СПЕЦТЕМА КИБЕРБЕЗОПАСНОСТЬ

Памятка для сотрудников, которая убережет деньги компании в банке

Суть: создайте памятку для работников, чтобы сохранить деньги компании. Число краж через клиент-банк за год выросло в семь раз. УНП с помощью экспертов по информационной безопасности разработала инструкцию, которую надо показать коллегам.

Проверьте, кому из сотрудников предоставляете доступ к клиент-банку и как защищаете систему. В прошлом году через клиент-банк хакеры пытались похитить деньги организаций в 7,3 раза чаще, чем годом ранее (данные ЦБ). Чаще всего мошенники обчищают компании в Санкт-Петербурге и Москве, а также в Уральском, Центральном и Приволжском округах (см. диаграмму).

По данным ЦБ, в 2018 году в 46 процентах краж со счетов компаний мошенники получали доступ к системе дистанционного банковского обслуживания с помощью вирусов. Хакеры взламывали программное обеспечение стационарных компьютеров, заходили в клиент-банк и переводили деньги организаций на посторонние счета. Сотрудники банков смогли пресечь только 63 процента таких операций, а 37 процентов переводов мошенники завершили. При этом компании обращались в полицию по каждой третьей несанкционированной операции.

Как рассказали эксперты по кибербезопасности, в последний год хакеры часто получают доступ к клиент-банкам компаний через поддельные бухгалтерские ресурсы. Например, мошенники «подсаживают» вирус на сайт, с которого главбухи скачивают шаблоны и образцы документов. Вместе с файлом сотрудник сохраняет на рабочем компьютере троян, который создали специально для взлома клиент-банков.

Где мошенники чаще всего воруют деньги компаний через клиент-банк
(количество операций, ед.)

Источник: данные ЦБ за 2018 год

> В июле прошлого года Центр круглосуточного реагирования на киберинциденты CERT Group-IB обнаружил сеть фальшивых бухгалтерских сайтов, заразивших около 200 тыс. пользователей. Жертвами атаки хакеров стали финансовые директора, юристы, бухгалтеры и другие специалисты, использующие в своей работе системы дистанционного банковского обслуживания, например клиент-банк. Новая преступная схема была раскрыта после того, как специалисты Group-IB зафиксировали попытку загрузки вредоносной программы в одном из российских банков. В ходе расследования мы обнаружили, что троян был “подсажен” с бухгалтерского ресурса с подборкой специализированных шаблонов: бланков, контрактов, счетов-фактур и документов налогового учета. При скачивании документов с сайта происходила загрузка, а затем и запуск троянской программы, нацеленной на кражу денег через клиент-банк.
>
> Павел Крылов, руководитель направления по развитию продуктов Secure Bank/Secure Portal Group-IB

Банкиры, которых мы опросили, рассказали, что не сразу переведут деньги со счета компании, если заподозрят, что клиент-банком организации завладели мошенники. Например, специалисты могут временно заморозить операцию, если компания переводит деньги контрагенту или «физику», с которыми раньше не сотрудничала.

Если банкиры заподозрят, что деньгами распоряжаются мошенники, специалисты вправе приостановить операцию, но максимум на два рабочих дня (п. 5.1 ст. 8 Федерального закона от 27.06.2011 № 161-ФЗ). За это время банк сообщит руководителю компании об операции и попросит ее подтвердить. Если директор сообщит, что знает о переводе, деньги сразу же поступят адресату. Но если за два дня специалисты не смогут связаться с директором, операцию разблокируют автоматически и деньги все равно уйдут. Поэтому компаниям безопаснее сообщать в свой банк, если директор или главбух меняют номер телефона.

Компании представляют в банк карточку с оттиском печати и образцами подписей сотрудников, которые вправе проводить операции с деньгами (гл. 7 Инструкции ЦБ от 30.05.2014 № 153-И). Банкиры рекомендуют регулярно проверять сведения в документе. Иначе есть риск, что экс-сотрудник может воспользоваться доступом к счету компании и украсть деньги. Банкиры рассказали, что если компания не исключила из карточки бывшего работника, то у специалистов нет повода отказать «физику» в доступе к счету. Поэтому сообщайте в банк об изменениях каждый раз, когда из компании уходит сотрудник, включенный в карточку.

Предупредите сотрудников, работающих в клиент-банке, чтобы не проходили с рабочего компьютера по незнакомым ссылкам, которые мошенники могут отправить в СМС-сообщениях и по e-mail, а также устанавливали приложения для мобильного устройства с оперативной системой Android только из Google Play. Вместе с экспертами по кибербезопасности и банкирами мы составили памятку, как защитить клиент-банк от посягательств мошенников (см. образец).

Алена Громова
Корреспондент УНП

Общество с ограниченной ответственностью «Компания»
ИНН 7801025478, КПП 780101001, ОГРН 123654852789
Санкт-Петербург, ул. Кораблестроителей, д. 12

Уважаемые сотрудники!

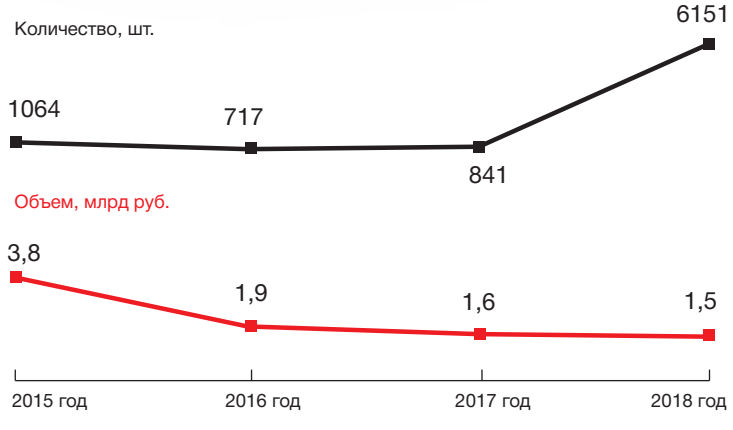
Ознакомьтесь с инструкцией по безопасной работе с системой клиент-банк.

1. Блокируйте компьютер, на котором установлена система, каждый раз, когда покидаете рабочее место, а также закрывайте кабинет на ключ в свое отсутствие.
2. Не допускайте доступа посторонних к компьютеру, на котором установлена система.
3. Самостоятельно составьте секретный и открытый ключи электронной подписи в системе, не храните сведения о ключах в открытом доступе: в блокнотах, записках и на стикерах.
4. Храните флеш-карту с ключом доступа к системе в сейфе. Не копируйте ключ на жесткий диск компьютера, в сетевые папки, на несъемные носители информации. Извлекайте флеш-карту с ключом каждый раз, когда завершаете работу в системе.
5. Используйте на компьютере только лицензионное программное обеспечение. Установите антивирусное программное обеспечение с автоматическим обновлением баз. Еженедельно проводите полную антивирусную проверку компьютера.
6. Ежемесячно меняйте пароль для входа в клиент-банк, никому не сообщайте новую комбинацию.
7. Если к вам обращаются по телефону или электронной почте от имени сотрудников банка и просят сообщить пароль к системе, не делайте этого. Срочно сообщите об обращении неизвестных в банк.
8. Не используйте на компьютере средства электронной почты, программы обмена мгновенными сообщениями, сайты социальных сетей.

В случае нарушения работы системы срочно обратитесь в IT-службу ООО «Компания» по телефону +7 (812) 111-11-11, а также уведомите о неполадках банк.

Генеральный директор И.И. Астахов

Как изменились количество и объем несанкционированных операций со счетов компаний



Источник: данные ЦБ

Как определить, что в письмо вшили вирус

Суть: эксперт по кибербезопасности рассказал, какие письма безопаснее не открывать с рабочего компьютера.

На электронную почту главбухов ежедневно приходят десятки писем, но не все сообщения безопасно открывать. Мошенники отправляют вирусы и ссылки на зараженные сайты.

Аферисты подгадывают, когда лучше рассылать фишинговые письма. Например, главбухам – в период отчетности, а директорам – в конце полугодий. Расчет на то, что сотрудник в спешке не обратит внимания на странный вид или сомнительные вложения письма и запустит вирус.

Руководитель направления по развитию продуктов Secure Bank/Secure Portal Group-IB Павел Крылов рассказал, как мошенники заставляют главбухов поверить сообщениям и на какие вложения опасно даже кликать мышью. Эксперт рекомендует обращать внимание на отправителя, тему, содержание и ссылки в сообщении.

«Если вы получили сообщение от незнакомого отправителя, а информация в письме не имеет к вам отношения, то, скорее всего, вы имеете дело с фишингом. Поддельный почтовый адрес, с которого делают рассылку, злоумышленники стараются замаскировать под реальный адрес компании, ее партнеров и клиентов, а также ведомств. Мошенники часто пользуются бесплатными почтовыми сервисами: Yandex, Gmail и т. д. Поэтому необычное, а иногда даже бессмысленное название почтового адреса, с которого пришло сообщение, – явный признак мошенничества».

Павел Крылов,
руководитель направления Secure Bank/Secure Portal Group-IB

Когда письмо вызывает подозрения, нельзя кликать по ссылкам в нем, даже если информация кажется безопасной или интересной.

«Мошенники цинично играют на человеческих слабостях, стараются запугать потенциальных жертв или, наоборот, вызвать любопытство. Если в письме слишком длинная или, наоборот, короткая ссылка, это повод насторожиться. Потенциальную опасность представляют короткие ссылки, созданные с помощью специальных сервисов. Мошенники используют их, чтобы обойти почтовую защиту. Иногда ссылки внутри письма могут быть замаскированы под вложения. Если кликнуть по такому якобы вложению, произойдет автоматический переход по ссылке и вредоносная программа автоматически загрузится».

Павел Крылов,
руководитель направления Secure Bank/Secure Portal Group-IB

Мошенники совершенствуют методы. Поэтому, если пришло письмо от неизвестного отправителя, надо обратиться в службу по информационной безопасности организации. Переходите по ссылке в сообщении и открывайте вложения только после того, как сотрудники службы проверят письмо. Иначе есть риск, что запустите вредоносную программу.

«Если вы не обнаружили в письме признаков фишинга и перешли по ссылке, а после в браузере стали открываться посторонние вкладки или скачиваться файлы, вы все-таки попались на уловки мошенников и атака на компьютер уже началась. Также признак заражения – если сайт выводит ошибки, пустые страницы или предлагает установить расширение. В таком случае срочно обратитесь в службу информационной безопасности».

Павел Крылов,
руководитель направления Secure Bank/Secure Portal Group-IB

Признаки фишинговых писем от мошенников

Мошенники часто пользуются бесплатными почтовыми сервисами: Yandex, Gmail и т. д.

Чтобы не вызвать подозрений и адресат точно открыл письмо, мошенники притворяются работниками компании

Хакеры маскируют сайты под настоящие и под любым предлогом убеждают пройти по ссылке или что-нибудь скачать

От: kadry@gmail.ru
Тема: Коллеги! Проголосуйте за наш отдел!
Дата: Пн 03.06.2019 14:26
Кому: 'Иванова Мария'

Уважаемые коллеги!

Отдел кадров ООО «Компания» участвует в региональном конкурсе профмастерства! Поддержите нас, пожалуйста! Чтобы проголосовать за нас и поддержать доброе имя компании, скачайте, пожалуйста, специальное приложение для голосования по ссылке konkurss.ru и нажмите «проголосовать за сотрудников ООО «Компания». Это займет всего одну минуту!

Большое спасибо всем откликнувшимся!

С уважением,
сотрудники отдела кадров ООО «Компания»

Предупредите сотрудников организации, что аферисты могут также прислать письмо якобы от руководителя компании. Мошенники уверены, что работник не станет игнорировать сообщение от начальства и по просьбе работодателя пройдет по любой ссылке. Поэтому, если не уверены, что письмо прислал директор, безопаснее не проходить по ссылкам до тех пор, пока сообщение не проверит служба безопасности.

Ольга Рэм
Корреспондент УНП

Компьютер главбуха: способы защиты

Суть: атаки на компьютеры главбухов участились. УНП получила рекомендации специалиста по безопасности. Он рассказал, как защититься.

Настройте на компьютере антифишинговый фильтр и автоматическую блокировку. Также запретите устанавливать новые программы и ограничьте права пользователей.

Автоматическая блокировка
Попросите системного администратора, чтобы он выставил таймер для блокировки компьютера. Если сотрудник не работает в течение 15 минут и при этом не выключил компьютер, система автоматически поставит блокировку. В таком случае у посторонних не будет доступа к файлам и документам на компьютере главбуха, а также никто не сможет запустить вирус с флешки.

Ограничение прав
Ограничьте доступ сотрудников к устройствам, с которых выходите в клиент-банк. Не подключайте эти компьютеры к сетевым папкам.

Эксперты рекомендуют выходить в клиент-банк с обособленного компьютера

«Причина подавляющего количества краж – получение мошенниками удаленного доступа к компьютерам, с которых производятся финансовые операции, или заражение устройств банковскими троянами. Поэтому, чтобы защитить компьютер от взлома, своевременно обновляйте и не отключайте антивирусные программы. Также, чтобы предотвратить попытки мошенников заразить систему, запретите сотрудникам установку и запуск на устройстве новых программ».

Вячеслав Медведев, ведущий аналитик компании «Доктор Веб»

Специальный компьютер
Сотрудникам, которые не могут выполнять обязанности без доступа к сетевым папкам организации, а также с ограниченными правами доступа, эксперты рекомендуют выходить в клиент-банк с обособленного компьютера.

«Одна из наиболее успешных мер защиты клиент-банка, а значит, и денег компании – перенос всех операций с банком на отдельный компьютер. Сотрудники не будут проводить на устройстве никаких действий, кроме работы с банком, а значит, мошенники не смогут отправлять на него письма, ссылки и вредоносные коды».

Вячеслав Медведев, ведущий аналитик компании «Доктор Веб»

Антифишинговый фильтр
Установите антиспамовую и антифишинговую защиту. Фильтры автоматически классифицируют письма, распознают сообщения со спамом и вирусами. При переходе по опасной ссылке система предупреждает пользователя об угрозе. В таком случае, даже если мошенники пришлют письмо с «сюрпризом» не вовремя и сотрудник поверит сообщению, программа напомнит о безопасности.

Контроль действий
Проверьте безопасность компьютеров всех сотрудников. Мошенники могут попытаться проникнуть в систему главбуха через устройства других работников. Например, через корпоративные хранилища. Эксперты рекомендуют установить систему контроля действий.

Программа позволяет отслеживать, на какие ресурсы заходят сотрудники. Ознакомьте работников с методом контроля под подпись. Тогда сотрудники подтвердят, что согласны с ограничениями, а значит, не смогут пожаловаться в ГИТ или прокуратуру на нарушение их прав.

Сообщите сотрудникам, что, если кто-то подхватит вирус на постороннем сайте, руководитель может применить меры дисциплинарного взыскания. Тогда работники будут внимательнее к сторонним ресурсам.

Петр Лобов
Корреспондент УНП