ООО «СтройТелеком»
ГУПС, а/я 240, г. Новый Уренгой, ЯНАО, 629300
Тел.: 8 800 222 5664 E-mail: info@usbc.ru
ОКПО 27004061 ОГРН 1138904001939
ИНН/КПП 8904072500/890401001

Клиентам
(по списку)

Рекомендовано к ознакомлению
всего персонала

09.12.2019 № 156

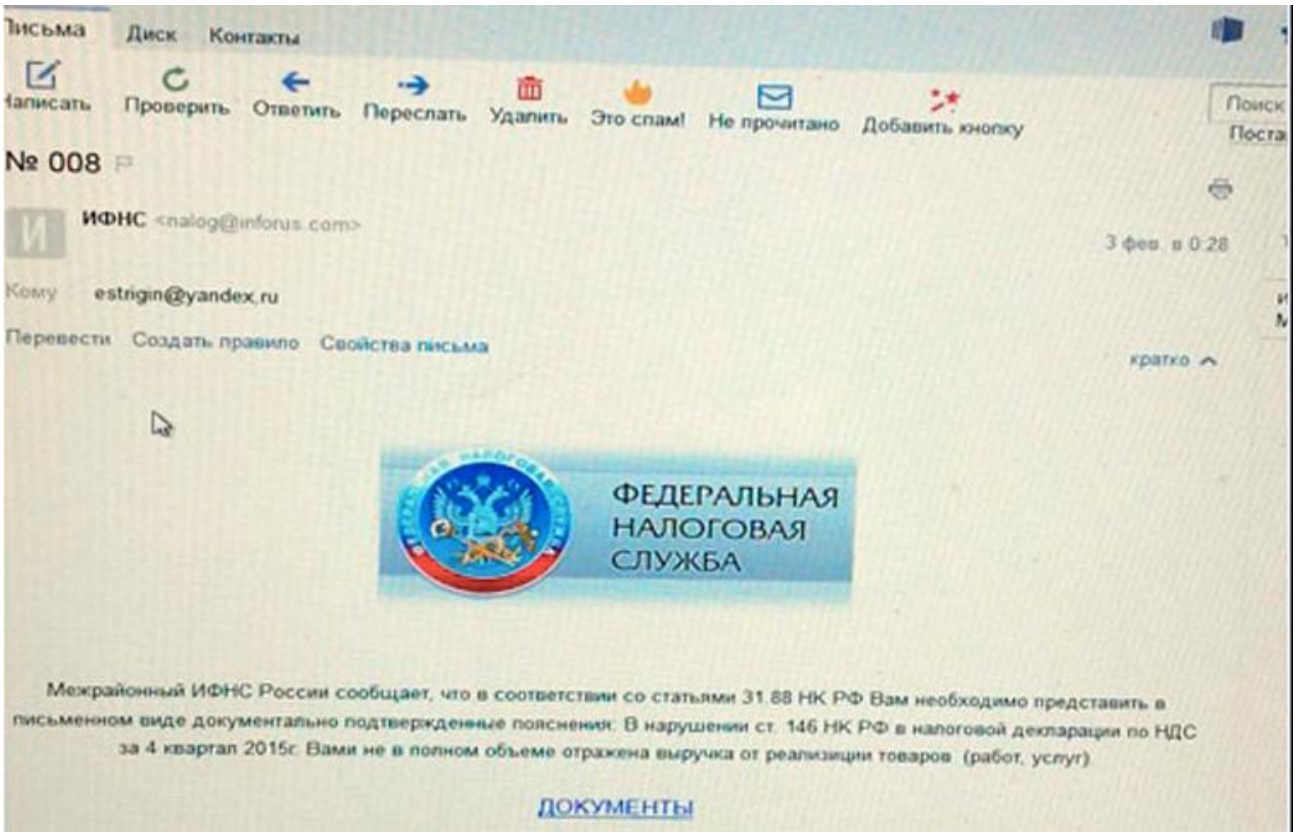
Об обеспечении информационной безопасности

Уважаемые клиенты!

Информируем Вас о том, что в последнее время участились случаи мошенничества с помощью массовой рассылки писем, содержащих вредоносный код. По разным данным, от 50 до 95% всех электронных писем в мире — спам от кибермошенников. Цели рассылки таких писем просты: заразить компьютер получателя вирусом, украсть пароли пользователя, заставить человека перевести деньги «на благотворительность», ввести данные своей банковской карты или прислать сканы документов.

Мы собрали из разных источников наиболее распространенные схемы мошенничества:

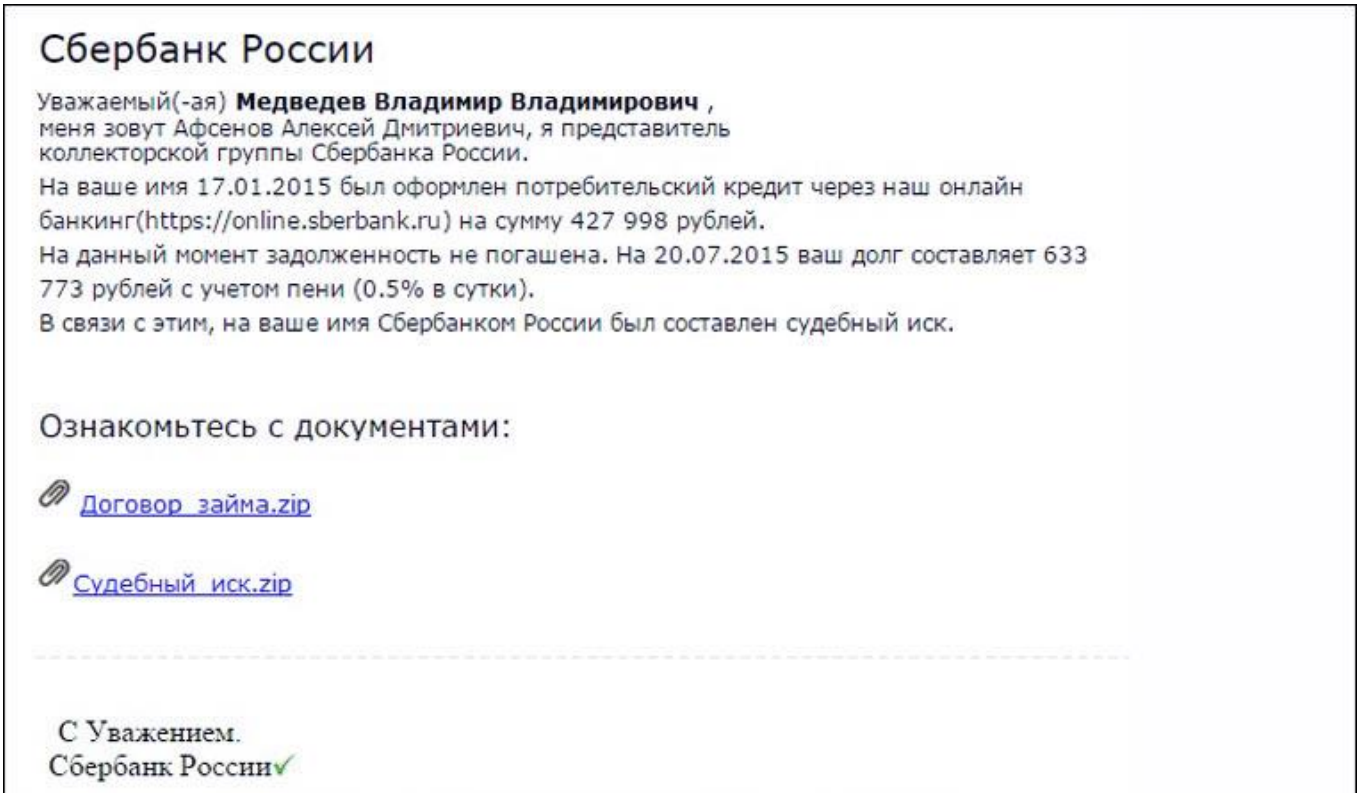
1. **Письма от «государственных организаций»**



Мошенники могут представляться Налоговой, Пенсионным фондом, Роспотребнадзором, санэпидемстанцией и другими госорганизациями. Для убедительности в письмо вставляют водяные знаки, сканы печатей и государственную символику. Чаще всего, задача преступников — напугать человека и убедить его открыть файл с вирусом во вложении.

Обычно это шифровальщик или блокатор Windows, который выводит компьютер из строя и требует прислать платное SMS для возобновления работы. Вредоносный файл может маскироваться под судебное постановление или повестку о вызове к начальнику организации.

2. Письма от «банков»



Сбербанк России

Уважаемый(-ая) **Медведев Владимир Владимирович** ,
меня зовут Афсенов Алексей Дмитриевич, я представитель
коллекторской группы Сбербанка России.
На ваше имя 17.01.2015 был оформлен потребительский кредит через наш онлайн
банкинг(https://online.sberbank.ru) на сумму 427 998 рублей.
На данный момент задолженность не погашена. На 20.07.2015 ваш долг составляет 633
773 рублей с учетом пени (0.5% в сутки).
В связи с этим, на ваше имя Сбербанком России был составлен судебный иск.

Ознакомьтесь с документами:

Договор_займа.zip

Судебный_иск.zip

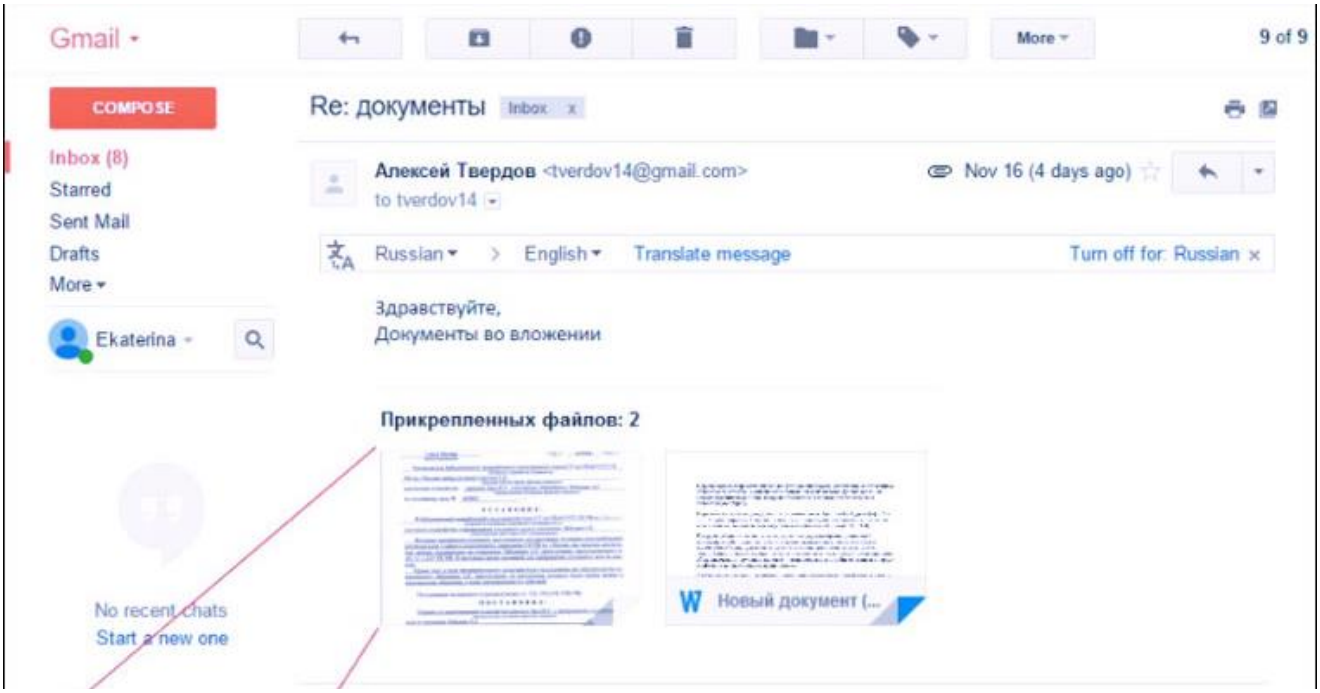
С Уважением.
Сбербанк России

Блокаторы Windows и шифровальщики могут прятаться в фальшивых письмах не только от госорганизаций, но и от банков. Сообщения «На Ваше имя взяли кредит, ознакомьтесь с судебным иском» действительно могут напугать и вызвать огромное желание открыть файл.

Также человека могут убедить войти в фальшивый личный кабинет, предлагая посмотреть начисленные бонусы или получить приз, который он выиграл в «Лотерее Сбербанка».

Реже мошенники отправляют счета для оплаты сервисных сборов и дополнительных процентов по кредиту, на 50-200 рублей, которые проще заплатить, чем разбираться.

3. Письма от «коллег» / «партнеров»



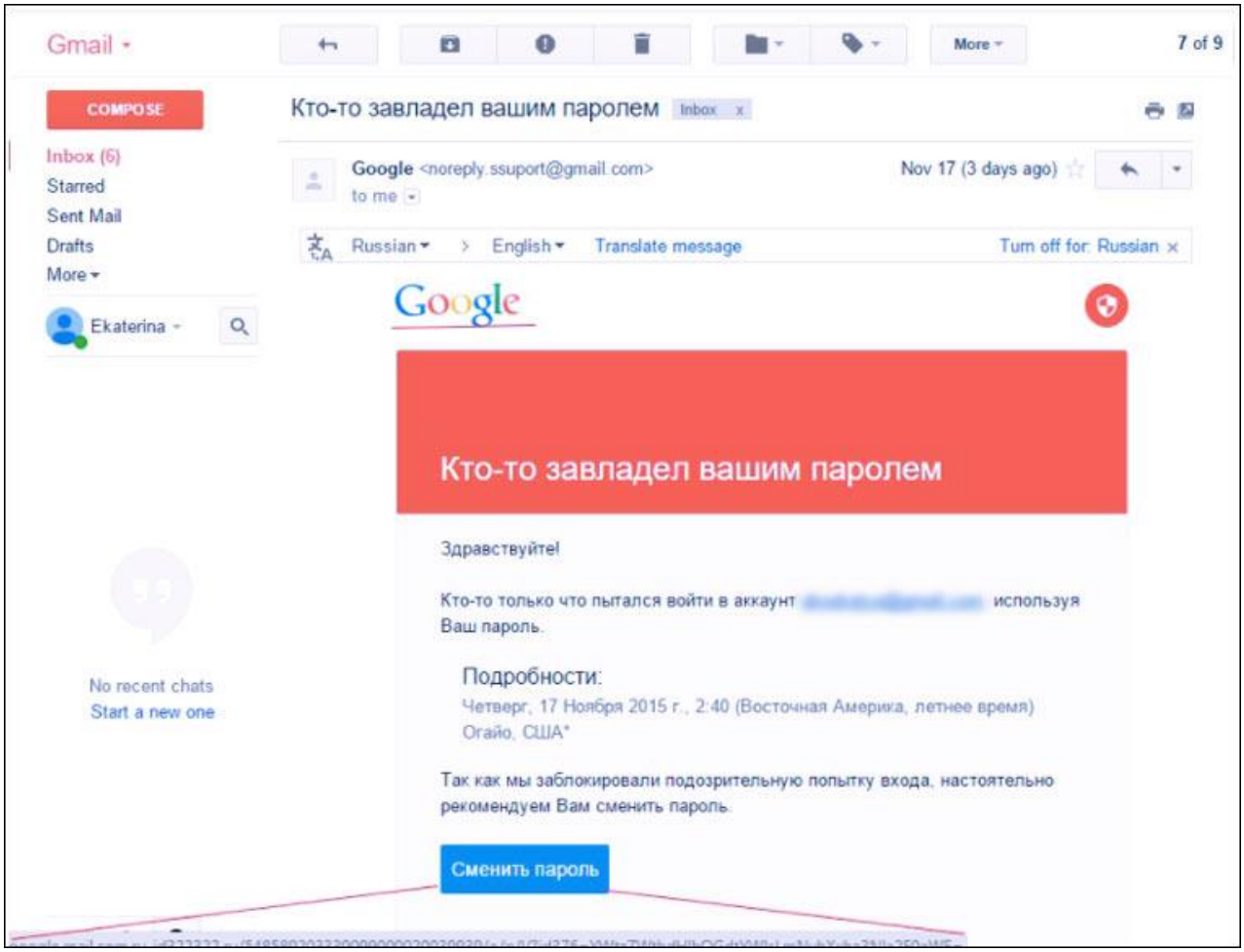
Некоторые люди получают десятки деловых писем с документами в течении рабочего дня. С такой нагрузкой можно легко повестись на метку «Re:» в теме письма и забыть про то, что с этим человеком вы пока не переписывались.

Особенно, если в поле отравитель указано «Александр Иванов», «Екатерина Смирнова» или любое простое русское имя, которые абсолютно не задерживаются в памяти человека, постоянного работающего с людьми.

Если целью мошенников является не сбор SMS-платежей за разблокировку операционки, а принесение вреда конкретной компании, то письма с вирусами и фишинговыми ссылками могут рассылать от имени реальных работников. Список сотрудников можно собрать в соцсетях или посмотреть на сайте компании.

Если человек видит в ящике письмо от человека из соседнего отдела, то он к нему особо не присматривается, может даже проигнорировать предупреждения антивируса и открыть файл несмотря ни на что.

4. Письма от «Google/Яндекс/Mail»



Google иногда присылает письма владельцам ящиков Gmail о том, что кто-то пытался зайти в их аккаунт или о том, что закончилось место на Google Drive. Мошенники успешно копируют их и заставляют пользователей вводить пароли на подставных сайтах.

Фальшивые письма от «администрации сервиса» также получают пользователи Яндекс.Почты, Mail.ru и прочих почтовых служб. Стандартные легенды такие: «ваш адрес добавлен в черный список», «срок действия пароля истек», «все письма с вашего адреса будут добавляться в папку спам», «посмотрите список недоставленных писем». Как и в трех предыдущих пунктах, основными оружиями преступников являются страх и любопытство пользователей.

Как защититься от подобных попыток взлома?

1. Внимательно читать входящую корреспонденцию и при малейшем подозрении на спам – удалять письмо в корзину.
2. Пользоваться антивирусом с актуальной лицензией и базами обновлений сигнатур.
3. Проверять все подключаемые носители (флеш, внешние HDD диски) на наличие вирусов.

4. Использовать только лицензионное программное обеспечение: от операционной системы Windows до любых пакетных приложений (Word, Excel, WinRar т.п.).
5. Организовать внутреннюю политику безопасности информационной сети таким образом, чтобы максимально исключить случайное открытие расширений файлов *.js *.bat и т.д.
6. Обращаться к квалифицированным специалистам в области информационных технологий.

Благодарим за уделенное время и надеемся, что предоставленная информация оказалась для Вас полезной. По любым вопросам, связанным с IT-структурой Вашего учреждения, Вы можете обращаться по бесплатному номеру: 8 800 222 56 64

С Уважением,
Коллектив СтройТелеком г. Новый Уренгой