МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТВЕРСКОЙ ОБЛАСТИ

Студенческий пер., д. 28,
г. Тверь, 170100
тел.: + 7 (4822) 33-30-30
эл.почта: digital@tverreg.ru
сайт: минцифры.тверскаяобласть.рф
сайт: 4822.digital

02.04.2025 № 817-СС

На № _____от _____

Руководителю Аппарата Правительства Тверской области

Руководителям исполнительных органов Тверской области

Руководителям органов местного самоуправления Тверской области

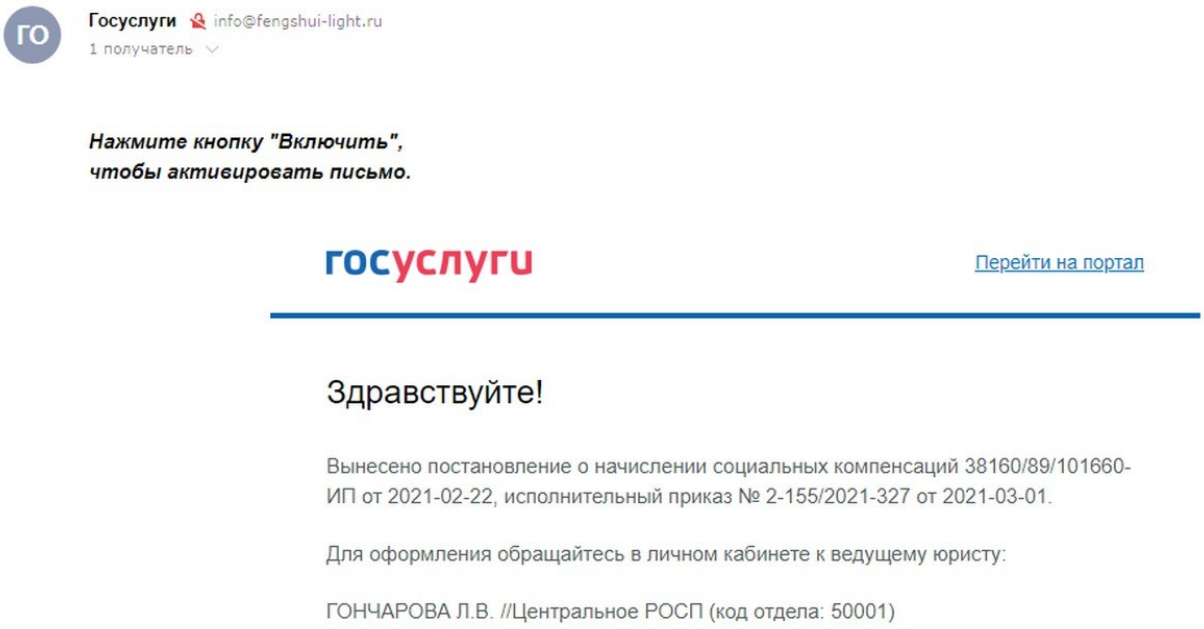
В связи с ростом числа поддельных ресурсов, рассылок и иных вариантов атак типа «фишинг», Министерство цифрового развития и информационных технологий Тверской области для избежания утечек персональных данных рекомендует соблюдать следующий свод правил, разработанный ФСТЭК России:

1. Всегда внимательно проверяйте ссылку, по которой предлагается перейти: не перепутаны ли буквы в названии сайта. Если с написанием что-то не так, это верный признак, что страница поддельная.
2. Перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где «s» означает secure — безопасное), то все в порядке.
3. Даже если письмо или сообщение со ссылкой пришло от известного пользователя, все равно следует помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя осторожно с любыми письмами со ссылками, а не только с пришедшими из неизвестного источника. В том числе и с письмами из официальных источников.
4. Вместо того чтобы переходить по ссылке, гораздо надежнее ввести адрес вручную в новом окне браузера. Следуя этому сценарию, вы существенно снижаете вероятность перехода по подложной ссылке.
5. Обнаружив фишинговую операцию, крайне желательно сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети (если такие ссылки рассылает кто-то из пользователей) и так далее. Так вы поможете вовремя остановить мошенников.
6. По возможности не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше

воспользоваться мобильным Интернетом. Дело в том, что за таким Wi-Fi могут стоять мошенники, подменяющие адрес сайта на уровне подключения и перенаправляющие вас таким образом на поддельную страницу.

7. Любой файл может оказаться трояном-шпионом или даже трояном-вымогателем, как и вложения к письмам и сообщениям. Будьте бдительны!
8. Используйте отечественное средство антивирусной защиты. В большинстве случаев фишинговая ссылка будет заблокирована на этапе перехода по ней.

Для иллюстрации признаков фишингового письма рассмотрим приведенный ниже скриншот.



В первую очередь обращайте внимание на адресата письма. Если отправителем указывается официальная организация (Госуслуги), но при этом почта отправителя не совпадает с официальным доменом отправителя (в данном случае fengshui-light.ru), то данное письмо является фишинговым.

Если в письме присутствуют очевидные призывы к действию (например, Нажмите кнопку «Включить») ни в коем случае не осуществляйте данное действие. Такое письмо также является фишинговым.

Еще одним признаком фишингового письма является психологическое давление и сжатые сроки реагирования. Как приведено на скриншоте выше – Вынесено постановление.

По имеющейся статистике количество фишинговых писем, содержащих вредоносные вложения, снижается в пользу писем, содержащих вредоносные ссылки.

В случае если отправитель является доверенным пользователем и его почтовый адрес написан без ошибок, но письмо пришло неожиданно или есть иные подозрения о взломе необходимо связаться с отправителем по телефону

и уточнить легитимность письма. В случае, если нет возможности проверить легитимность письма звонком необходимо сообщить о поступлении подозрительного письма вашему администратору информационной безопасности, либо напрямую дежурному сотруднику отдела ГосСОПКА ГКУ ТО «ЦИТ» по круглосуточному номеру телефона 84822333368 либо адресу электронной почты gossopka@tverreg.ru.

Просим довести данные правила кибергигиены до сотрудников Ваших организаций и организаций, подведомственных Вашей.

Министр **С.В. Снегирев**

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота Правительства Тверской области.

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 0D08AA6A55671725CD69B1A87386BC5B
Кому выдан: Снегирев Сергей Владимирович
Действителен: с 24.04.2024 до 18.07.2025

Храмов Игорь Сергеевич
8 (4822) 33 33 68