Содержание

Что такое спам? 2
Как определять спам-сообщения 2
Проверить адрес отправителя 2
Оценить запрашиваемую информацию 2
Соблюдать осторожность, если сообщение требует срочных действий 2
Проверить, используется ли в электронном письме ваше имя 3
Проверить грамматику и орфографию 3
Соблюдать осторожность при открытии вложений 3
Последствия 3
Последствия для личности 3
Последствия для НГТУ 3
Примеры спам-сообщений 4
Примеры поддельных сайтов 8

Что такое спам?

В широком смысле спамом называют нежелательные сообщения, которые, как правило, носят коммерческий или вводящий в заблуждение характер. Спам существует столько же, сколько и сам интернет, и, несмотря на значительные усилия по борьбе с ним, проблема спама остается актуальной.

Как определять спам-сообщения

Иногда очевидно, что сообщение является спамом. Однако, если непонятно на первый взгляд, существует несколько признаков, на которые стоит обратить внимание:

Проверить адрес отправителя

Большая часть спам-сообщений поступает с адресов электронной почты, которые выглядят как бессмысленный набор символов, например ***amazondeals@tX94002222aitx2.com*** или аналогичные. Наведя курсор на имя отправителя, которое само по себе может быть написано странно, можно увидеть полный адрес электронной почты. Если непонятно, является ли адрес электронной почты настоящим, его можно ввести в поисковую систему для проверки.

Оценить запрашиваемую информацию

Легально работающие компании не связываются с пользователями без конкретной причины посредством нежелательных сообщений электронной почты и не просят предоставить личную информацию, такую как банковские реквизиты, данные кредитной карты, номер социального страхования и прочую информацию. Как правило, к нежелательным сообщениям с просьбой «подтвердить данные учетной записи» или «обновить информацию учетной записи» следует относиться с осторожностью.

При необходимости лучше самостоятельно перейти на соответствующий веб-сайт, введя его веб-адрес прямо в браузере или выполнив поиск в поисковой системе, и войти в свою учетную запись, не переходя по ссылке в электронном письме.

Соблюдать осторожность, если сообщение требует срочных действий

Спамеры часто пытаются оказать давление на пользователей, создавая ощущение срочности. Например, тема сообщения может содержать такие слова, как «срочно» или «требуется немедленное действие», чтобы заставить пользователя действовать.

Проверить, используется ли в электронном письме ваше имя

Некоторые спам-сообщения составляются довольно сложно, однако потенциальная опасность скрывается за расплывчатыми выражениями, например, «Уважаемый клиент» и аналогичными. Легальные компании, на рассылки которых вы подписаны, знают ваше имя и направляют электронные письма с соответствующим обращением.

Проверить грамматику и орфографию

Опечатки и грамматические ошибки – это тоже сигналы опасности, как и странные формулировки или необычный синтаксис, которые могут возникнуть в результате перевода текста электронного письма на разные языки несколько раз с помощью Google Translate.

Соблюдать осторожность при открытии вложений

Легально работающие организации стараются не рассылать электронные письма с вложениями, поскольку они могут содержать вредоносное ПО. Получение электронного письмо от неизвестного отправителя с призывом открыть вложение является признаком спама. Не следует открывать вложения в неизвестных письмах, поскольку они могут загружать на устройство вредоносное ПО.

Последствия

Последствия для личности

В случаях ввода по фишинговым ссылкам своих личных данных (номер телефона, учетные данные, банковские реквизиты, коды от госуслуг) вы передаете злоумышленникам доступ к своим банковским счетам и госуслугам.

Последствия для НГТУ

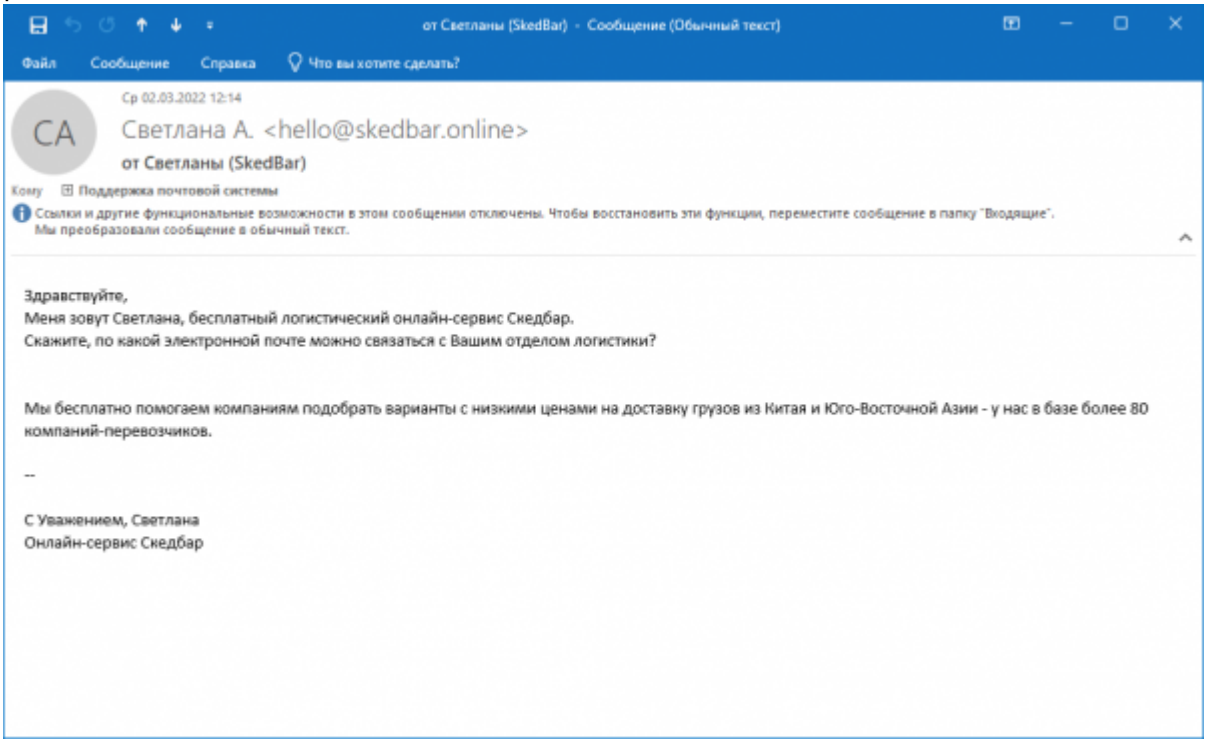
В случаях ввода по фишинговым ссылкам своих корпоративных учетных данных вы передаете злоумышленнику доступ к единой учетной записи НГТУ. Злоумышленник может пользоваться Вашей учетной записью для совершения других компьютерных атак, в том числе фишинговых. В случаях запуска вредоносных файлов вы компрометируете компьютер, на котором работаете. Вредоносные программы могут привести к ряду ситуаций, в которых пострадают информационные системы НГТУ - файлы могут быть безвозвратно зашифрованы, удалены, украдены. Также компьютер может быть задействован для совершения других компьютерных атак. Оба описанных случая могут привести к репутационному и правовому ущербу НГТУ - корпоративная почта будет блокироваться другими почтовыми сервисами (корпоративные

сервисы других организаций и общедоступные сервисы, такие как mail.ru и yandex.ru), украденные или поврежденные данные могут содержать охраняемую законом информацию (персональные данные), скомпрометированные компьютеры могут быть использованы для совершения противоправных действий, попадающих под административную и уголовную ответственность, в которых НГТУ будет фигурировать.

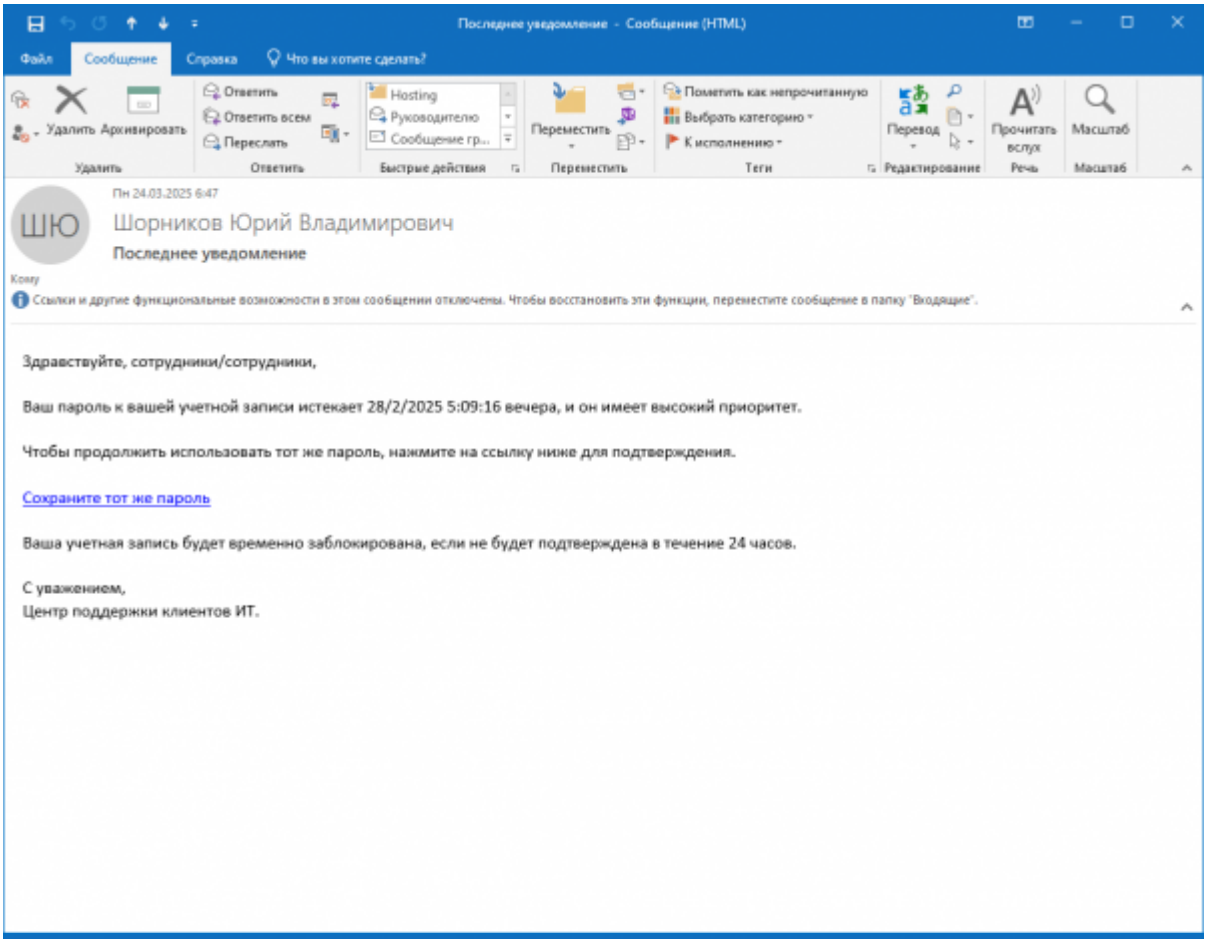
Примеры спам-сообщений

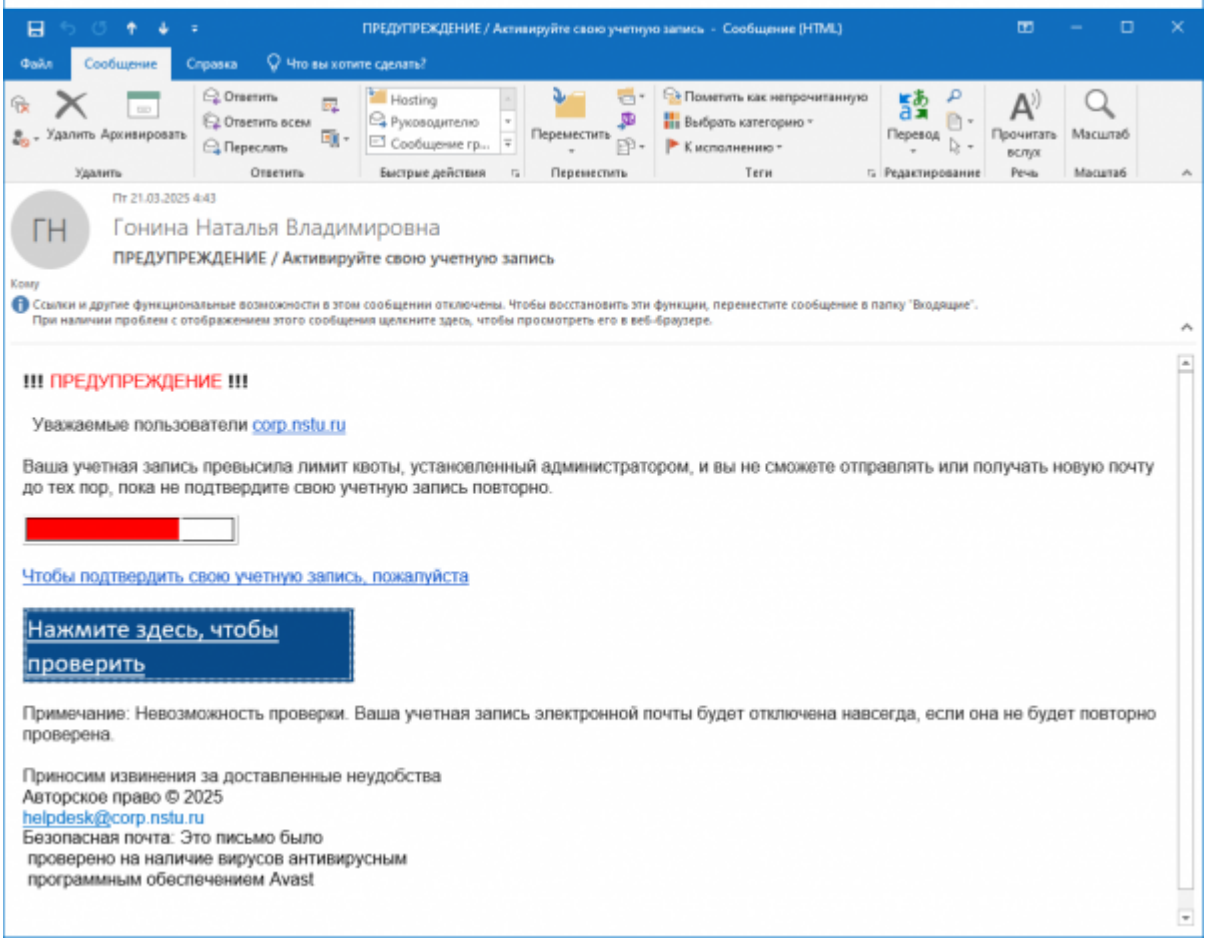
Спам-сообщения бывают различных категорий. Ниже приведены примеры наиболее распространенных из них:

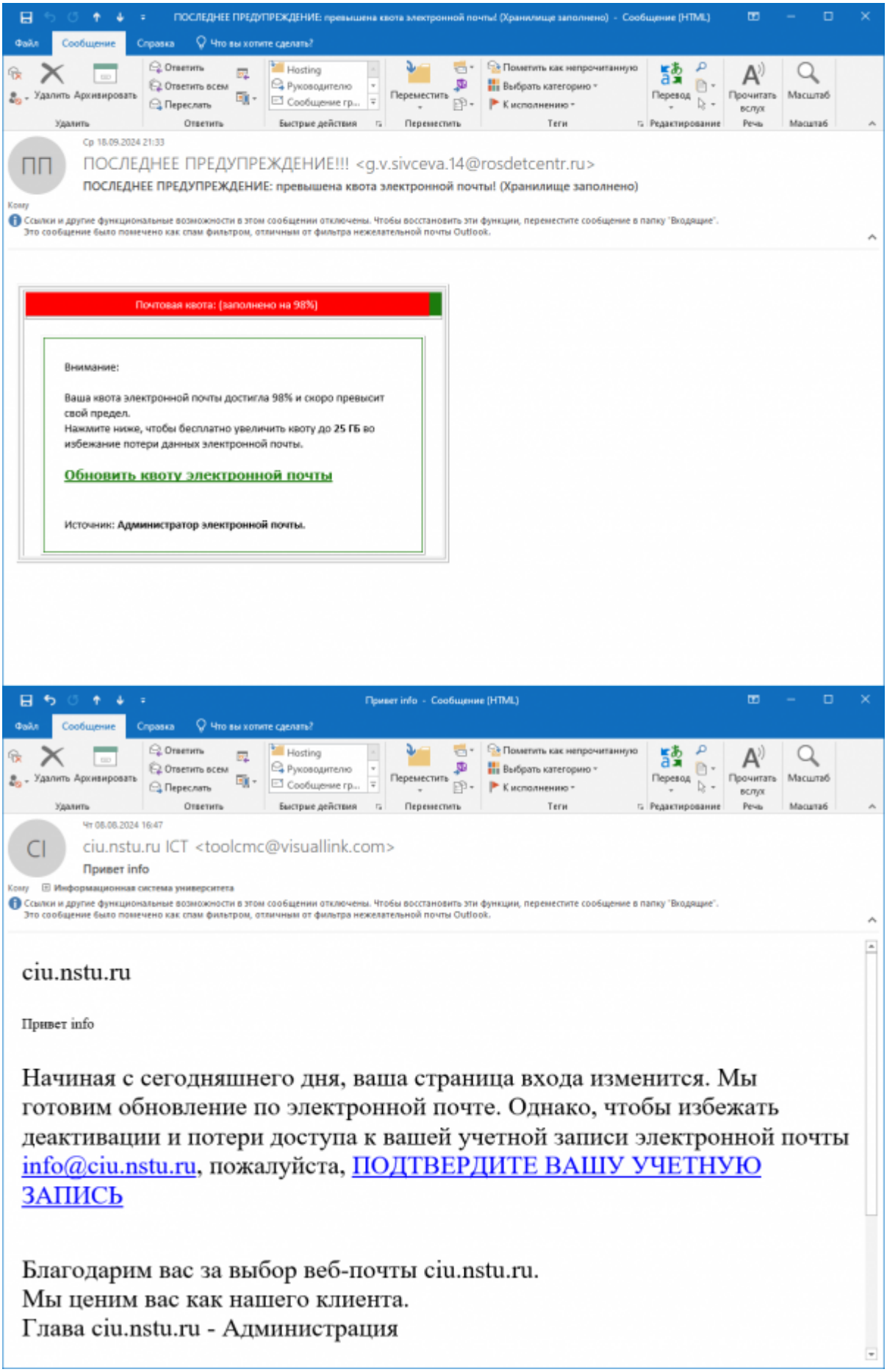
- **Реклама** – попытка продать товары или услуги. Иногда это может быть реальной рекламой, но чаще это мошенничество.



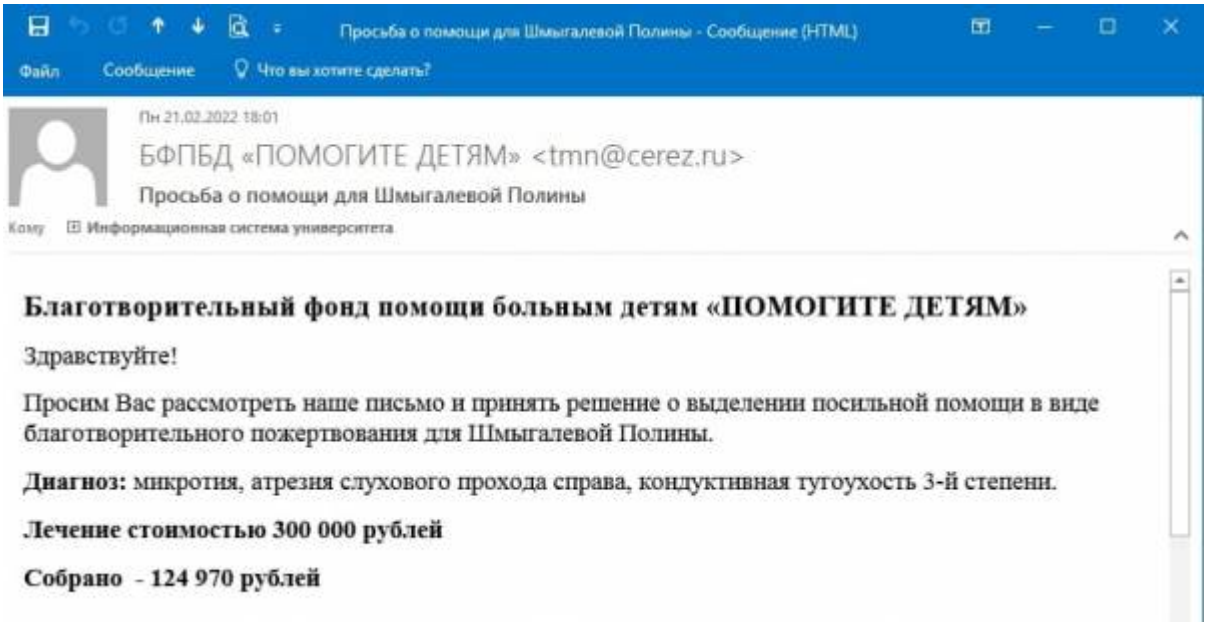
- **Поддельные электронные письма** якобы от легальных организаций, в которых используется фишинг, чтобы обманным путем получить личную или конфиденциальную информацию.


Последнее уведомление - Сообщение (HTML)
Файл
Сообщение
Справка
Что вы хотите сделать?
Удалить
Архивировать
Ответить
Ответить всем
Переслать
Hosting
Руководителю
Сообщение гр...
Переместить
Пометить как непрочитанную
Выбрать категорию
К исполнению
Перевод
Прочитать вслух
Масштаб
Удалить
Ответить
Быстрые действия
Переместить
Теги
Редактирование
Речь
Масштаб
ШЮ
Пн 24.03.2025 6:47
Шорников Юрий Владимирович
Последнее уведомление
Кому
Ссылки и другие функциональные возможности в этом сообщении отключены. Чтобы восстановить эти функции, перенестите сообщение в папку "Входящие".
Здравствуйте, сотрудники/сотрудники,
Ваш пароль к вашей учетной записи истекает 28/2/2025 5:09:16 вечера, и он имеет высокий приоритет.
Чтобы продолжить использовать тот же пароль, нажмите на ссылку ниже для подтверждения.
Сохраните тот же пароль
Ваша учетная запись будет временно заблокирована, если не будет подтверждена в течение 24 часов.
С уважением,
Центр поддержки клиентов ИТ.

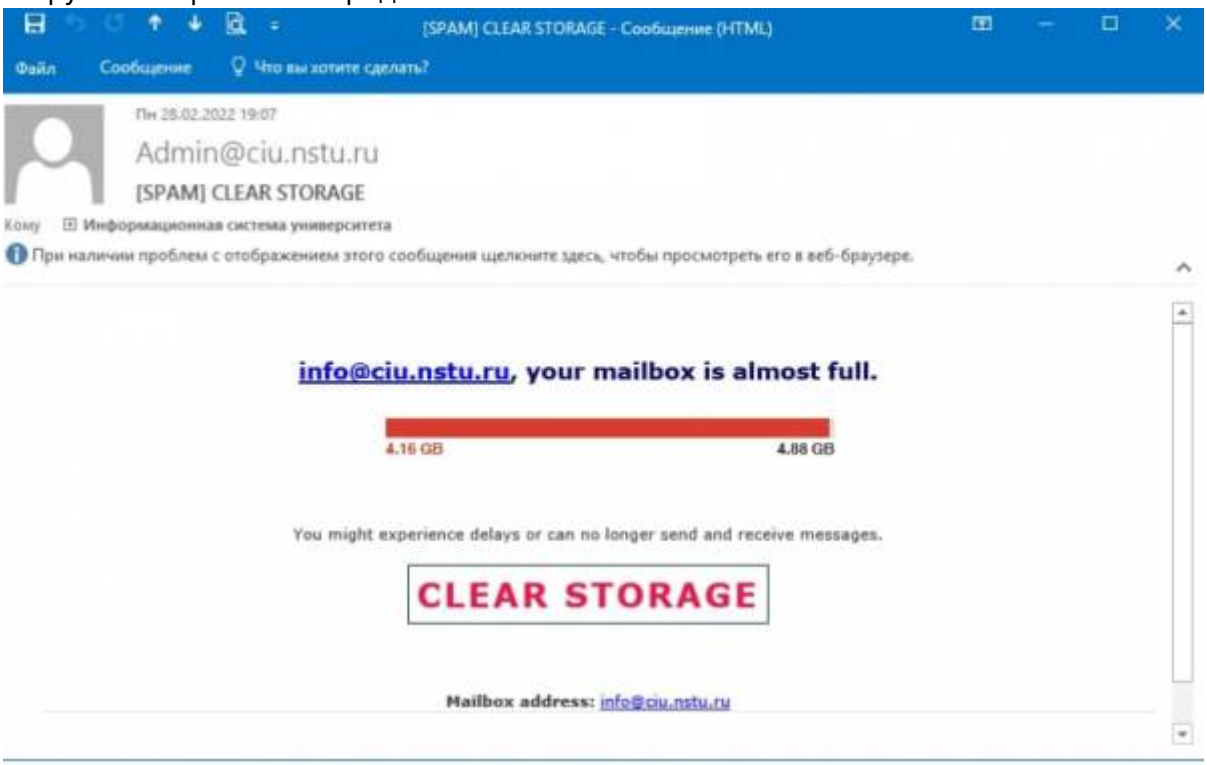

ПРЕДУПРЕЖДЕНИЕ / Активируйте свою учетную запись - Сообщение (HTML)
Файл
Сообщение
Справка
Что вы хотите сделать?
Удалить
Архивировать
Ответить
Ответить всем
Переслать
Hosting
Руководителю
Сообщение гр...
Переместить
Пометить как непрочитанную
Выбрать категорию
К исполнению
Перевод
Прочитать вслух
Масштаб
Удалить
Ответить
Быстрые действия
Переместить
Теги
Редактирование
Речь
Масштаб
ГН
Пт 21.03.2025 4:43
Гонина Наталья Владимировна
ПРЕДУПРЕЖДЕНИЕ / Активируйте свою учетную запись
Кому
Ссылки и другие функциональные возможности в этом сообщении отключены. Чтобы восстановить эти функции, перенестите сообщение в папку "Входящие".
При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.
!!! ПРЕДУПРЕЖДЕНИЕ !!!
Уважаемые пользователи corp.nstu.ru
Ваша учетная запись превысила лимит квоты, установленный администратором, и вы не сможете отправлять или получать новую почту до тех пор, пока не подтвердите свою учетную запись повторно.
Чтобы подтвердить свою учетную запись, пожалуйста
Нажмите здесь, чтобы проверить
Примечание: Невозможность проверки. Ваша учетная запись электронной почты будет отключена навсегда, если она не будет повторно проверена.
Приносим извинения за доставленные неудобства
Авторское право © 2025
helpdesk@corp.nstu.ru
Безопасная почта: Это письмо было проверено на наличие вирусов антивирусным программным обеспечением Avast



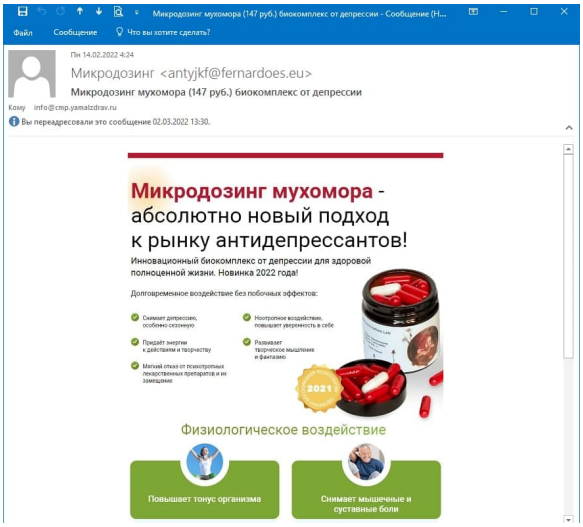
- **Денежное мошенничество**: от пресловутых «нигерийских принцев» до более изощренных попыток мошенничества, таких как поддельные призывы к благотворительности.

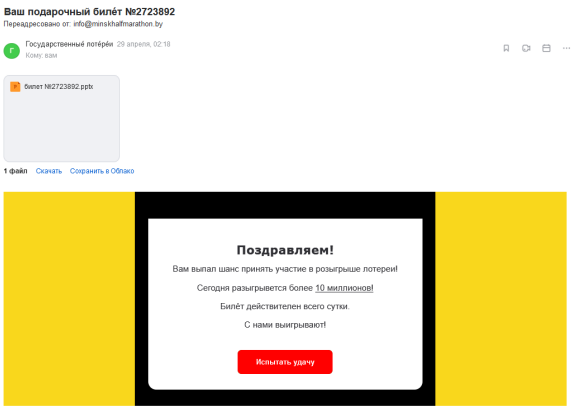


- **Предупреждения о вредоносном ПО**, сообщающие, что на устройствах обнаружены вредоносные программы, например вымогатели или вирусы. Часто эти сообщения предлагают открыть вложение или перейти по ссылке, в результате чего на устройство загружается реальное вредоносное ПО.



- **Принудительные или случайные подписки**: при покупках в интернете или подписках на новые приложения, можно непреднамеренно подписаться на информационные рассылки. Некоторые компании действуют непрозрачно, в результате чего подписка на их рассылки происходит незаметно.
- **Нереалистичные обещания**, такие как схемы быстрого обогащения, чудодейственные диеты, невероятные скидки и предложения, выигрыши в розыгрышах и лотереях и прочие.

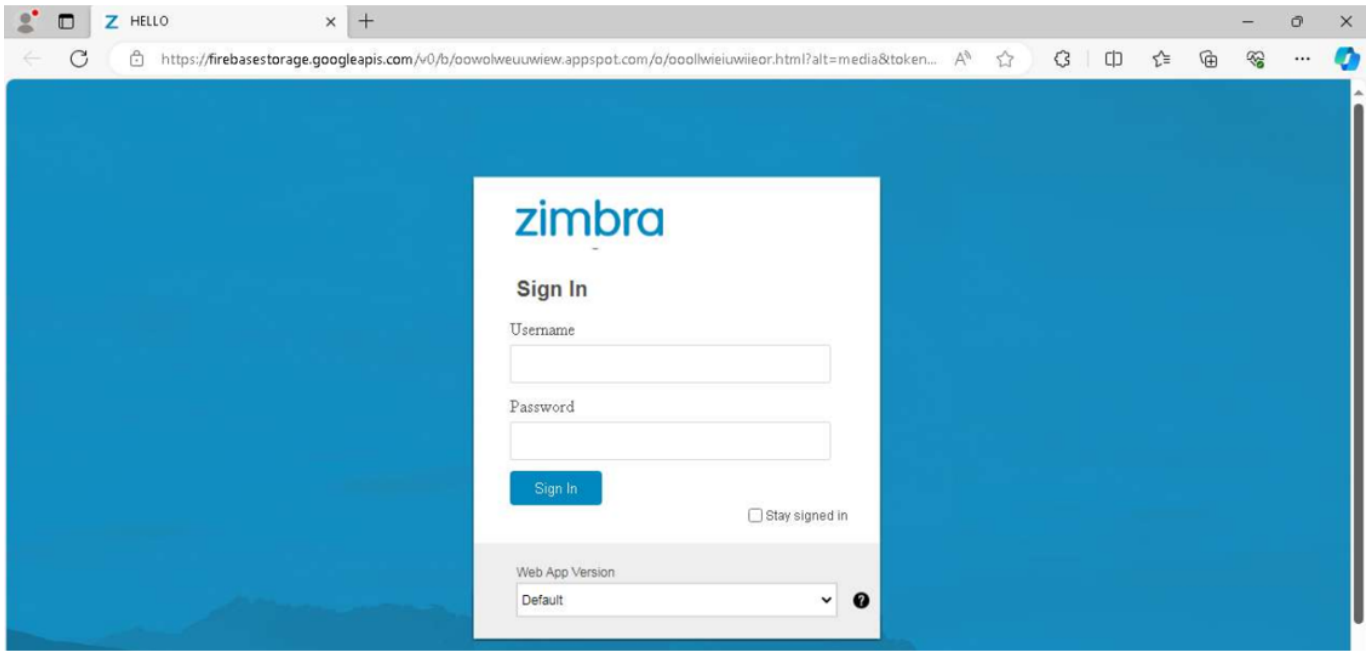


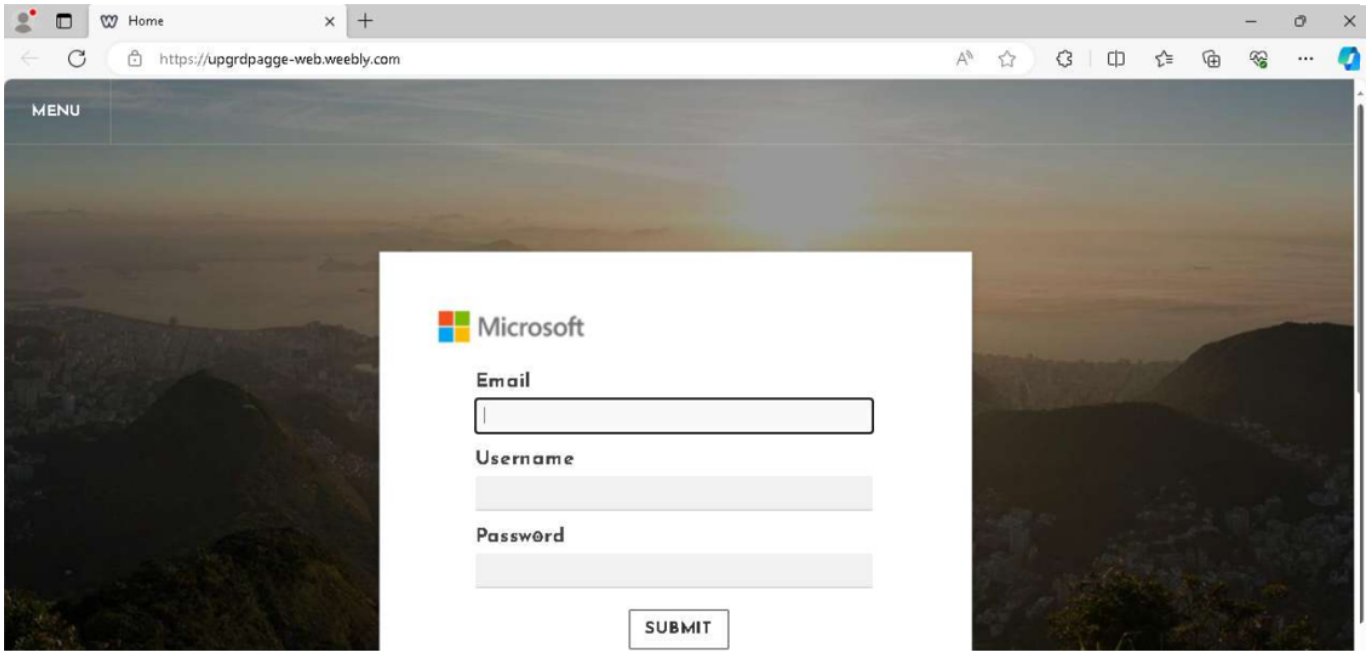


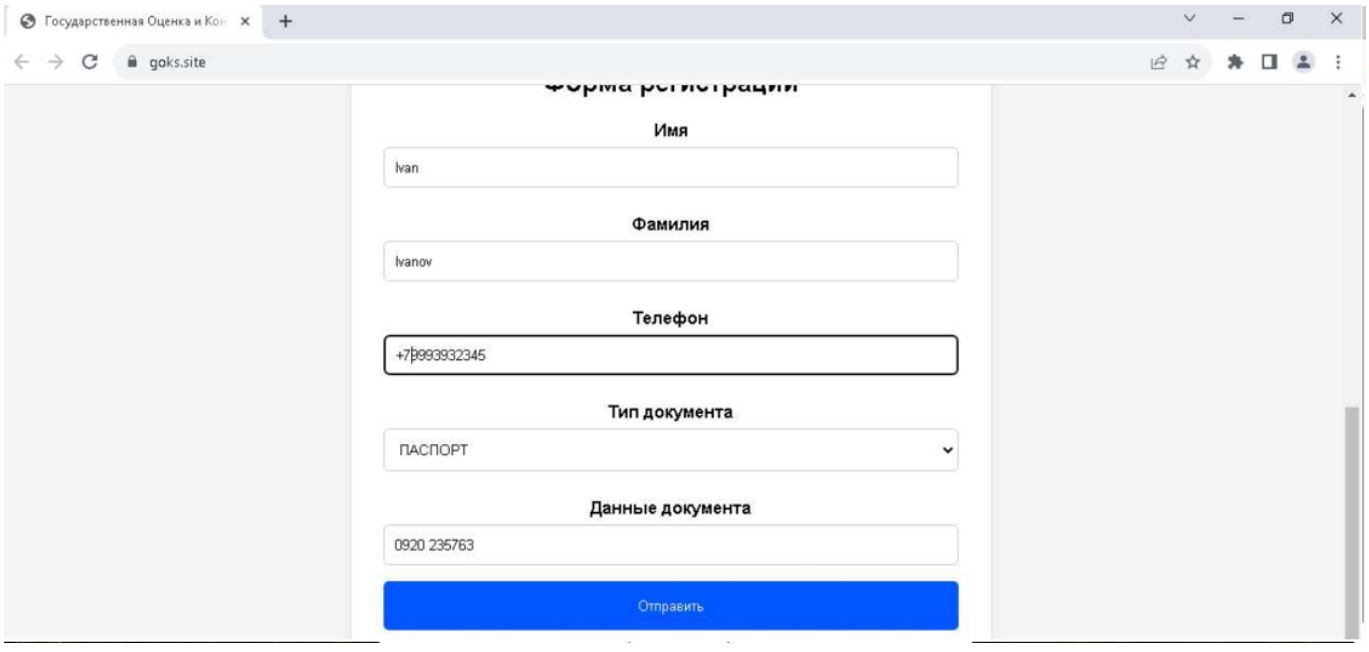
- **Письма счастья** – письма, которые обязательно нужно переслать, иначе «с вами случится что-то плохое».

Примеры поддельных сайтов

Ниже вы можете ознакомится с тем как может выглядеть поддельный сайт из фишингова письма.


HELLO
https://firebasestorage.googleapis.com/v0/b/oowolweuuwiew.appspot.com/o/ooollwieiuwiieor.html?alt=media&token...
zimbra
Sign In
Username
Password
Sign In
Stay signed in
Web App Version
Default


Home
https://upgrdpagge-web.weebly.com
MENU
Microsoft
Email
Username
Password
SUBMIT


Государственная Оценка и Ко
goks.site
Имя
Ivan
Фамилия
Ivanov
Телефон
+79993932345
Тип документа
ПАСПОРТ
Данные документа
0920 235763
Отправить

From:
https://kb.nstu.ru/ - **База знаний НГТУ НЭТИ**

Permanent link:
https://kb.nstu.ru/it:mail:spam

Last update: **2025/03/25 10:56**