Руководство пользователя по противодействию кибератакам с использованием электронной почты

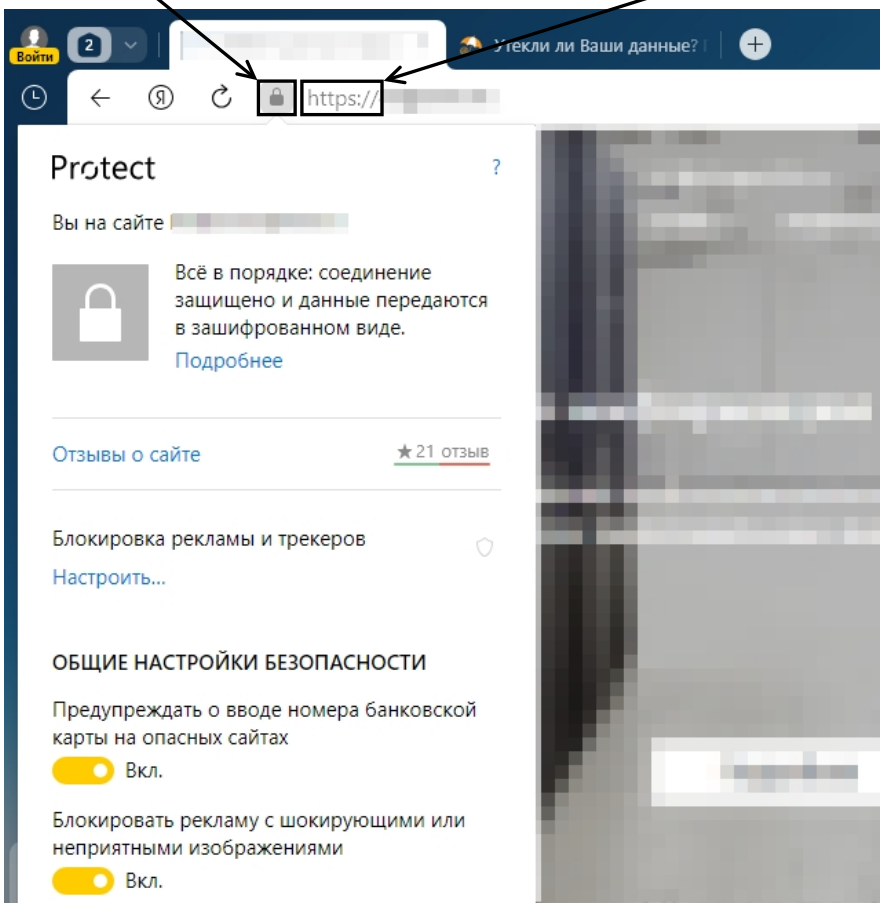
- Проверяйте почтовый адрес и имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обратить внимание на наименование почтового адреса (домена), указанного после символа «@», и сравнить его с официальным адресом (доменом) организации, с которой осуществляется 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;
- Для проверки домена отправителя электронного письма используйте сервис https://www.reg.ru/whois/;
- Проявляйте осторожность при получении подозрительных запросов или ссылок, 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 представлять опасность;
- Для проверки безопасности сайтов и ссылок воспользуйтесь специализированными сервисами (https://yandex.ru/safety, https://vms.drweb.ru);
- Не открывайте подозрительные файлы, особенно если они имеют незнакомые форматы (.7z, .rar, .zip, doc, .exe, .xlx-файлы) или двойные расширения, например .pdf.exe. Открытие таких вложений создает предпосылки к возникновению угроз информационной безопасности, возможности получения доступа посторонних лиц к служебной переписке, парольной-ключевой и прочей чувствительной информации;
- 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

• При регистрации на различных интернет-ресурсах в личных целях, запрещается использовать служебные данные, включая адрес электронной почты. Указанная информация используется злоумышленниками для проведения фишинговых атак и создания угроз информационной безопасности;

• 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

1. Запустите Kaspersky Internet Security на вашем компьютере.
2. Кликните на иконку «Настройки» (шестеренка) в правом нижнем углу окна программы.
3. В открывшемся окне выберите пункт «Проверка», затем «Проверка файлов».
4. Выберите файл, который хотите проверить, нажав на кнопку «Обзор...» и указав путь к файлу.
5. Нажмите на кнопку «Открыть», а затем «ОК».
6. Файл будет добавлен в список для проверки. Нажмите на кнопку «Запустить проверку».
7. Ожидайте окончания проверки. Время проверки зависит от размера файла и мощности вашего компьютера.
8. По окончании проверки вы увидите результат - файл чист от вредоносного ПО или содержит вирусы.
9. При обнаружении вирусов вы можете выбрать действие, которое необходимо выполнить с вредоносным файлом: удалить, поместить на карантин или игнорировать.
10. После выбора действия нажмите на кнопку «Применить», чтобы подтвердить свой выбор.

Для Dr.Web

1 вариант

1. Запустите антивирусное программное обеспечение Dr.Web на своем компьютере.
2. В главном окне программы нажмите на кнопку «Сканер».
3. В открывшемся окне выберите режим «Быстрая», «Полная» или «Выборочная».
4. После выбора нажмите на кнопку «Начать проверку».
5. Дождитесь окончания проверки и получите результаты. Если файл содержит вирусы, Dr.Web предложит удалить их. Если файл чист, вы получите соответствующее сообщение.

2 вариант

1. Выберите файл для проверки, выделив его щелчком мыши.
2. Нажмите правой кнопкой мыши на выбранный файл.
3. Запустите проверку, выбрав в появившемся меню пункт «Проверить Dr.Web».

Правила пользования паролей

- пароли от учетных записей на разных сервисах должны отличаться;
- не следует использовать пароли «по умолчанию» (они не соответствуют требованиям ИБ);

Требования к сложности паролей

- длина пароля должна быть не менее 15 символов;
- пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), цифры (от 0 до 9), специальные символы (например, !, », №, %, *, /);
- в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов);
- запрещается использование комбинаций соседних клавиш и словарных слов;

Рекомендации

- не рекомендуется сохранять логины и пароли в менеджерах паролей браузеров;
- вместо автоматического сохранения паролей, рекомендуется запоминать их самостоятельно. Для формирования удобного для запоминания пароля, рекомендуется определить набор несвязанных слов, взять от каждого первые три буквы, и дополнить получившееся сочетание цифрами и специальными символами.

1. Выберите 3-4 несвязанных друг с другом слова:

• Зонт • Летит • Над • Пустыней

2. Сократите каждое слово до первых трех букв:

• Зонт → Зон • Летит → Лет • Над → Над • Пустыней → Пус

3. Переключите клавиатуру на английскую раскладку (Shift+Alt);

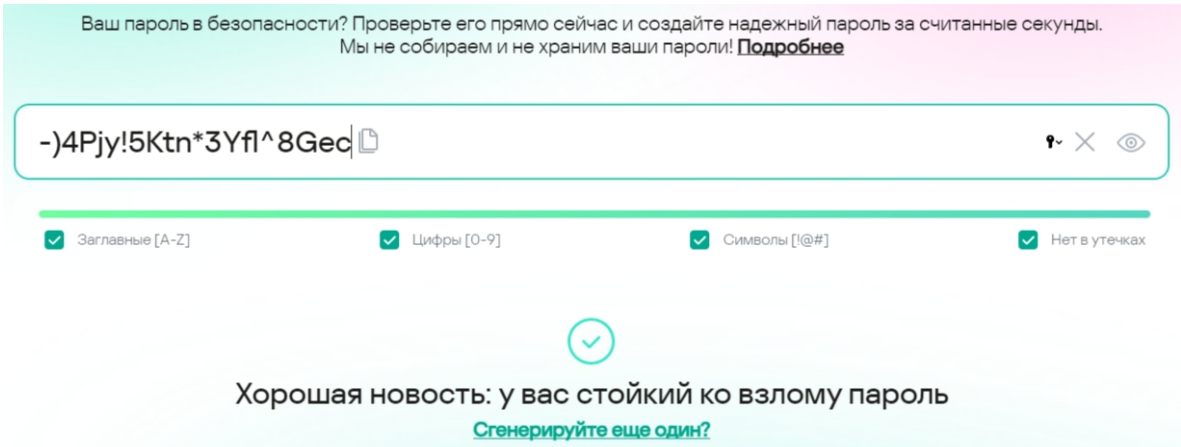
4. Наберите в английской раскладке получившееся буквенное сочетание, ориентируясь на русские буквы:

• Зон → Pjy • Лет → Ktn • Над → Yfl • Пус → Gec

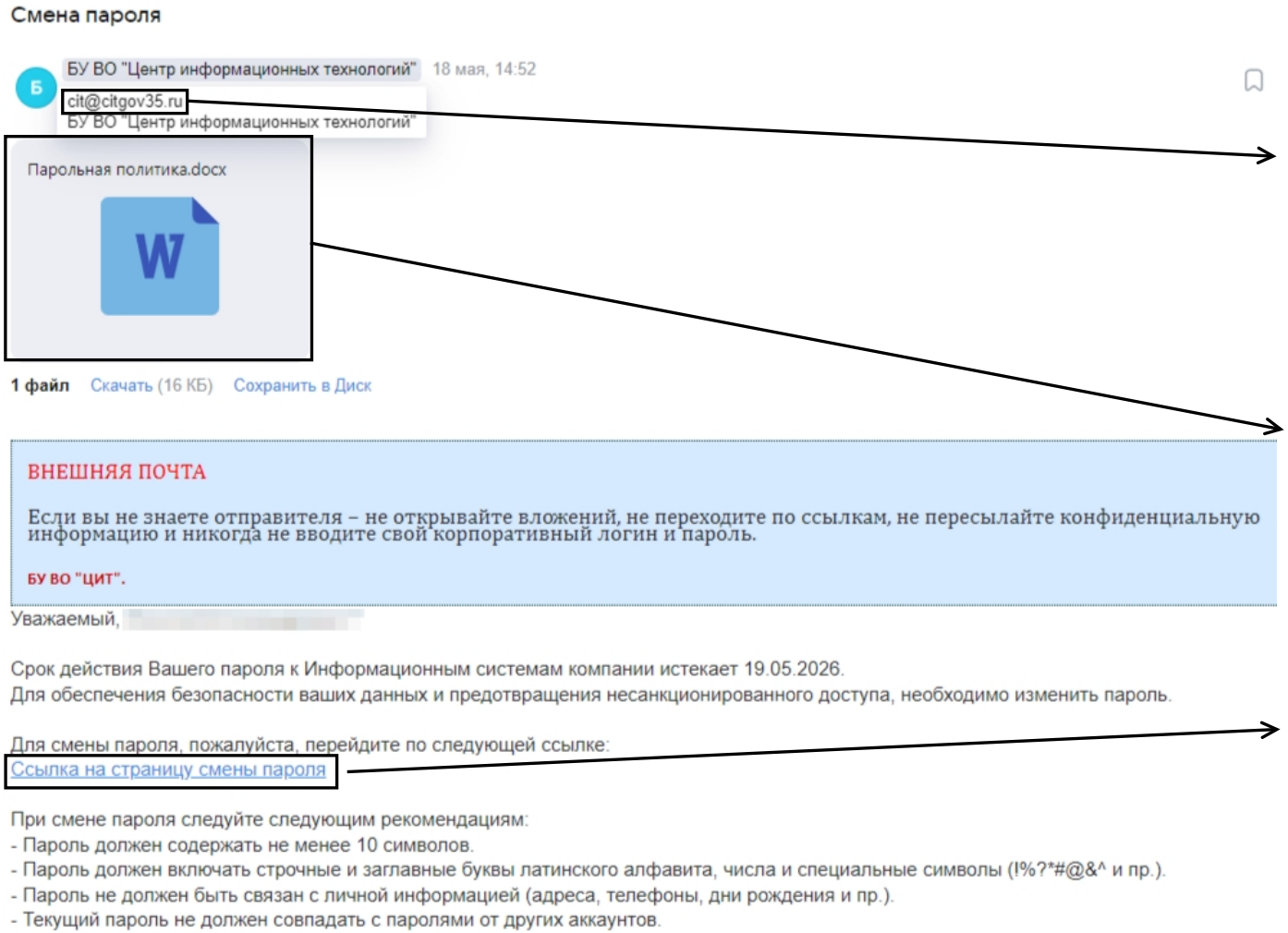
5. Дополните получившееся сочетание цифрами и специальными символами:

-)4 Pjy**!5**Ktn***3**Yfl**^8**Gec

6. Для проверки надежности пароля используйте специальные сервисы, например https://password.kaspersky.com/ru/



Руководство по противодействию кибератакам с использованием электронной почты



1. Подменный почтовый адрес отправителя

Письмо получено с подменного почтового адреса электронной почты. Официальным адресом в данном случае является **cit@cit.gov35.ru**

2. Подозрительное вложение

Замаскированный файл (архив) может содержать загрузчик вредоносного программного обеспечения, предназначенного для кражи конфиденциальной информации.

3. Замаскированная ссылка

Может вести на подменный сайт. При переходе по ссылке злоумышленники получают доступ к служебной информации пользователя.

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

Примеры фишинговых писем

Коллеги,

В настоящее время осуществляется массовая проверка компаний на устойчивость к мошенническим рассылкам.
Призываем вас быть бдительными и помнить несколько важных правил:
- обращать внимание на стилистику письма;
- всегда проверять отправителя;
- не переходить по подозрительным ссылкам из письма.

С подробным руководством по противодействию социальной инженерии можно ознакомиться в методологических рекомендациях.

Уважаемый, [redacted]!

Срок действия Вашего пароля к Информационным системам компании истекает.
Для обеспечения безопасности ваших данных и предотвращения несанкционированного доступа, необходимо изменить пароль.

Для смены пароля, пожалуйста, перейдите по следующей ссылке:
Ссылка на страницу смены пароля

При смене пароля следуйте следующим рекомендациям:
- Пароль должен содержать не менее 10 символов.
- Пароль должен включать строчные и заглавные буквы латинского алфавита, числа и специальные символы (!%?*#@&^ и пр.).
- Пароль не должен быть связан с личной информацией (адреса, телефоны, дни рождения и пр.).
- Текущий пароль не должен совпадать с паролями от других аккаунтов.

С уважением,

Клиент ООО [redacted] заявил об ущербе после ДТП по Вашей вине. Просим немедленно отнестись к следующим документам в приложении.

Извещение о ДТП: извещение_00029112022.pdf

В случае отсутствии возражений с Вашей стороны, ООО [redacted] выступит с требованием о выплате ущерба с вашего ОСАГО.

С уважением

Департамент экспертизы
и урегулирования убытков

От: office@digital-gov.tech
Кому: территориальный многофункциональный центр (МФЦ)
Тема: Важное уведомление об обеспечении безопасности

Уважаемые представители Государственного автономного учреждения "Цифровой Севастополь-многофункциональный центр предоставления государственных и муниципальных услуг в городе Севастополе",

Обращаемся к Вам от имени Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации с целью повышения безопасности Ваших данных в системе ЕСИА.

В ходе регулярного мониторинга безопасности учетных записей государственных учреждений, были выявлены уязвимости, касающиеся учетных данных администраторов ЕСИА Вашей организации. В связи с этим, мы просим Вас принять срочные меры для усиления защиты и предоставить следующую информацию:

электронно-цифровые подписи (ЭЦП) с контейнерами и паролями от них, принадлежащие исключительно администраторам ЕСИА. Это критически важно для проведения анализа и предотвращения возможных попыток несанкционированного доступа.
Мы понимаем, что обеспечение безопасности данных таких сотрудников может оказаться хлопотным процессом, однако он необходим для непрерывной и надежной работы наших информационных систем.

Просим Вас отреагировать на это уведомление и предоставить запрошенные данные в ответ на данное письмо, приложив к нему необходимые ЭЦП с контейнерами и паролями. Это позволит нам быстро провести необходимый анализ и принять соответствующие меры.

С уважением и надеждой на Ваше сотрудничество,

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Департамент развития государственных платформ

Сводка по фишинговым атакам, с использованием электронной почты

1. Хакерской группировкой BO_team с подменных почтовых адресов solodovnikov.sn@rostransnadsor.ru и konovaltsev.ma@cfo-rostransnadzor.ru, зарегистрированных в фишинговом домене @rostransnadsor.ru, от лица Ространснадзора России осуществляется рассылка электронных писем, содержащих вредоносное вложение в виде файла. После открытия пользователем указанного исполняемого файла осуществляется загрузка и внедрение вредоносного программного обеспечения, предназначенного для кражи конфиденциальной информации.

2. Злоумышленниками, с подменного почтового адреса office@digital-gov.tech от лица Минцифры России в адрес территориальных многофункциональных центров осуществляется рассылка электронных писем с тематикой «Важное уведомление об обеспечении безопасности». В электронном письме злоумышленники просят направить парольную и ключевую информацию работников организации на подменный почтовый адрес.

3. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица поддельных или скомпрометированных адресов почты контрольных и регулирующих органов. Во вложениях указанных писем прикреплен вредоносный файл с инструкцией и QR-кодом. После открытия пользователем указанной инструкции с QR-кодом осуществляется загрузка и внедрение вредоносного программного обеспечения, которое фиксирует все нажатия клавиш на клавиатуре компьютера или другого устройства ввода.

4. Хакерскими группировками, с подменного почтового адреса postin@fsteck-gov[.]ru в адрес федеральных органов исполнительной власти, субъектов критической информационной инфраструктуры и организаций Российской Федерации направляются фишинговые письма от имени ФСТЭК России с тематикой «Критическое обновление — ФСТЭК России». В вложениях указанных писем содержатся документ-приманка с наименованием «KB5051430.pdf» и архив с наименованием «KB5051430.zip», содержащий исполняемый файл с наименованием «KB5051430.exe». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер».

<u>При этом официальным почтовым ящиком ФСТЭК России, с которого осуществляется рассылка электронных писем, являются адреса электронной почты с наименованием домена «@fstec.ru».</u>

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