Правила обращения с входящими электронными письмами, содержащими подозрительные вложения (фишинговые письма)

В целях обеспечения безопасности рабочего места и минимизации потенциальных рисков, проявляйте осторожность при работе с электронной почтой. По данным Федеральной службы по техническому и экспортному контролю (ФСТЭК России), хакерскими группировками, с адресов ufo@fstec.ru, feo.ufo@fstec.ru, kii.ufo@fstec.ru, oek.ufo@fstec.ru, omto.ufo@fstec.ru, otd2 ufo@fstec.ru, otd9 ufo@fstec.ru, в адрес федеральных органов исполнительной власти, субъектов критической информационной инфраструктуры и организаций Российской Федерации, направляются фишинговые письма, содержащие подозрительные электронные вложения. **Прежде чем открывать такие письма, удостоверьтесь, что вы следуете правилам обращения с входящими электронными сообщениями.**

• Производите проверку почтовых вложений с использованием средств антивирусной защиты. Это поможет защитить ваши данные от вредоносных программ (см. Руководство пользователя при работе с антивирусным программным обеспечением и проверкой файлов);

• Проверяйте имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание на наименование почтового адреса (домена), указанного после символа «@», и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка;

• Для обмена информацией с коллегами, рекомендуется использовать только те адреса электронной почты организаций, с которыми вы регулярно взаимодействуете, и вести список таких адресов;

• Обратите внимание на тему письма. Она должна быть связана с содержанием и актуальна для вас. Злоумышленники могут использовать привлекательные темы, чтобы побудить вас открыть вложение или перейти по ссылке;

• Не открывайте подозрительные файлы, особенно если они имеют незнакомые форматы (.7z, .rar, .zip, doc, .exe, .xlx-файлы) или двойные расширения, например .pdf.exe.

• Будьте осторожны с подозрительными запросами или ссылками, которые приходят к вам по электронной почте или через сообщения от незнакомых отправителей. Вирусы и шпионские программы часто распространяются через электронные письма и ссылки;

• Перед тем как перейти по ссылке, убедитесь, что она ведёт на нужный сайт и не содержит подозрительных символов (#, $, ?). Такие ссылки могут быть опасными. Для проверки безопасности сайта воспользуйтесь специализированными сервисами (https://yandex.ru/safety, https://vms.drweb.ru);

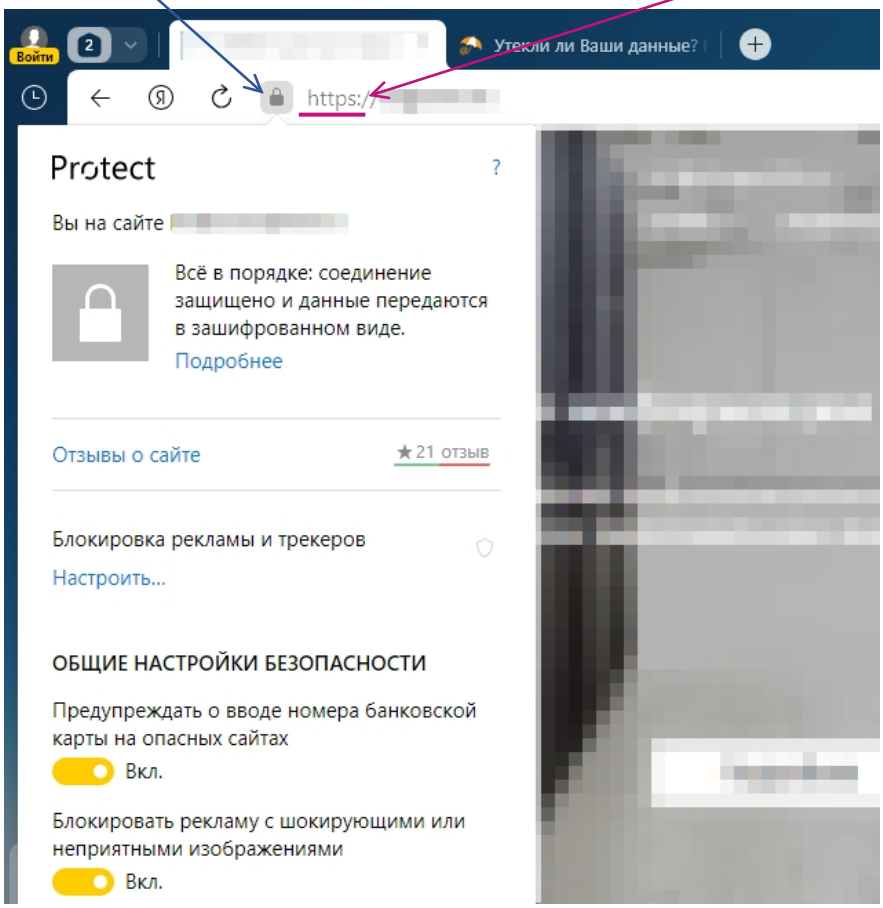
• Ограничьте доступ к личной информации - не разглашайте свои личные данные и информацию о своей работе на публичных ресурсах и социальных сетях.

Если вы подозреваете, что получили фишинговое письмо, сообщите о нем на электронный адрес: ozi@cit.gov35.ru

Руководство пользователя по обеспечению безопасности, связанной с регистрацией на сайтах и сервисах

• Не предоставляйте личные данные на сайтах и сервисах, которые не имеют отношения к вашей работе. Не регистрируйтесь на таких сайтах и сервисах, используя рабочие данные;

• При необходимости указания служебных данных на стороннем сайте или сервисе осуществляйте проверку достоверности и безопасности данных сайта или сервиса, обращая внимание на соединение по **протоколу HTTPS** и наличие действительного **SSL-сертификата**:



• Не рекомендуется сохранять логины и пароли от сервисов, где применяются личные данные сотрудников, в менеджерах паролей браузеров. Вместо автоматического сохранения паролей, рекомендуется запоминать их самостоятельно.

Если у вас есть подозрения о возможной утечке Ваших данных, для проверки вашей конфиденциальной информации, используйте сервис https://chk.safe-surf.ru

Руководство пользователя при работе с антивирусным программным обеспечением и проверкой файлов

Для Kaspersky Internet Security

Шаг 1. Запустите Kaspersky Internet Security на вашем компьютере.

Шаг 2. Кликните на иконку «Настройки» (шестеренка) в правом нижнем углу окна программы.

Шаг 3. В открывшемся окне выберите пункт «Проверка», затем «Проверка файлов».

Шаг 4. Выберите файл, который хотите проверить, нажав на кнопку «Обзор...» и указав путь к файлу.

Шаг 5. Нажмите на кнопку «Открыть», а затем «ОК».

Шаг 6. Файл будет добавлен в список для проверки. Нажмите на кнопку «Запустить проверку».

Шаг 7. Ожидайте окончания проверки. Время проверки зависит от размера файла и мощности вашего компьютера.

Шаг 8. По окончании проверки вы увидите результат - файл чист от вредоносного ПО или содержит вирусы.

Шаг 9. При обнаружении вирусов вы можете выбрать действие, которое необходимо выполнить с вредоносным файлом: удалить, поместить на карантин или игнорировать.

Шаг 10. После выбора действия нажмите на кнопку «Применить», чтобы подтвердить свой выбор.

Для Dr.Web

Шаг 1. Запустите антивирусное программное обеспечение Dr.Web на своем компьютере.

Шаг 2. В главном окне программы нажмите на кнопку «Выбрать объекты для проверки».

Шаг 3. В открывшемся окне нажмите на кнопку «Добавить файл» и выберите файл, который вы хотите проверить.

Шаг 4. После выбора файла нажмите на кнопку «ОК», а затем на кнопку «Начать проверку».

Шаг 5. Дождитесь окончания проверки и получите результаты. Если файл содержит вирусы, Dr.Web предложит удалить их. Если файл чист, вы получите соответствующее сообщение.

Сводка по фишинговым атакам, через электронную почту

1. Хакерскими группировками путем подмены почтовых адресов Управления ФСТЭК России по Уральскому федеральному округу в адрес федеральных органов исполнительной власти, субъектов критической информационной инфраструктуры и организаций Российской Федерации направляются фишинговые письма, во вложениях которых находится архив с наименованием «запрос5161-2.7z». Архив содержит исполняемый файл «20250203_5_161.scr», замаскированный под официальное письмо Управления ФСТЭК России по Уральскому федеральному округу с расширением «.pdf», который является экземпляром вредоносного программного обеспечения типа «троян» (Trojan.Win32.AntiVM.das).

2. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Минпромторга России. Во вложениях указанных писем содержится файл-приманка с наименованием «Письмо_в_организации_по_ привлечению_осужденных.docx» и вредоносный архив с наименованием «Форма заполнения.rar». Внутри указанного архива содержится файл-приманка «список рассылки.docx» и вредоносный исполняемый файл с наименованием «Форма заполнения.pdf.exe». После запуска пользователем указанного исполняемого файла на целевую систему осуществляется загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Ozone RAT).

3. Хакерской группировкой Sticky Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лиц федеральных органов исполнительной власти Российской Федерации. Во вложениях указанных писем содержится вредоносный исполняемый файл с наименованием «АО-*******-12904ДО.pdf.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Darktrack RAT).

4. Хакерской группировкой Horns&Hooves, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с расширением «.zip». Внутри указанного архива содержатся вредоносные файлы, замаскированные под коммерческие документы с расширением «.js». После запуска пользователем указанных файлов осуществляется выполнение вредоносного скрипта JavaScript для демонстрации документа-приманки (например, изображение (PNG), текстовый файл (TXT), документ (PDF)) и внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (BurnsRAT и NetSupport RAT).

Примеры фишинговых писем

От: Tina <tina@sunlinesankei.com.hk>
Отправлено: 6 сентября 2024 г. 1:05
Кому:
Тема: NEW ORDER P24002603 > modified OC 21114020 > shipment 211014093

Dear Team,

kindly like to inform that we have prepared the 2nd shipment for the above-mentioned order.
Please check the attached drafts of shipping documents.
As soon as we have your OK, we continue with the release from our foreign control and the customs export declaration.

Thank you for your kind support.

Tina
Customer Support Administrator
Sunline Sankei Yokohama (H.K.) Co. Ltd.
Tel : 2763-1233
Fax : 2786-2156
e-mail : tina@sunlinesankei.com.hk

От: info@inforussia.org <info@inforussia.org>
Отправлено: 16 сентября 2024 г. 16:18
Кому: Вожегодский территориальный сектор ЗАГС
Тема: ЦИБ ФСБ РФ №1091/119/05 от 16.09.2024.

Центр информационной безопасности ФСБ России
Добрый день, ! В связи с проведением Центром проверки ряда государственных и частных организаций из-за подозрений в незаконном распространении персональных данных и сотрудничестве с **украинскими спецслужбами**, просим Вас предоставить перечень финансовых документов в срок до 17.09.2024 в электронном виде по адресу cib@fsb.ru.

Перечень документов –документы.zip.

--
С уважением,
Андреев Н.В.
6 отдел 7 управления ЦИБ ФСБ России.
107031, г.Москва, ул.Большая Лубянка, дом 1.
+7 (495) 224-2222
+8 (800) 224-2222
Это письмо является конфиденциальной информацией и не подлежит распространению. Если вы считаете, что получили его ошибочно – немедленно сообщите по адресу cib@fsb.ru и удалите письмо.
Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, либо представление таких сведений (информации) в неполном объеме или в искаженном виде ведёт за собой ответственность согласно статьям 19.7, 5.39 КоАП РФ и статьёй 137 УК РФ.

От: БУЗ ВО "Вологодская областная детская больница № 2" <vodb2@yandex.ru>
Отправлено: 5 сентября 2024 г. 14:12
Кому: ozi@cit.gov35.ru
Тема: Информация о мошенниках

Добрый день. Сообщаем Вам, что сотрудникам БУЗ ВО " Вологодская областная детская больница№2" массово поступают поддельные письма в Telegram от Министерства здравоохранения Российской федерации, с последующими звонками от имени главного врача, копированием ее голоса и использованием фотографии . Фото письма прилагается.
--
С уважением,
БУЗ ВО "Вологодская областная детская больница № 2"

МИНИСТЕРСТВО
МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
127994, ГСП-4, г. Москва, Рахмановский пер, д. 3

Главному врачу, БУЗ ВО Областной детской больницы № 2,

Уважаемая, !

В рамках реализации комплекса мер по обеспечению информационной безопасности в учреждениях здравоохранения, утвержденного из Министерства здравоохранения, мне поручено провести консультационные беседы с рядом сотрудников вверенной Вам Областной детской больницы № 2.

Прошу Вас оказать содействие в организации телефонных бесед с сотрудниками, список которых приведен в Приложении 1 к данному документу. Обращаю Ваше внимание, что Приложение 1 имеет гриф "Для служебного пользования" и не подлежит распространению.

Цель данных бесед - повышение уровня информированности сотрудников по вопросам обеспечения защиты конфиденциальных данных и соблюдения требований информационной безопасности в условиях работы больницы.

Прошу Вас ознакомить указанных в Приложении 1 сотрудников с предстоящими беседами в период с 29.08.2024 по 06.09.2024 в рабочее время.

Содержание бесед имеет служебный характер и не подлежит дополнительному согласованию.

Рассчитываю на Ваше понимание и поддержку в реализации мероприятий, направленных на укрепление информационной безопасности в системе здравоохранения.

С уважением, Шевчук Александр Николаевич.

Сотрудник Аппарата
Прикомандированных Сотрудников
ФСБ при Министерстве
здравоохранения **А.Н. Шевчук**