



Информационный буклет

Корпоративное мошенничество



do your thing

О чем этот информационный буклет?

В данном буклете описаны наиболее распространённые случаи мошенничества, с которыми каждый может столкнуться в повседневной жизни и при ведении бизнеса.

Следует помнить, что мошенники умны, их действия хорошо спланированы, а случаи мошенничества - не редкость: они происходят в мире каждый день. Чтобы не стать жертвой мошенничества, необходимо следовать приведенным далее рекомендациям.

Компрометация деловой электронной почты

Компрометация деловой электронной почты (Business email compromise - BEC) является одним из распространенных финансовых интернет-преступлений. Оно использует тот факт, что многие из нас полагаются на электронную почту для деловой переписки.

Что происходит?

Мошенник может:

- Подделать учетную запись электронной почты или веб-сайт, используя незначительные вариации адресов компаний, заставляя жертву думать, что поддельные аккаунты являются подлинными, например: john.kelly@examplecompany.com и john.kelly@exemplecompany.com;
- Получить неправомерный доступ к корпоративной учетной записи электронной почты другого лица путем:
- ✓ Использования вредоносного программного обеспечения, которое проникает в сети компании и получает незамеченный доступ к данным жертвы, включая пароли, информацию о счетах, сообщения электронной почты о выставленных счетах. Эта информация может быть использована, чтобы усыпить бдительность бухгалтеров и финансовых работников или обойти контрольные процедуры;
- ✓ Рассылки электронных фишинговых писем – сообщений похожих на письма от надежного отправителя или методов социальной инженерии, заставляя жертву раскрыть конфиденциальную информацию. Эта информация позволяет преступникам получить доступ к счетам, календарям, электронной переписке и данным компании для осуществления схем BEC.

Компрометация деловой электронной почты: виды

При афере ВЕС преступники отправляют по электронной почте сообщение, которое кажется исходящим от известного контрагента с уместным запросом, как в этих примерах:

- Поставщик, с которым компания регулярно работает, присылает счет с обновленными реквизитами.
- Генеральный директор компании просит помощника приобрести несколько десятков подарочных карт для поощрения сотрудников и срочно сообщить их серийные номера, чтобы сразу же отправить им по электронной почте.
- Покупатель жилья получает сообщение от компании застройщика с инструкциями о том, как перевести первый взнос.

Такие сценарии произошли с реальными жертвами. Все сообщения были поддельными. И в каждом случае старания преступников щедро окупались.

Компрометация деловой электронной почты: Какие меры защиты можно применить?

- Будьте осторожны с информацией, которой Вы делитесь в Интернете или в социальных сетях. Открыто сообщая такие вещи, как клички домашних животных, школы, в которых Вы учились, имена членов семьи и их дни рождения, Вы можете дать мошенникам всю необходимую информацию, чтобы угадать Ваш пароль или ответить на вопросы безопасности.
- Не переходите по ссылкам в подозрительных электронных письмах или текстовых сообщениях, в которых Вас просят обновить или проверить информацию о счете. Найдите номер телефона компании самостоятельно (не используйте тот, который дает потенциальный мошенник) и позвоните в компанию, чтобы проверить подлинность запроса.
- Обращайте внимание на адреса электронной почты, URL. Мошенники используют незначительные различия, чтобы обмануть Вас и завоевать доверие.
- Будьте внимательны к тому, что Вы скачиваете. Никогда не открывайте вложения электронной почты от незнакомых людей, с опаской относитесь к пересылаемым Вам вложениям.
- Установите двухфакторную (или многофакторную) аутентификацию на любой учетной записи, которая позволяет это сделать, и никогда не отключайте ее.
- По возможности проверяйте запросы на оплату и покупку лично или позвонив человеку, чтобы убедиться в их подлинности. Любые изменения в номере счета или процедуре оплаты следует осуществлять в соответствии с установленными в компании контрольными процедурами.
- Будьте особенно осторожны, если сообщение требует от Вас срочных, безотлагательных действий.

Социальная инженерия и мошенничество от имени должностного лица

Социальная инженерия - это метод получения доступа к информации или системам хранения информации без использования технических средств с целью ее дальнейшего несанкционированного использования. **Объектом** атаки, как правило, выступает **сотрудник компании**, от которого злоумышленник пытается получить закрытую/ конфиденциальную информацию, манипулируя его сознанием.

Социальная инженерия: что происходит?

1. Мошенники связываются с сотрудником компании (по электронной почте, по телефону и пр.), представляясь каким-либо уполномоченным лицом, например, аудитором, сотрудником государственных органов и т.п. Таким образом, они стараются собрать как можно больше информации о сотрудниках, их полномочиях и внутренних процедурах компании.
2. Далее они связываются с нужным сотрудником, представляются должностным лицом, например, генеральным или финансовым директором, часто зная, что он/она находится в отъезде в данный момент, ссылаются на сделку и необходимость перевода на крупную сумму денег. Сценариев много, но, как правило, все они побуждают к тому, что транзакция должна быть исполнена как можно скорее и без огласки.
3. Для большей убедительности мошенники могут связаться с сотрудником компании и представиться третьим лицом (участником сделки, подтверждающим транзакцию), чьи данные они также получили незаконным путем, и подтвердить транзакцию, а также напомнить о конфиденциальности и срочности платежа. Если все же сотрудник будет сомневаться, мошенник может воспользоваться такими техниками, как ссылка на высокопоставленное имя, лесть или даже запугивание.

Социальная инженерия: Какие меры защиты можно применить?

- Необходимо **настороженно относиться** к поступающим нестандартным запросам, особенно если просят провести срочный и/или секретный платеж.
- В случае получения подобного запроса необходимо **перезвонить человеку**, инициировавшему запрос, по известному номеру телефона из имеющегося списка контактов.
- Назначьте **ответственное контактное лицо** (не генерального и не финансового директора), с которым необходимо будет связаться для подтверждения платежей на крупные суммы, включая конфиденциальные платежи. Ответственное лицо должно будет связаться с генеральным директором компании для подтверждения запроса. Внимание: о данной процедуре не должно быть известно посторонним лицам.

Электронное мошенничество (Интернет-мошенничество)

К электронному мошенничеству относят **фишинг** и **заражение вредоносным программным кодом**. С этими видами мошенничества можно столкнуться как на работе, так и в повседневной жизни.

О каком бы виде данного мошенничества мы не говорили, кибермошенники пытаются украсть деньги **посредством незаконного получения данных** (логинов, паролей или электронных подписей), используя подложные сайты или присылая вложения, содержащие вредоносный код. Получив информацию, они переводят деньги на свои счета, опустошая Ваши.

Электронное мошенничество: что происходит?

По электронной почте Вы получаете **письма, похожие на официальные запросы/обращения** с обратными адресами, ссылками и торговыми марками, которые выглядят так, словно получены от настоящих банков, государственных органов, розничных фирм и т.д. Такие электронные **письма часто содержат ссылку на поддельный веб-сайт** и просят владельцев денежных счетов ввести имя и прочую конфиденциальную информацию под предлогом того, что Ваш личный кабинет был взломан и для восстановления необходимо сообщить данные о логинах, паролях, кодовых словах или другую конфиденциальную информацию. На подложной странице Вы вводите свои данные, которые впоследствии используются мошенниками на настоящих страницах для снятия денег с Ваших счетов.

Электронное мошенничество: Какие меры защиты можно применить?

- Пароли должны храниться в защищенном месте, не доступном третьим лицам.
- Относитесь с осторожностью к электронным письмам, призывающим предоставить Вашу конфиденциальную информацию.
- Никогда и никому не давайте свои коды доступа (логины и пароли) к компьютеру, приложениям и личным кабинетам.
- Пользуйтесь программным обеспечением от известных поставщиков, которым Вы доверяете.
- Регулярно обновляйте свой компьютер путем установки последних версий программного обеспечения и обновлений безопасности (патчей).
- Установите и регулярно обновляйте антивирус, чтобы защитить свой компьютер от вирусов, задача которых, как правило, получить доступ к Вашей информации или вовсе получить управление над Вашим компьютером.
- Используйте фильтр спама.
- Никогда не отвечайте на спам, поскольку Ваш адрес электронной почты будет отмечен в качестве действующего, и объем спама может вырасти.
- Если Вы все таки получили сообщение и распознали в нем спам, пометьте его соответствующим знаком СПАМ, чтобы помочь Вашему фильтру в дальнейшем блокировать сообщения от этого отправителя.

Мошенничество со счетами (“фальшивые счета”)

Во всех случаях мошенники изменяют платежные реквизиты компании, которая выпустила счет, на свои, в результате получают деньги, оплаченные по счету.

Что происходит?

- Мошенники перехватывают счет на интервале с момента его выпуска до момента его получения.
- Мошенники производят подмену реквизитов в счете. Есть несколько способов это сделать: выпустить новый счет с новыми платежными реквизитами или приложить письмо с изменением банковских реквизитов. Затем мошенники направляют счет получателю.
- Счет получен и оплачен по новым платежным реквизитам. То же самое может происходить и с последующими счетами, пока поставщик не свяжется с получателем по вопросу неполучения оплаты за предоставленные услуги.

Мошенничество со счетами: виды

Существуют разные вариации данного вида мошенничества. Например, компания, которая должна оплатить счет, получает электронное сообщение от поставщика с информацией о смене его банковских реквизитов. Данное письмо оформлено на бланке компании и кажется вполне реальным. Все ранее полученные, но еще неоплаченные и все новые счета должны оплачиваться по новым банковским реквизитам.

Каким бы ни был сценарий мошенника, его цель – изменить информацию поставщика (номер телефона, банковские реквизиты, электронный адрес и т.д.) с целью незаконного присвоения денег.

Мошенничество со счетами: Какие меры защиты можно применить?

Как обезопасить себя будучи компанией, выпускающей счет?

- Ограничьте риск перехвата Ваших счетов: избегайте их отправки в конвертах с логотипом Вашей компании, или другими признаками, указывающими на Вашу компанию.
- Рекомендуем направлять счета сразу по двум каналам передачи данных, например, по электронной почте и по обычной почте, так получатель счета будет знать, что должен оплатить полученный счет только в том случае, если он идентичен второму счету.
- Выделяйте Ваши платежные реквизиты на счете, тем самым привлекая внимание получателя, побуждая его проверить их перед оплатой.

Как обезопасить себя будучи компанией, получившей счет на оплату?

- Не оплачивайте счета, содержащие реквизиты, отличные от согласованных в договоре с контрагентом, предварительно не подтвердив их.
- Любое изменение контактов и реквизитов поставщика (номера телефона, банковских реквизитов, электронного адреса и т.д.) должно сопровождаться звонком по номеру телефона, который уже содержится в Ваших контактах, а не по номеру указанному в полученном счете или сообщении.

Ограничение ответственности

Настоящий буклет является документом справочного характера и не составляет какого-либо обязательства, обещания или совета с нашей стороны.

Настоящий буклет является кратким обзором определенных вопросов, и не должен рассматриваться в качестве консультации. ИНГ БАНК (ЕВРАЗИЯ) АО (далее – ИНГ Банк) настоятельно рекомендует привлечь для соответствующих консультаций независимых профессиональных консультантов (юридических, консультантов по безопасности и т.п.).

ИНГ Банк не ручается за полноту и достоверность изложенных в настоящем буклете сведений. Настоящий буклет не является заверением относительно каких-либо обстоятельств. Любая информация, содержащаяся в настоящем буклете, должна использоваться исключительно в справочных целях и рассматриваться как предположение, без ручательства за достижение конкретного результата.

ИНГ Банк не принимает на себя никакой ответственности за убытки, связанные с использованием содержащихся в настоящем буклете сведений.

ИНГ Банк сохраняет все интеллектуальные права относительно информации, содержащейся в настоящем буклете.