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	***Переадресация на платный номер*** – 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. Не перезванивайте по предложенным номерам, если Вам позвонил неизвестный абонент, тем более из другого региона. 2. Проверьте данные о расчетах и долгах в личном кабинете налогоплательщика и обратитесь за разъяснениями в инспекцию по месту своего учета. 3. Сообщайте инспекторам о фактах звонков с информацией о задолженностях по автоответчику - такие номера будут блокировать, чтобы мошенники не смогли обмануть Ваших коллег. 4. Когда видите пропущенный звонок с незнакомого номера, пробейте его в любом поисковике. Там увидите отзывы обманутых пользователей. Если в поисковике номера нет, проверьте контакты на сайте ФНС ***nalog.ru*** в разделе «Контакты и обращения».
2	***Требования с вложенными файлами и ссылками*** - 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. ***ФНС России советует, как самостоятельно отличить***

	отправителя похож на налоговый, а содержание напоминает письма из инспекции. 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. 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. Еще один вариант — вирус шифрует все данные на компьютере, в том числе базу бухгалтерской программы. За расшифровку мошенники требуют деньги.	***настоящий запрос инспекции от подделки:*** 1. Обращайте внимание на техническую часть письма. 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. Заранее уточните у представителей почтового сервиса, который используете в работе, поддерживают ли они эти механизмы защиты. 3. Своевременно обновляйте антивирусные базы, операционную систему и другие программы (почтовый клиент, браузер). 4. Не открывайте подозрительные письма, приложенные к письму файлы, и не переходите по ссылкам. Пока файл не скачали и не запустили, опасности нет. Опасны файлы с расширением.exe или.bat. Это исполняемые файлы, то есть программы. 5. Перепрaвьте пришедшее письмо сисадмину или производителю Вашего антивируса для проверки. 6. Обращайте внимание на стиль письма (в нем могут сообщать о задолженности по НДС, когда компания на упрощенке). 7. Смотрите, как автор обращается к Вам. На поддельное письмо указывает отсутствие данных о Вас или Вашей компании.
3	***Платежки с липовыми реквизитами*** – 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. Мошенники рассчитывают на то, что бухгалтер не заметит подмены и перечислит деньги.	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. ***Пресс-служба ФНС России разъясняет, какие рассылки безопасны:*** 1. Официальная рассылка ФНС России направляется только тем, кто указал и подтвердил адрес своей электронной почты в сервисе «Личный кабинет налогоплательщика». 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. Новостную рассылку сайта **nalog.ru** направляют пользователям сайта, которые оформили подписку, и дублируют на главной странице сайта. 3. Проходите перед отчетной кампанией сверки с налоговиками. Так мошенникам будет сложнее ввести Вас в заблуждение насчет долгов. 4. Всегда сверяйте реквизиты платежек, которые отправляете в банк.
4	***Расспросы о компании и сотрудниках.*** 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	Практические правила безопасной работы с электронными запросами: 1. Набирайте ссылки вручную, т.к. опасно кликать по ссылкам в письмах или копировать их в строку браузера. Вид ссылки и реальный адрес, на который она указывает, могут различаться. 2. Не предоставляйте данные о физлицах кому попало – 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

	компании, чтобы оценить выгоду от захвата и перейти к активным действиям. В открытых источниках этих данных нет, но налоговики их вправе проверить.	персональные данные попали в руки злоумышленникам по вине компании. 3. Вы не обязаны отвечать на устные запросы и информационные письма налоговиков, 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*). 4. Если решите представить информацию, сначала убедитесь в том, что Вам действительно звонит сотрудник инспекции. Есть 2 варианта убедиться, что это звонил инспектор: ○ *Первый* — сразу уточните ФИО, должность и отдел, в котором работает налоговик. - 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. ○ *Второй вариант* — 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. - 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.
5	***Благотворительные акции и помощь инспекции.*** 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*). 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*.) Иногда просят перечислить предоплату по налогам на специальный счет.	Налоговики могут обращаться к руководству компании только по вопросам, которые связаны с соблюдением налогового законодательства и уплатой налогов и взносов. 1. Сообщайте при получении подобных предложений в полицию и по телефону доверия ФНС. 2. Не перечисляйте предоплату на предоставленный мошенниками специальный счет. Если Вы добровольно переведете средства, их будет проблематично вернуть и учесть в расходах. Когда перевод оформлен на счет физлица, инспекторы также могут начислить НДФЛ и взносы. 3. Не поддавайтесь на провокации! Инспекторы не собирают пожертвования.