталось примерно 150. Но сегодня российские специалисты стали знать в десятки раз больше о работе этих call-центров - что они делают, кому звонят и какие действия есть в их планах.

Судебный эксперт-психолог Олег Долгицкий указывает на ряд важных факторов, которые позволяют аферистам чувствовать себя на Украине вполне комфортно.

Во-первых, преступления против россиян там не влекут за собой уголовной ответственности, а, напротив, поощряются киевскими властями.

Во-вторых, уровень коррупции на Украине настолько высок, что попадание call-центров мошенников в поле зрения местных правоохранительных органов возможно лишь ради извлечения коррупционной выгоды, — говорит специалист.

Наконец, по словам Долгицкого, сегодня с украинской территории ведется информационная война против России. Деятельность телефонных мошенников в целом вписывается в парадигму этой войны. Схожей точки зрения придерживается и эксперт по кибербезопасности компании «Вебмониторэкс» Екатерина Старостина.

— Телефонное мошенничество - отнюдь не новое явление для Украины, где всегда были проблемы с борьбой с преступностью, - объясняет она.

— На текущий момент оно используется и как оружие, и как средство обогащения.

Таким образом, подчеркивают специалисты, на Украине сложилась идеальная социально-экономическая и политическая ситуация для работы мошеннических call-центров.

## Механизмы защиты

Несмотря на то, что деятельность телефонных мошенников на Украине достигла небывалого размаха, существуют простые правила, которые помогают не попасться на их крючок. Самое простое - вообще не принимать звонки с незнакомых номеров.

— Важно понимать, что, какими бы программно-аппаратными средствами и методами психологического воздействия ни пользовались киберпреступники, общая схема фрода (телефонного мошенничества) остается неизменной, - напоминает Сергей Гатауллин.

Главная задача аферистов - вывести человека из устойчивого психоэмоционального состояния, а затем гибкими методами социальной инженерии вынудить его предпринять действия, необходимые мошенникам. Именно поэтому никогда не следует передавать по телефону информацию, относящуюся к персональным данным. Между тем есть признаки, которые могут подсказать, что связаться с вами пытаются именно злоумышленники с контролируемой Киевом территории.

— Мошенников с Украины обычно выдают специфический говор, импровизация работы call-центра на фоне звонящего и ошибки в объяснении российского законодательства, — рассказывает Екатерина Старостина.

По словам собеседницы «Известий», если раньше такие аферисты обычно представлялись сотрудниками служб финмониторинга банков, то сейчас среди них стало популярно звонить от имени Центробанка РФ или Следственного комитета России (СКР). Однако банковский работник или сотрудник правоохранительных органов не будет действовать таким образом.

— Банку проще заблокировать ваш счет и дождаться, пока вы сами придете выяснять, в чем дело, - резюмирует эксперт. - А сотрудники правоохранительных органов вызовут вас повесткой или по телефону, но решать вопросы дистанционно никто не станет. Мыслите критически - повесьте трубку и перезвоните по официальному номеру. Если вам и правда звонили, то вас обязательно соединят.