

Как защититься от телефонных и электронных мошенников.

Электронные письма с вирусами Вы можете получить не только от имени налоговиков, но и от имени судебных приставов и многих прочих ведомств. Мошенники сообщают, что у компании долги по исполнительным листам, и всю информацию обещают привести во вложении. В итоге компьютер бухгалтера блокируется, и пропадают деньги со счетов.

Лучшая тактика, когда Вам звонит или пишет мошенник под видом чиновника, — не исполнять его требования, не скачивать файлы из письма и не переходить по ссылкам. Чиновники рекомендуют сразу связаться с ведомством, сотрудником которого представился звонивший или отправитель письма. Например, сообщить об инциденте по телефону доверия, а также в полицию.

Памятка: «Как защититься от мошенников».

I. При личном звонке от «чиновника»:

- Выясните данные инспектора и задайте вопрос, ответ на который знает только чиновник. Общедоступная информация может быть доступна и мошенникам.
- Игнорируйте и не перезванивайте по номерам, которые называют в телефонных разговорах. Проверяйте номера в разделе «Контакты и обращения» на сайте nalog.ru.
- Свяжитесь с инспекцией по телефону, который указан на сайте налоговиков. Запросите в инспекции официальный запрос на бумаге или по ТКС и ответьте письменно.

II. При получении электронного письма от «чиновника»:

- Проверьте адрес отправителя. У налоговиков всегда заканчивается на @nalog.ru.
- Игнорируйте вложения и ссылки. Потенциально опасные файлы заканчиваются на .exe, .bat.
- Пересылайте полученное письмо системному администратору. Опасно доверяться только антивирусу, который встроен в почту.

III. Когда убедитесь, что звонок или письмо поступили от мошенников, сообщите об этом в инспекцию или в полицию.

Ниже расскажем о схемах, которые используют злоумышленники, и дадим советы, как не попасть в их ловушку.

	Мошенническая схема	Как не попасть в ловушку.
1	<u>Переадресация на платный номер</u> — это один из новых способов мошенничества с использованием автоответчика, который сообщает о налоговой задолженности или несданной декларации и штрафах и предлагает срочно связаться с инспекцией по названному номеру. Иногда мошенники звонят несколько секунд, а затем сбрасывают звонок с расчетом на то, чтобы Вы на него не успели ответить и перезвонили. При соединении на другой стороне — тишина, и пока Вы ждете ответа, начисляется плата за соединение, которая идет в карман мошенникам.	ФНС не обзванивает налогоплательщиков в автоматическом режиме, а информирует компании и физических лиц только на официальном сайте nalog.ru и в операционных залах налоговых инспекций. 1. <u>Не перезванивайте по предложенным номерам</u> , если Вам позвонил неизвестный абонент, тем более из другого региона. 2. <u>Проверьте данные о расчетах и долгах в личном кабинете налогоплательщика</u> и обратитесь за разъяснениями в инспекцию по месту своего учета. 3. <u>Сообщайте инспекторам о фактах звонков с информацией о задолженностях по автоответчику</u> - такие номера будут блокировать, чтобы мошенники не смогли обмануть Ваших коллег. 4. <u>Когда видите пропущенный звонок с незнакомого номера, пробейте его в любом поисковике</u> . Там увидите отзывы обманутых пользователей. Если в поисковике номера нет, <u>проверьте контакты на сайте ФНС nalog.ru в разделе «Контакты и обращения».</u>
2	<u>Требования с вложенными файлами и ссылками</u> - это электронные письма под видом налоговых уведомлений и требований, где адрес	Такие документы налоговики не присылают на обычную электронную почту, а - либо выдают лично, либо направляют на бумаге заказным письмом, либо электронно через спецоператора. <u>ФНС России советует, как самостоятельно отличить</u>

<p>отправителя похож на налоговый, а содержание напоминает письма из инспекции.</p> <p>Название и текст письма составлены так, чтобы бухгалтер наверняка его открыл. В самом письме нет подробностей, их можно получить, только открыв вложенный файл или перейдя по ссылке в письме. Если этого не сделать, грозят штрафами и блокировкой счета.</p> <p>К таким письмам мошенники прикладывают вирусы в виде архивных файлов или ссылки на вредоносные программы. Они могут красть информацию, подменять данные в платежках и отправлять деньги на счета мошенников.</p> <p>Еще один вариант — вирус шифрует все данные на компьютере, в том числе базу бухгалтерской программы. За расшифровку мошенники требуют деньги.</p>	<p>настоящий запрос инспекции от подделки:</p> <ol style="list-style-type: none"> 1. <u>Обращайте внимание на техническую часть письма.</u> В поле «Return-Path:» будет реальный адрес отправителя письма, который может отличаться от того, что указан в поле «От:». Подделать адрес в технической части невозможно. В настоящих письмах от ФНС России указан домен @nalog.ru. Он же должен быть указан в полях «Message-ID:» и «Received:». 2. <u>Заранее уточните у представителей почтового сервиса, который используете в работе, поддерживают ли они эти механизмы защиты.</u> 3. <u>Своевременно обновляйте антивирусные базы, операционную систему и другие программы (почтовый клиент, браузер).</u> 4. <u>Не открывайте подозрительные письма, приложенные к письму файлы, и не переходите по ссылкам.</u> Пока файл не скачали и не запустили, опасности нет. Опасны файлы с расширением.exe или.bat. Это исполняемые файлы, то есть программы. 5. <u>Переправьте пришедшее письмо сисадмину или производителю Вашего антивируса для проверки.</u> 6. <u>Обращайте внимание на стиль письма</u> (в нем могут сообщать о задолженности по НДС, когда компания на упрощенке). 7. <u>Смотрите, как автор обращается к Вам.</u> На поддельное письмо указывает отсутствие данных о Вас или Вашей компании.
<p>3 <u>Платежки с липовыми реквизитами</u> — это еще один способ украсть деньги компании без прямого доступа к счету. Для этого мошенники под видом налоговиков присылают на электронную почту письмо о задолженности. К письму прилагают заполненную платежку и требуют оплатить задолженность именно по ней, ссылаясь на то, что реквизиты недавно изменились. За неуплату грозят блокировкой счета.</p> <p>Мошенники рассчитывают на то, что бухгалтер не заметит подмены и перечислит деньги.</p>	<p>Налоговики не информируют налогоплательщиков о задолженности по электронной почте. Всю информацию о долгах по налогам и взносам можно получить в интернет-сервисах на сайте ФНС.</p> <p><i>Пресс-служба ФНС России разъясняет, какие рассылки безопасны:</i></p> <ol style="list-style-type: none"> 1. <u>Официальная рассылка ФНС России направляется только тем, кто указал и подтвердил адрес своей электронной почты в сервисе «Личный кабинет налогоплательщика».</u> И там обычно указана информация об изменениях в личном кабинете налогоплательщика, о регистрации обращения в Службу и получении ответа на него. А формат ответа на обращение (.pdf, .xml) пользователь выбирает самостоятельно при обращении через сайт. 2. <u>Новостную рассылку сайта nalog.ru направляют пользователям сайта, которые оформили подписку, и дублируют на главной странице сайта.</u> 3. <u>Проходите перед отчетной кампанией сверки с налоговиками.</u> Так мошенникам будет сложнее ввести Вас в заблуждение насчет долгов. 4. <u>Всегда сверяйте реквизиты платежей, которые отправляете в банк.</u>
<p>4 <u>Расспросы о компании и сотрудниках.</u></p> <p>Мошенники звонят или присылают запросы с просьбой представить данные о сотрудниках или компании. Например, информацию о ее финансовом состоянии. Эти данные обычно интересуют рейдеров. Им нужны сведения об активах, обязательствах, выручке</p>	<p>Практические правила безопасной работы с электронными запросами:</p> <ol style="list-style-type: none"> 1. <u>Набирайте ссылки вручную, т.к. опасно кликать по ссылкам в письмах или копировать их в строку браузера.</u> Вид ссылки и реальный адрес, на который она указывает, могут различаться. 2. <u>Не предоставляйте данные о физлицах кому попало</u> — это опасно! Роскомнадзор оштрафует компанию на сумму от 15 000 до 75 000 руб., а бухгалтера — от 10 000 до 20 000 руб. (ч. 2 ст. 13.11 КоАП РФ), если узнает, что

<p>компании, чтобы оценить выгоду от захвата и перейти к активным действиям. В открытых источниках этих данных нет, но налоговики их вправе проверить.</p>	<p>персональные данные попали в руки злоумышленникам по вине компании.</p> <p>3. <u>Вы не обязаны отвечать на устные запросы и информационные письма налоговиков</u>, согласно НК РФ. Оштрафовать за отказ Вас не вправе. Компания обязана представлять инспекторам документы, пояснения и сведения только на основании письменного требования (ст. 88, 93 и 93.1 НК РФ) и только то, что налоговики вправе запросить (ст. 23 НК РФ).</p> <p>4. Если решите представить информацию, сначала <u>убедитесь в том, что Вам действительно звонит сотрудник инспекции</u>. Есть 2 варианта убедиться, что это звонил инспектор:</p> <ul style="list-style-type: none"> ○ <u>Первый</u> — сразу уточните ФИО, должность и отдел, в котором работает налоговый. <ul style="list-style-type: none"> - Если ответ устраивает, выслушайте, запишите все вопросы, но не спешите на них отвечать. - Возьмите тайм-аут для подготовки ответа и договоритесь, что перезвоните сами. - Уточните номер, по которому можете связаться с инспектором, пробейте его на сайте nalog.ru в разделе «Контакты и обращения». - Если все верно, свяжитесь с инспекцией по номеру телефона на сайте, попросите соединить со звонившим налоговиком и направить Вам официальный запрос. - Чтобы исключить повторные запросы и разночтения, отвечать на обращения безопаснее письменно. ○ <u>Второй вариант</u> — сразу задайте звонящему вопросы, ответы на которые может знать только настоящий инспектор («Напомните, какого числа началась „камералка“? Три месяца еще не прошло?», или «Как удобнее проехать в инспекцию, чтобы лично привезти документы?»). Мошенник вряд ли ответит на них, и Вы сможете спокойно закончить разговор. <ul style="list-style-type: none"> - Не задавайте вопросов, ответы на которые можно найти в открытом доступе (об ИНН или адресе компании) мошенник может заранее подготовить их, чтобы вызвать у Вас чувство ложного спокойствия.
<p>5 <u>Благотворительные акции и помощь инспекции.</u></p> <p>Мошенники от имени руководителя налоговой инспекции предлагают участвовать в благотворительной акции. Они часто хорошо осведомлены о делах компании, (называют сотрудников по фамилиям, знают нюансы Вашей деятельности).</p> <p>Иногда мошенники просят оказать спонсорскую помощь самой инспекции (оплатить административные расходы, положив деньги на мобильные номера; организовать встречу руководства в ресторане; приобрести бытовую технику и пр.)</p> <p>Иногда просят перечислить предоплату по налогам на специальный счет.</p>	<p>Налоговики могут обращаться к руководству компании только по вопросам, которые связаны с соблюдением налогового законодательства и уплатой налогов и взносов.</p> <p>1. <u>Сообщайте при получении подобных предложений в полицию и по телефону доверия ФНС.</u></p> <p>2. <u>Не перечисляйте предоплату на предоставленный мошенниками специальный счет.</u> Если Вы добровольно переведете средства, их будет проблематично вернуть и учесть в расходах. Когда перевод оформлен на счет физлица, инспекторы также могут начислить НДСЛ и взносы.</p> <p>3. <u>Не поддавайтесь на провокации!</u> Инспекторы не собирают пожертвования.</p>