Шахрайство і малий бізнес:

посібник для бізнесу

Ukranian

Коли шахраї переслідують ваш бізнес або неприбуткову організацію, це може зашкодити вашій репутації та фінансовим результатам. Як найкраще захиститися від цього? Дізнайтеся про ознаки шахрайства, спрямованого на бізнес. Потім розкажіть своїм співробітникам і колегам, на що слід звертати увагу, щоб уникнути шахрайства.

- **Тактики шахраїв**
- **Захистіть свій бізнес**
- **Поширені шахрайства, спрямовані на малий бізнес**
- **Інші сумнівні практики**

► Тактики шахраїв

- **Шахраї прикидаються тими, кому ви довіряєте.** Вони видають себе за відому вам компанію або державну установу, щоб змусити заплатити їм. Але це брехня.
- **Шахраї створюють відчуття терміновості, залякування та страху.** Вони хочуть, щоб ви діяли до того, як у вас з'явиться можливість перевірити їхні твердження. Не дозволяйте нікому змушувати вас платити або надавати конфіденційну ділову інформацію.
- **Шахраї просять заплатити їм певними способами.** Вони часто вимагають оплату банківськими переказами, криптовалютою або подарунковими картками. Не платіть нікому, хто вимагає оплату таким чином. Це шахрайство.

► Захистіть свій бізнес

Навчіть своїх співробітників

- Ваш найкращий захист — це поінформовані працівники. Навчіть працівників не надсилати паролі та конфіденційну інформацію електронною поштою, навіть якщо здається, що лист надійшов від керівника. Поясніть їм, як відбуваються шахрайства, і заохочуйте їх говорити зі своїми колегами, якщо вони підозрюють, що відбувається щось підозріле. Замовте безкоштовні примірники цієї брошури на сайті **ftc.gov/bulkorder** та поділіться ними зі своїми співробітниками.

Перевіряйте рахунки та платежі

- Переконайтеся, що процедури затвердження закупівель та рахунків-фактур є чіткими, і попросіть своїх співробітників ретельно перевіряти всі рахунки-фактури. Звертайте увагу

на те, як хтось просить вас заплатити, і кажіть своїм співробітникам робити те ж саме. Якщо хтось вимагає, щоб ви заплатили банківським переказом, криптовалютою або подарунковими картками, не платіть. Це шахрайство.

Виявляйте шахрайство, пов'язане з технологіями

- Оскільки шахраї часто підробляють телефонні номери, не довіряйте ідентифікатору абонента. Якщо ви отримали несподіване текстове повідомлення або електронний лист, не переходьте за посиланнями, не відкривайте вкладення і не завантажуйте файли. Саме так шахраї завантажують шкідливе програмне забезпечення у вашу мережу або намагаються переконати вас відправити гроші чи поділитися конфіденційною інформацією. Шахраї іноді навіть зламують акаунти в соціальних мережах людей, яких ви знаєте, і надсилають повідомлення, які здаються реальними, але не є такими. Дізнайтеся більше про захист вашого малого бізнесу або неприбуткової організації від кібершахраїв та хакерів: перегляньте статтю **«Кібербезпека для малого бізнесу»** за посиланням **ftc.gov/cybersecurity**.

Знайте, з ким маєте справу

- Перед тим, як вести справи з новою компанією, пошукайте її назву в Інтернеті за словами «шахрайство» або «скарга». Почитайте, що інші говорять про цю компанію. Попросіть рекомендацій у людей, яким ви довіряєте. Ви також можете отримати безкоштовні поради та консультації з розвитку бізнесу через такі програми, як **SCORE.org**.

► Поширені шахрайства, спрямовані на малий бізнес

Фальшиві рахунки-фактури та незамовлені товари

Шахраї створюють фальшиві рахунки-фактури, які виглядають так, ніби ви замовили товари чи послуги для свого бізнесу. Вони сподіваються, що людина, яка оплачує ваші рахунки, вважатиме їх справжніми і здійснить платіж. Тільки вони несправжні. Або ж шахрай може зателефонувати і заявити, що хоче «підтвердити» існуюче замовлення, «перевірити» адресу або запропонувати «безкоштовний» каталог чи зразок. Якщо ви погодитеся на будь-яку з цих пропозицій, незамовлений товар з'явиться на вашому порозі, а за ним — вимога заплатити за нього під тиском. Не платіть. І пам'ятайте, якщо ви отримали товар, який не замовляли, ви маєте законне право залишити його собі і користуватися ним безкоштовно.

Шахрайство з оголошеннями та рекламою в Інтернеті

Шахраї намагаються обдурити вас і змусити заплатити за неіснуючу рекламу або за розміщення в фальшивому бізнес-довіднику. Вони можуть попросити вас надати контактну інформацію для «безкоштовного» розміщення оголошення або сказати, що телефонують лише для того, щоб «підтвердити» вашу інформацію. Пізніше ви отримаєте великий рахунок, і шахрай може використати деталі, або навіть запис попереднього дзвінка, щоб змусити вас заплатити.

Шахрайство з видаванням себе за представників бізнесу та уряду

Шахраї прикидаються кимось, кого ви знаєте або кому довіряєте, і намагаються залякати або змусити

вас заплатити або надати їм інформацію. Наприклад:

- Шахраї кажуть, що телефонують з комунальної компанії і що ваші послуги з газо-, електро- чи водопостачання будуть відключені через (фальшивий) рахунок з простроченою оплатою.
- Шахраї називають себе урядовими агентами і погрожують призупинити ліцензію на ведення бізнесу, оштрафувати або навіть подати на вас до суду. Вони можуть сказати, що ви заборгували податки або вам потрібно поновити ліцензію чи реєстрацію.
- Деякі шахраї переконують вас купити плакати про дотримання норм на робочому місці, які ви можете отримати безкоштовно від Департаменту праці США.
- Деякі шахраї обманом змушують вас заплатити за подання заявки на так звані бізнес-гранти від державних програм, які виявляються фальшивими.
- Шахраї видають себе за Бюро патентів і торговельних марок США і погрожують, що ви втратите свою торговельну марку, якщо негайно не сплатите збір. В інших випадках вони брешуть і кажуть, що ви винні гроші за додаткові послуги з реєстрації.
- Деякі шахраї кажуть, що телефонують від імені технологічної компанії, погрожуючи, що ваша компанія втратить URL-адресу вебсайту, якщо ви негайно не заплатите.

Шахрайство з технічною підтримкою

Шахрайство з технічною підтримкою починається з дзвінка або тривожного спливаючого повідомлення на екрані. Шахраї представляються представниками відомої технологічної компанії, повідомляючи вам про проблеми з безпекою вашого комп'ютера. Їх мета — отримати ваші гроші, доступ до вашого

комп'ютера або і те, і інше. Вони можуть попросити вас заплатити за усунення проблеми, якої насправді немає, зареєструвати вашу компанію в неіснуючій або беззмістовній програмі технічного обслуговування комп'ютерів або проникнути у вашу комп'ютерну мережу, щоб викрасти конфіденційні дані, які вони можуть використати для крадіжки особистих даних.

Соціальна інженерія, фішинг та програми-вимагачі

Кібершахраї можуть обманом змусити працівників надсилати їм гроші або надавати конфіденційну чи секретну інформацію, наприклад, паролі чи банківські реквізити. Часто це починається з фішингового електронного листа, контакту в соціальних мережах або дзвінка, який здається надійним джерелом — наприклад, від керівника або іншого старшого співробітника, — що викликає нагальну потребу або страх. Інші електронні листи можуть виглядати як звичайні запити на оновлення паролю або інші автоматичні повідомлення, але насправді є спробами викрасти вашу інформацію. Шахраї також можуть використовувати шкідливе програмне забезпечення для блокування файлів організацій та утримання їх з метою отримання викупу.

Шахрайство з бізнес-коучингом

Деякі шахраї продають фальшиві програми бізнес-тренінгів, часто використовуючи фальшиві відгуки, відео, презентації семінарів та телемаркетингові дзвінки. Вони брехливо обіцяють приголомшливі результати, якщо ви заплатите за їхню ексклюзивну «перевірену» систему досягнення успіху в бізнесі. Вони також можуть заманити вас низькими початковими витратами, щоб потім вимагати тисячі доларів. Насправді ж шахраї залишають підприємців-

початківців без допомоги, яку вони шукали, і з тисячами доларів боргу.

Зміна відгуків в Інтернеті

Деякі шахраї стверджують, що можуть замінити негативні відгуки про ваш товар або послугу, додати позитивні відгуки або підвищити ваші бали на рейтингових сайтах. Однак розміщення фейкових відгуків є незаконним. У рекомендаціях FTC сказано, що відгуки, в тому числі огляди, повинні відображати чесні думки та досвід особи, яка їх опублікувала.

Шахрайство з кредитними картками та лізингом обладнання

Деякі шахраї обіцяють нижчі тарифи на обробку транзакцій за кредитними картками або кращі умови лізингу обладнання. Ці шахраї вдаються до дрібного шрифту, напівправди та відвертої брехні, щоб отримати підпис власника бізнесу на контракті. Деякі недобросовісні торгові агенти просять власників бізнесу підписати порожні документи. (Не робіть цього!) Відомо, що деякі з них змінювали умови постфактум. Попросіть продавця видати вам копії всіх документів прямо на місці. Якщо він відмовляється або відтягує час, обіцяючи надіслати їх пізніше, це може бути ознакою того, що ви маєте справу з шахраєм.

Шахрайство з підробленими чеками

Деякі шахраї дають вам правдоподібну причину переплати за чеком. Потім вони попросять вас надіслати зайві гроші назад їм або комусь іншому. Але чек буде фальшивим, хоча він може навіть відображатися як «сплачений» у вашому обліковому записі. До того часу, як банк виявить, що чек фальшивий, шахрай вже отримає гроші, які ви йому відправили. Ви застрягнете у боргах перед банком.

► Інші сумнівні практики

Іноді шахраї ховаються за іншими сумнівними методами — наприклад, стверджуючи, що пропонують високооплачувану роботу за кордоном, але потім не виконують своїх обіцянок щодо заробітку. Або ж вони можуть спробувати продати вам непотрібні послуги з неправдивим твердженням, що вам потрібно заплатити, щоб покращити кредитний звіт вашого бізнесу. А після стихійних лих можуть з'явитися неліцензовані підрядники та шахраї з неправдивими обіцянками відновити роботу вашого бізнесу за допомогою швидкого ремонту, прибирання чи розбору завалів, які ніколи не відбудуться.

► Дізнайтеся більше

- Щоб отримати більше порад щодо захисту вашої організації від шахрайства, перейдіть за посиланням **ftc.gov/SmallBusiness**.
- Залишайтеся на зв'язку з FTC, підписавшись на бізнес-блог FTC на сайті **ftc.gov/subscribe**.

► Повідомляйте

- Якщо ви стали свідком шахрайства, зателефонуйте за номером 877-382-4357 і натисніть 3 для вибору іншої мови, а потім 0, щоб вибрати потрібну мову з додаткового переліку, або перейдіть на сайт **ReportFraud.ftc.gov.**
- Попередьте генерального прокурора вашого штату. Ви можете знайти контактну інформацію за посиланням **NAAG.org**.

► Задіюйте

- Пам'ятайте: найкращий захист — це поінформовані працівники. Поговоріть зі своїми співробітниками про те, як відбуваються шахрайства.
- Поділіться цією брошурою зі своїми співробітниками.
- Безкоштовно завантажити цю брошуру можна на сайті **ftc.gov/languages**.

Про FTC

FTC прагне допомогти власникам малого бізнесу уникнути шахрайства, захистити свої комп'ютери та мережі, а також зберегти дані своїх клієнтів. Для отримання інформації для малого бізнесу перейдіть на сторінку **ftc.gov/SmallBusiness.** Там ви знайдете інформацію про шахрайство, спрямоване на малий бізнес, і про те, як його уникнути, а також інформацію про кібербезпеку для малого бізнесу, яка допоможе власникам захистити свої мережі.

Для отримання найсвіжішої інформації для малого бізнесу підпишіться на бізнес-блог FTC за адресою **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

Липень 2023 р.