ФИШИНГ ПИСЬМО.
КАК РАСПОЗНАТЬ? ЧТО ДЕЛАТЬ?

Фишинг (англ. phishing) *— вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.*

КАК РАСПОЗНАТЬ?

1. Вы не ждали этого письма.

Конечно, следует обращать внимание на отправителя и получателя письма.

Но злоумышленники научились имитировать письма от известных организаций, и адрес отправителя, и содержания письма может выглядеть очень достоверно.

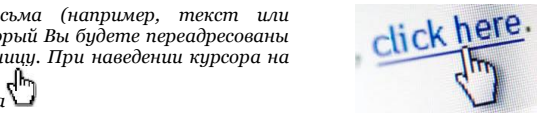
Письмо может быть передано и от знакомого вам человека, если его ПК заражен вредоносным ПО или он по неосторожности переадресовал письмо Вам.

2. В письме Вас просят срочно совершить действие: перейти по ссылке, открыть вложение и т.д.

Получив письмо, в котором сообщается о блокировке важного аккаунта (например, интернет-банка), о наличии задолженности или штрафа, важном сообщении от организации, люди стремятся поскорее выполнить указание в письме, не задумываясь о потенциальной опасности.

3. В письме имеется ссылка для скачивания файлов.

Ссылка *– элемент письма (например, текст или картинка), нажав на который Вы будете переадресованы на некую интернет страницу. При наведении курсора на ссылку он меняет форму на*



Перейдя по ссылке в письме Вы можете загрузить вредоносное ПО!

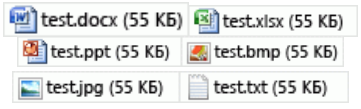
Наведите курсор мышки на ссылку (не нажимая на нее, ссылка появится или рядом с курсором или в левой нижней части окна) и посмотрите на название сайта, который Вам предлагают посетить. В новой вкладке браузера в ручную вбейте полученную ссылку (не копируя ее). Такой метод позволит заметить ошибки в ссылке.

4. Обратите внимание на вложение к письму.

В архиве, прикрепленном к письму, может содержаться вредоносное ПО.

Очень часто злоумышленники архивируют вредоносное ПО. В таком виде его сложнее обнаружить системам защиты. Также в архиве помимо видимых, на первый взгляд безвредных файлов, могут быть скрытые файлы, которые активируют вредоносное ПО.

Важно проверить, что в почтовом клиенте у вас отображается расширение файлов!



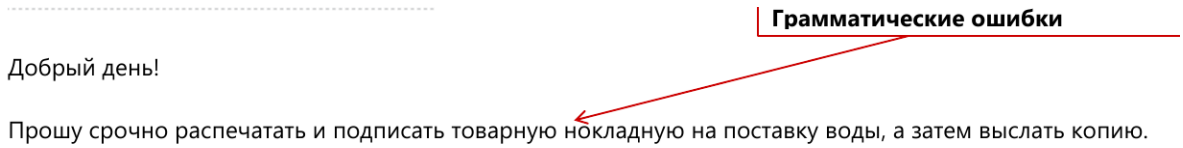
Расширение файла *– формат файла, группа букв после последней точки.*
Слева приведены наиболее распространенные форматы файлов.
Обратите внимание на иконки и расширения!

Нельзя открывать файлы следующих расширений: **.app, .exe, .bat, .js, .scr**!
Также остерегайтесь файлов с двойным расширением (например, **Регламент.docx.js**)!

На практике встречаются случаи получения по электронной почте обычного «вордовского», «экселевского» файла, внутри которого, помимо текста, есть изображение, гиперссылка (на неизвестный сайт в Интернете), встроенный OLE-объект (объекты, созданные в других программах – чертежи, рисунки, схемы). При нажатии на такой объект может произойти заражение.
Также такие файлы могут содержать программный код (макросы). При запуске файлов с макросами система их блокирует. Для активации макроса необходимо нажать «Включить содержимое». Запускайте содержимое только в проверенных файлах.

5. Обратите внимание на опечатки.

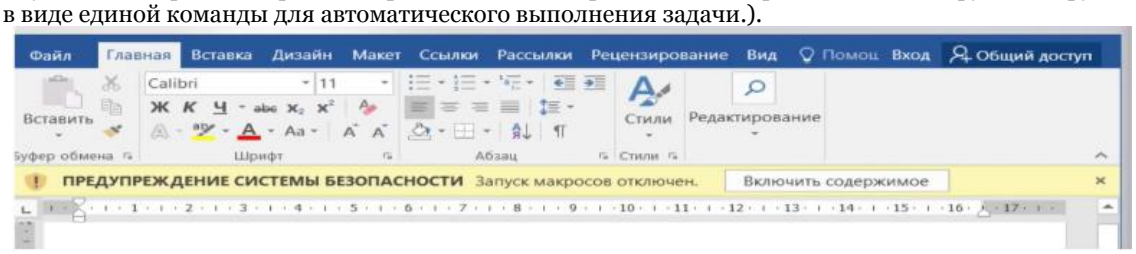
Обращайте внимание на возможные опечатки, орфографические ошибки, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого в тексте электронного письма.



ЧТО ДЕЛАТЬ?

1. Если Вы получили письмо, в котором от Вас требуют какого-либо взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у Вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:
- ожидаю ли я это письмо?
- есть ли смысл в том, что от меня требуют?
- знаю ли я автора этого письма?
- уверен ли я в безопасности полученного электронного письма?

Если ответ хотя бы на один из озвученных выше вопросов «**нет**» -внимательно проанализируйте содержимое письма и, при необходимости, свяжитесь для консультации со своим администратором безопасности или сотрудником технической поддержки.
2. Не нажимайте на ссылки, если они заменены на слова.
3. Не копируйте адрес ссылки.
4. 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.
5. Не подгружайте картинки от незнакомых людей.
6. Не запускайте макросы в офисных приложениях (макрос – это набор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи.).



7. Не пересылайте письма коллегам.
8.В случае наличия признаков потенциально-опасного письма откройте письмо и перешлите его с пометкой «Прошу проверить приложенное письмо на наличие вредоносной активности» на адрес servicedesk@tularegion.ru (omnitracker).