

## **Интернет-мошенники действуют под маской швейцарской таможни | Les escrocs se présentent comme les douaniers suisses sur Internet**

Автор: Татьяна Гирко, Берн-Сион, 1. 12. 2015.



(DR)

В последнее время жители Швейцарии все чаще получают сообщения, автором которых якобы является Федеральная таможенная администрация (AFD). Ведомство предупреждает о мошенническом характере таких сообщений и советует их игнорировать или удалять.]

Ces derniers temps, des habitants suisses reçoivent de plus en plus souvent des messages provenant prétendument de l'Administration fédérale des douanes (AFD) qui met en garde contre ces messages frauduleux et conseille de les ignorer et de les supprimer.

На прошлой неделе Федеральная таможенная администрация выступила с официальным заявлением, в котором говорится, что ее сотрудники никогда не отправляют сообщения, касающиеся финансовых операций, по электронной почте или смс. Именно таким путем, под видом AFD, мошенники в последнее время пытаются выманить деньги у швейцарцев.

В большинстве случаев, сообщает AFD, злоумышленники предлагают получателям письма сообщить некоторую информацию, связанную с банковскими счетами, или персональные данные. Федеральная таможенная администрация подчеркивает, что в письмах от ее имени графа «отправитель» должна выглядеть следующим образом: имя@ezv.admin.ch.

---

From: Eidgenössische Zollverwaltung EZV [REDACTED]  
Sent: Donnerstag, 26. November 2015 12:24  
To: [REDACTED]  
Subject: Tax Refund Mitteilung

Nach der letzten jährlichen Berechnung Ihrer steuerlichen Aktivität haben wir festgestellt, dass Sie eine Steuerrückzahlung von 418.17 Euro erhalten können.

Bitte senden Sie das Formular Rückerstattung Steuern auf Eidgenössische Zollverwaltung EZV Website und erlauben Sie uns 2-4 Werktage dauern, bis die Informationen zu verarbeiten.

Eine Rückerstattung kann für eine Vielzahl von Gründen verzögert werden.

Zum Beispiel senden ungültige Datensätze oder nach Ablauf der Frist anwenden.

Das Formular für Ihre Steuererstattung sind abrufbar:

[Klicken Sie bitte hier Ihr Konto überprüfen](#)

Vielen Dank,

Eidgenössische Zollverwaltung EZV

Подозрительные письма рекомендуется игнорировать или удалять, при этом их получатели могут также сигнализировать о «фишинге» в Центр регистрации и анализа для защиты информационных данных ([MELANI](#)). Туда же следует обратиться и тем, кто уже попался на удочку интернет-мошенников и потерял деньги. В таком случае AFD рекомендует также уведомить полицию.

*Так выглядит подозрительное сообщение © admin.ch*

Киберпреступники все чаще и изобретательнее маскируются под официальные органы. Так, в начале ноября власти кантона Вале предостерегли местных жителей от разглашения конфиденциальных данных по запросу, якобы рассылаемому местной налоговой службой. Несколько бдительных граждан пожаловались властям на полученные ими письма с просьбой предоставить дополнительную информацию. Юридическим компаниям предлагалось заполнить декларацию с описью недвижимости и прислать квитанции о перечислении арендной платы.

Проигнорировав подобные электронные сообщения, некоторые адресаты получили звонки от

«налоговых инспекторов», потребовавших ответить на запросы в кратчайший срок под угрозой санкций. Валежанская полиция считает, что мошенники могли собирать информацию с целью незаконного присвоения арендной платы или организации другой финансовой аферы в будущем.

В этом случае некоторых адресатов «фишинга» снова выручила внимательность: в графе «отправитель» значился адрес типа @dr.com, в то время как налоговая служба Вале пользуется адресами с окончанием @admin.vs.ch. Кроме того, как и Федеральная таможенная администрация, фискальные органы не отправляют запросы подобного рода электронной почтой, предупреждает местная полиция.

Добавим, что неделю назад швейцарский орган по защите информационных данных MELANI предупредил о новой угрозе, распространяющейся в киберпространстве Конфедерации. Речь идет о вымогательстве со стороны хакеров. Авторы DDoS-атак, в результате которых пользователи не могут получить доступ к определенным ресурсам или сервисам, требуют выкуп с владельцев сайтов для восстановления его нормальной работы.

Атаки подобного типа давно известны, отмечают специалисты MELANI. Однако раньше они чаще были связаны с политическими акциями или направлены против конкурентов. Теперь же мошенники используют атаки типа «отказ в обслуживании» для того, чтобы вымогать деньги у своих жертв. Среди последних чаще всего оказываются компании, чья работа зависит от функционирования их сайта, к которому пользователи в случае атаки не могут получить доступ.

Объектом одной из самых масштабных DDoS-атак в Европе недавно стал швейцарский [сервис ProtonMail](#), предоставляющий в распоряжение своих пользователей сверхзащищенную электронную почту. Хакеры не добрались до содержимого писем, однако заблокировали доступ к сервису. «ProtonMail оказался в довольно необычной ситуации, поскольку атака против нас была масштабной, изощренной и длилась очень долго. Дело в том, что первая группа, которая обрушилась на нас с DDoS-атакой, не требовала денег. Она хотела вывести нас навсегда из строя, так что, возможно, это было политически мотивировано», – поделился с «Нашей Газетой.ch» своим опытом генеральный директор стартапа Энди Йен. Помощь лучших швейцарских специалистов позволила ProtonMail наладить нормальную работу сервиса в течение нескольких дней.

Что же делать, если хакеры требуют денег? «При атаке с целью вымогательства хакеры, как правило, не атакуют ваш сайт в течение длительного периода времени, поскольку это довольно дорого. Они попытаются испугать вас, а потом отступят, если вы будете их игнорировать. Поэтому мы рекомендуем не идти на поводу у хакеров, требующих выкуп, но только убедившись, что ваша компания технически подготовлена и может отразить крупномасштабную атаку, поскольку такое – хотя и редко – тоже может случиться, в чем мы лично убедились», – сказал Энди Йен.

Служба MELANI также предупреждает: заплатив шантажистам, жертвы способствуют финансированию их деятельности и не получают взамен никакой гарантии, что атака прекратится.

Напомним, что, согласно [последнему исследованию](#) компании EY, 9 из 10 крупных компаний не

чувствуют себя в полной кибербезопасности с информационными технологиями, имеющимися в их распоряжении.



## Добавить комментарий

Пожалуйста, [войдите](#) или [зарегистрируйтесь](#) , чтобы отправить комментарий

---