Мошенничество и малый бизнес:

руководство для бизнеса

Russian

Когда мошенники охотятся за вашим бизнесом или некоммерческой организацией, это может повредить вашей репутации и итоговым показателям. Как лучше всего защититься? Узнайте о признаках мошенничества, направленного против предприятий. Затем расскажите своим сотрудникам и коллегам, на что следует обратить внимание, чтобы они могли избежать мошенничества.

- **Тактики мошенников**
- **Защитите свой бизнес**
- **Распространенные виды мошенничества, направленные на малый бизнес**
- **Другие сомнительные методы**

► Тактики мошенников

- **Мошенники выдают себя за человека, которому вы доверяете.** Они выдают себя за известную вам компанию или государственное учреждение, чтобы заставить вас заплатить. Но это обман.
- **Мошенники создают ощущение срочности, запугивания и страха.** Они хотят, чтобы вы действовали до того, как у вас появится шанс проверить их утверждения. Не позволяйте никому заставлять вас платить или сообщать конфиденциальную деловую информацию.
- **Мошенники просят заплатить им определенным образом.** Они часто требуют оплаты через банковские переводы, криптовалюту или подарочные карты. Не платите никому, кто требует оплаты таким образом. Это мошенничество.

► Защитите свой бизнес

Обучите своих сотрудников

- Ваша лучшая защита — это информированный персонал. Научите сотрудников не отправлять пароли или конфиденциальную информацию по электронной почте, даже если кажется, что письмо пришло от руководителя. Объясните сотрудникам, как происходят мошенничества, и посоветуйте им поговорить со своими коллегами, если они подозревают, что происходит нечто подобное. Закажите бесплатные экземпляры этой брошюры на сайте **ftc.gov/bulkorder** и передайте их своим сотрудникам.

Проверяйте счета-фактуры и платежи

- Убедитесь, что процедуры утверждения закупок и счетов-фактур четко прописаны, и попросите

сотрудников тщательно проверять все счета-фактуры. Обращайте внимание на то, как вас просят заплатить, и попросите своих сотрудников делать то же самое. Если кто-то требует, чтобы вы заплатили банковским переводом, криптовалютой или подарочными картами, не платите. Это мошенничество.

Отслеживайте мошенничество, связанное с техникой

- Поскольку мошенники часто подделывают телефонные номера, не доверяйте определителю номера. Если вы получили неожиданное текстовое сообщение или электронное письмо, не переходите по ссылкам, не открывайте вложения и не скачивайте файлы. Так мошенники загружают вредоносное ПО в вашу сеть или пытаются убедить вас отправить деньги или поделиться конфиденциальной информацией. Мошенники иногда даже взламывают аккаунты знакомых вам людей в социальных сетях, отправляя сообщения, которые кажутся реальными, но таковыми не являются. Узнайте больше о защите вашего малого бизнеса или некоммерческой организации от кибермошенников и хакеров: посмотрите раздел **«Кибербезопасность для малого бизнеса»** на сайте **ftc.gov/cybersecurity**.

Знайте, с кем вы имеете дело

- Прежде чем вести дела с новой компанией, поищите ее название в Интернете по словам «мошенничество» или «жалоба». Прочитайте, что другие говорят об этой компании. Попросите рекомендации у людей, которым вы доверяете. Вы также можете получить бесплатные советы и консультации по развитию бизнеса через такие программы, как **SCORE.org**.

► Распространенные виды мошенничества, направленные на малый бизнес

Поддельные счета-фактуры и незаказанные товары

Мошенники создают фальшивые счета-фактуры, которые выглядят так, будто вы заказали товары или услуги для своего бизнеса. Они надеются, что человек, оплачивающий счета, решит, что счета настоящие, и произведет оплату. Но это подделка. Или мошенник может позвонить, утверждая, что хочет «подтвердить» существующий заказ, «проверить» адрес или предложить «бесплатный» каталог или образец. Если вы ответите «да» на любой из этих вопросов, к вашему порогу прибудет незаказанный товар, за которым последует требование оплатить его под сильным давлением. Не платите. И помните, если вы получите товар, который вы не заказывали, у вас есть законное право оставить его себе и пользоваться им бесплатно.

Мошенничество при размещении объявлений и рекламы в Интернете

Мошенники пытаются обмануть вас, заставляя платить за несуществующую рекламу или объявление в фальшивом бизнес-каталоге. Они могут попросить вас сообщить свои контактные данные для получения «бесплатного» объявления или сказать, что звонят просто для «подтверждения» вашей информации. Позже вы получите крупный счет, и мошенник может использовать детали — или даже запись — предыдущего звонка, чтобы заставить вас заплатить.

Мошенничество с выдачей себя за представителей бизнеса и правительства

Мошенники выдают себя за человека, которого вы знаете или которому доверяете, и пытаются напугать или поторопить вас, чтобы вы заплатили или предоставили им информацию. Например:

- Мошенники говорят, что звонят из коммунальной компании и что услуги по газо-, электро- или водоснабжению вот-вот будут отключены из-за (фальшивого) просроченного счета.
- Мошенники говорят, что они правительственные агенты, и угрожают приостановить действие лицензии на ведение бизнеса, оштрафовать вас или даже подать на вас в суд. Они могут сказать, что это связано с задолженностью по налогам или необходимостью продлить лицензию или регистрацию.
- Некоторые мошенники убеждают вас купить плакаты о соблюдении трудового законодательства, которые вы можете бесплатно получить в Министерстве труда США.
- Некоторые мошенники обманом заставляют вас заплатить за подачу заявки на так называемые бизнес-гранты от государственных программ, которые оказываются поддельными.
- Мошенники выдают себя за сотрудников Бюро патентов и торговых марок США и угрожают, что вы потеряете свой товарный знак, если немедленно не заплатите пошлину. В других случаях они лгут и говорят, что вы должны деньги за дополнительные услуги по регистрации.
- Некоторые мошенники говорят, что звонят из технической компании, и угрожают, что ваш бизнес потеряет URL-адрес сайта, если вы немедленно не заплатите.

Мошенничество с технической поддержкой

Мошенничество с технической поддержкой начинается со звонка или тревожного всплывающего сообщения на вашем экране. Мошенники выдают себя за представителей известной технической компании и сообщают, что в системе безопасности вашего компьютера возникли проблемы. Их цель — получить ваши деньги, доступ к вашему компьютеру или и то, и другое. Они могут попросить вас заплатить за устранение проблемы, которой на самом деле нет, записать ваш бизнес на несуществующую или бесполезную программу обслуживания компьютера или проникнуть в вашу компьютерную сеть, чтобы получить конфиденциальные данные, которые они могут использовать для совершения кражи личных данных.

Социальная инженерия, фишинг и вымогательство

Кибермошенники могут обманом заставить сотрудников отправить им деньги или передать конфиденциальную или секретную информацию, например, пароли или банковские данные. Часто это начинается с фишингового электронного письма, контакта в социальных сетях или звонка, который, как кажется, исходит из надежного источника — например, от начальника или другого высокопоставленного сотрудника, — что создает срочность или страх. Другие письма могут выглядеть как обычные запросы на обновление пароля или другие автоматические сообщения, но на самом деле это попытки украсть вашу информацию. Мошенники также могут использовать вредоносное ПО для блокировки файлов организаций и получения за них выкупа.

Мошенничество в сфере бизнес-коучинга

Некоторые мошенники продают фиктивные программы бизнес-коучинга, часто используя поддельные отзывы, видео, презентации семинаров и телемаркетинговые звонки. Они лживо обещают потрясающие результаты, если вы заплатите за их эксклюзивную «проверенную» систему достижения успеха в бизнесе. Они также могут заманить вас низкими первоначальными затратами, а потом потребовать тысячи долларов. В действительности, мошенники оставляют начинающих предпринимателей без помощи, к которой они стремились, и с долгами в тысячи долларов.

Изменение отзывов в Интернете

Некоторые мошенники утверждают, что они могут заменить негативные отзывы о вашем товаре или услуге, добавить положительные отзывы или повысить ваши оценки на рейтинговых сайтах. Однако размещение фальшивых отзывов является незаконным. Согласно руководству FTC, одобрительные отзывы, включая обзоры, должны отражать честное мнение и опыт пользователя.

Мошенничество при обработке кредитных карт и лизинге оборудования

Некоторые мошенники обещают более низкие тарифы на обработку операций по кредитным картам или лучшие предложения по лизингу оборудования. Эти мошенники прибегают к мелкому шрифту, полуправде и откровенной лжи, чтобы получить подпись владельца бизнеса на контракте. Некоторые недобросовестные торговые агенты просят владельцев бизнеса подписать пустые документы. (Не делайте этого!) Известно, что некоторые меняют условия уже после подписания. Попросите продавца

выдать вам копии всех документов прямо здесь и сейчас. Если они отказываются или отговаривают вас обещанием прислать их позже, это может быть признаком того, что вы имеете дело с мошенниками.

Мошенничество с поддельными чеками

Некоторые мошенники дают вам, казалось бы, правдоподобную причину, чтобы переплатить вам по чеку. Затем они попросят вас отправить лишние деньги обратно им или кому-то другому. Но чек окажется фальшивым, хотя на вашем счету он может даже отображаться как «оплаченный». К тому времени, когда банк обнаружит, что чек был недействительным, мошенник уже получит деньги, которые вы ему отправили. Вы будете вынуждены выплачивать долг банку.

▶ Другие сомнительные методы

Иногда мошенники прикрываются другими сомнительными методами — например, заявляют, что предлагают работу в гиг-экономике с большими деньгами, но потом не выполняют своих обещаний. Или они могут попытаться продать вам ненужные услуги с ложным утверждением, что вам нужно заплатить, чтобы улучшить кредитный отчет вашего бизнеса. А после стихийных бедствий могут появиться нелицензированные подрядчики и мошенники с ложными обещаниями, что они быстро вернут ваш бизнес к работе с помощью ремонта, очистки или уборки завалов, которые так и не будут выполнены.

▶ Подробнее

- Дополнительные советы по защите вашей организации от мошенничества можно найти на сайте **ftc.gov/SmallBusiness**.
- Оставайтесь на связи с FTC, подписавшись на блог FTC о бизнесе на сайте **ftc.gov/subscribe**.

▶ Сообщите

- Если вы обнаружили факт мошенничества, позвоните по телефону 877-382-4357, нажмите 3 для выбора другого языка, а затем 7 для русского, или зайдите на сайт **ReportFraud.ftc.gov.**
- Предупредите генерального прокурора вашего штата. Контактную информацию можно найти на сайте **NAAG.org.**

▶ Задействуйте

- Помните: ваша лучшая защита — это информированные сотрудники. Поговорите со своими сотрудниками о том, как происходят мошенничества.
- Поделитесь этой брошюрой со своими сотрудниками.
- Скачать бесплатные копии этой брошюры можно на сайте **ftc.gov/languages**.

О FTC

FTC работает над оказанием помощи владельцам малых предприятий в предотвращении мошенничества, защите их компьютеров и сетей, а также сохранении данных их клиентов. С информацией для малого бизнеса можно ознакомиться на сайте **ftc.gov/SmallBusiness.** Там вы найдете информацию о мошенничествах, направленных на малый бизнес, и о том, как их избежать, а также сведения по кибербезопасности для малого бизнеса, которые помогут владельцам обеспечить безопасность своих сетей.

Для получения самой свежей информации для малого бизнеса подпишитесь на бизнес-блог FTC на сайте **ftc.gov/subscribe.**

This brochure is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **ftc.gov/bulkorder**.

FEDERAL TRADE COMMISSION

business.ftc.gov

Июль 2023 г.