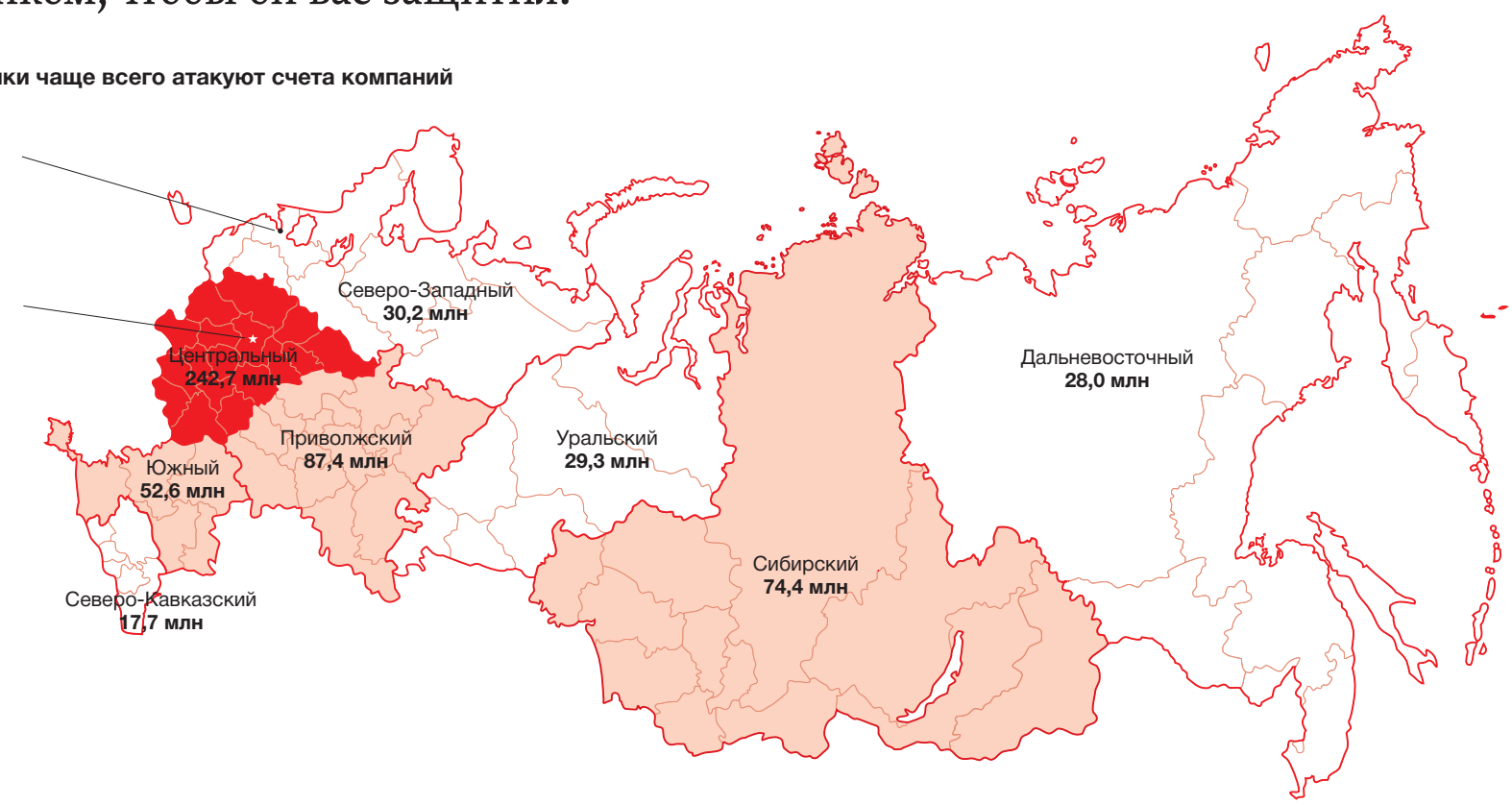
Мошенники крадут деньги компании через компьютер бухгалтера новыми способами

Суть: хакеры используют новые уловки, чтобы запустить на компьютер в бухгалтерии вирус, который украдет деньги со счета компании. Предупредите об опасности коллег и договоритесь с банком, чтобы он вас защитил.

В каких регионах России мошенники чаще всего атакуют счета компаний

66,1 млн
Пытались похитить со счетов компаний в Санкт-Петербурге

1,1 млрд
Пытались похитить со счетов компаний в Москве



Со счетов компаний пытались списать более 100 млн руб.
Со счетов компаний пытались списать от 50 до 100 млн руб.
Со счетов компаний пытались списать менее 50 млн руб.

Источник: данные ЦБ

Какие суммы списывают мошенники со счетов компаний, руб.

10 млн и больше	3%
От 1 до 10 млн	38,2%
От 100 тыс. до 1 млн	50,9%
От 10 до 100 тыс.	7,3%
Меньше 10 тыс.	0,6%

Источник: данные ЦБ

Офисные работники давно знают, что нельзя открывать письма с вложениями от неизвестных отправителей. Поэтому злоумышленники придумали новые способы, чтобы заставить бухгалтера поверить их письмам. Информацией с УНП поделились эксперты Group-IB и InfoWatch. Банкиры рассказали, чем они могут помочь компании.

Как уводят деньги

Стоит регулярно проверять по выписке банка, нет ли там платежей, которые компания не проводила. В 2017 году число попыток хищений со счетов увеличилось, но мошенники стараются уводить деньги некрупными суммами. Злоумышленники не обчищают счет компании, их самая частая добыча – суммы от 100 тыс. до 1 млн руб. Основная часть хищений происходит в Москве и Подмосковье.

По данным ЦБ, самым популярным способом для воровства денег со счетов в 2017 году стали вирусы. Они подменяют реквизиты платежек перед отправкой. Бухгалтер считает, что отправляет деньги контрагенту или в бюджет, а на самом деле они уходят на счет мошенников. Другие вирусы позволяют хакерам управлять клиент-банком.

Как рассказали эксперты по кибербезопасности, в последний год мошенники чаще всего внедряли вирус на компьютер главбуха через фишинговые сообщения в почту или соцсети. К письмам либо прикрепляют файл с вирусом, либо дают ссылку на зараженный сайт. Этот способ старый. Многие опасаются открывать ссылки и вложения. Поэтому мошенники идут на новые хитрости, чтобы заставить сотрудника занести на компьютер вирус.

Например, сотруднику приходит послание, что его письмо не доставлено. Сообщение хакеров похоже на автоматическую рассылку от почтового сервиса. Сотрудник знает, что ничего не отправлял. Он хочет выяснить, почему получил такое письмо, и переходит по ссылке. Так он скачивает вирус.

Еще один вид опасных писем – фальшивая переписка. В тексте письма мошенники имитируют историю сообщений, а в теме проставляют «RE…». Письмо также содержит вложение или ссылку.

Чтобы уговорить бухгалтера перейти по ссылке, хакеры могут на самом деле вступить в переписку. Например, приходит письмо такого содержания: «Добрый день, не могли бы вы отправить документы по этому счету…». Но никакого счета во вложении нет. Есть вероятность, что бухгалтер попросит дослать вложение. В ответ придет письмо с вложением и извинением: «Прошу прощения, не заметила, что не прикрепила файл». Поскольку переписка реальная, сотрудник может поверить отправителю и открыть письмо. В нем окажется вирус.

Зараженные письма могут приходить от имени руководства. Мошенники стараются выбрать высокопоставленных сотрудников, письма от которых подчиненные наверняка откроют. В таких сообщениях могут, например, предложить проголосовать за организацию в интернете или зарегистрироваться якобы на новом корпоративном портале.

Хакеры копируют типовую структуру письма, принятую в организации, в том числе форму подписи. Выяснить, как в организации оформляют электронные письма, несложно. Достаточно написать любому сотруднику письмо с каким-либо вопросом и дождаться ответа.

Есть и другие способы вызвать доверие к сообщению с вирусом.

Иногда злоумышленники ставят в копию письма с вирусом адресатов, которым потенциальная жертва доверяет. При этом тем, кто стоит в копии, может ничего не прийти. А доверие потенциальной жертвы к такому письму будет выше. Имеет значение также время отправки письма. Злоумышленники стараются рассылать спам в тот момент, когда сотрудники могут в спешке открыть опасное письмо. Это период с 11.00 до 13.00 – пик активности на работе, когда работники не очень внимательны к входящей почте. Также люди теряют бдительность после 18.00, когда стараются расправиться с делами и быстрее уйти с работы.

Мария Воронова, директор по консалтингу ГК InfoWatch

Киберпреступники уделяют все больше внимания созданию фишинговых писем, чтобы ввести получателя в заблуждение. Рассылка оформлена максимально похоже на письма реального отправителя, текст написан без ошибок. В мае 2018 года хакеры атаковали финансовые организации. Рассылка шла от имени известной антивирусной компании. Сотрудники получили жалобу на английском языке о том, что их компьютеры якобы нарушают закон. Пользователям предлагали ознакомиться с поясняющим документом и представить объяснения. Если ответ не поступит в течение 48 часов, «антивирусная компания» угрожала наложить санкции на web-ресурсы получателя.

Ярослав Каргалев, заместитель руководителя CERT Group-IB

Часто от опасных писем не защищает даже антивирус. Во-первых, постоянно появляются новые вирусы. Во-вторых, мошенники хитростями обходят защиту компаний.

Чтобы обойти антивирусы и защиту почты, злоумышленники используют многоходовые схемы. Например, некоторые средства защиты проверяют все входящие письма, в том числе и гиперссылки в них. Злоумышленники делают так, что ссылка на вирус становится активной лишь спустя некоторое время после того, как пришло письмо. Так, зная график работы потенциальной жертвы, злоумышленники могут отправить письмо заранее. До прихода этого сотрудника на работу вредоносная программа не будет доступна по ссылке в письме и антивирус не заблокирует ее в момент доставки.

Ярослав Каргалев, заместитель руководителя CERT Group-IB

Кроме зараженных писем есть другие способы внедриться в клиент-банк. Компания Group-IB выявила новую схему, которая направлена на бухгалтеров и финансовых директоров. Мошенники создали сайты, с которых можно было скачать образцы документов – типовые договоры, заявления, первичку и т. д. Например, в черный список попали сайты buh-docum[.]ru и buh-blanks[.]ru. Вместе с файлом с опасного сайта скачивался вирус, который пытался получить доступ к счетам организации.

Преступники могут обойтись и без вирусной программы. Они вводят в заблуждение сотрудника, чтобы тот сам перевел деньги на их счет. Для этого они вступают в переписку с работником под видом руководителя или важного поставщика.

Как уберечь деньги на счетах

Напомните сотрудникам, что нельзя ходить по ссылкам, открывать вложения в письмах, нужно все проверять антивирусом. Стоит запретить на рабочем компьютере личную почту и социальные сети. Игнорируйте сообщения с неизвестных адресов до тех пор, пока не пообщаетесь с отправителем лично или хотя бы по телефону. Кроме того, предупредите сотрудников, что любые платежи надо согласовывать с главбухом лично.

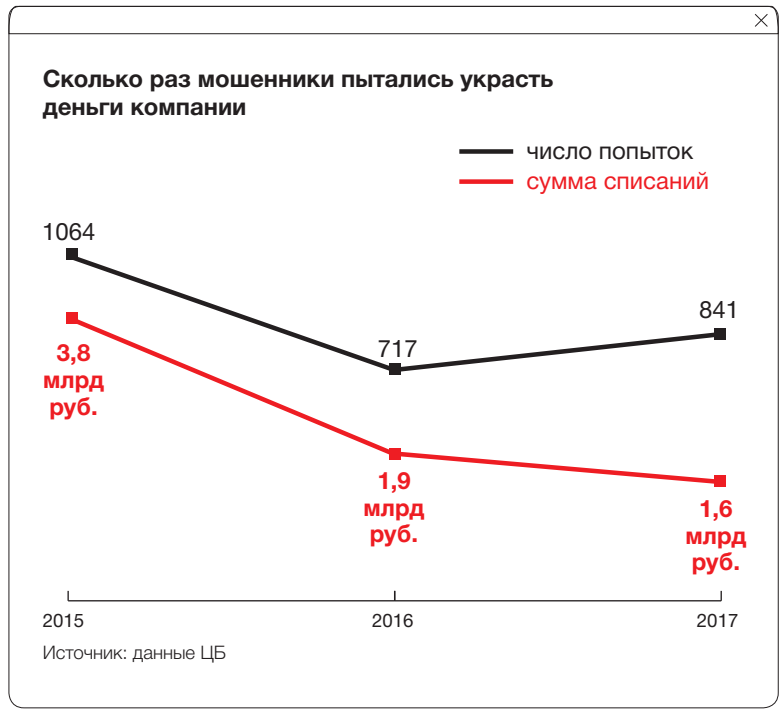
От мошенников поможет защититься банк. Можно договориться с ним, чтобы он дополнительно согласовывал списания на сумму больше оговоренной. Банк также может запрашивать подтверждения на все платежи в адрес новых контрагентов.

Кроме подтверждения платежей необходимо выполнить еще несколько действий, которые помогут защититься от мошенников. Например, на компьютере, который предназначен только для клиент-банка, заведите учетную запись пользователя. Важно, чтобы у этой учетной записи не было прав администратора. Используйте клиент-банк только с этого аккаунта. Логин и пароль для клиент-банка нельзя сохранять в системе. Самый безопасный способ – запомнить их.

Наталья Добренкова, адвокат адвокатского бюро «Правозащита»

Если видите, что со счета организации уже ушла сумма, которую вы не отправляли, в первую очередь свяжитесь с банком и постарайтесь заблокировать перевод. Далее извлеките флешку с электронным ключом и отключите от сети компьютер, на котором установлен клиент-банк. После сообщите об инциденте в службу безопасности и системному администратору компании.

Артур Сергеев
Корреспондент УНП



51,25

процента мошеннических операций компаниям удалось остановить в 2017 году, по данным ЦБ