ЧТО ДЕЛАТЬ, ЕСЛИ ОБНАРУЖИЛ ФИШИНГ?

НЕ переходить по ссылке

НЕ копировать её адрес

НЕ скачивать документы из письма

НЕ открывать их

НЕ пересылать письма коллегам

НЕ использовать телефон для перехода по ссылке

НЕ подгружать картинки от незнакомых людей

Если вы сомневаетесь, письмо от мошенника или нет, ***свяжитесь с собеседником по другому виду связи! И не забудьте поменять пароль***

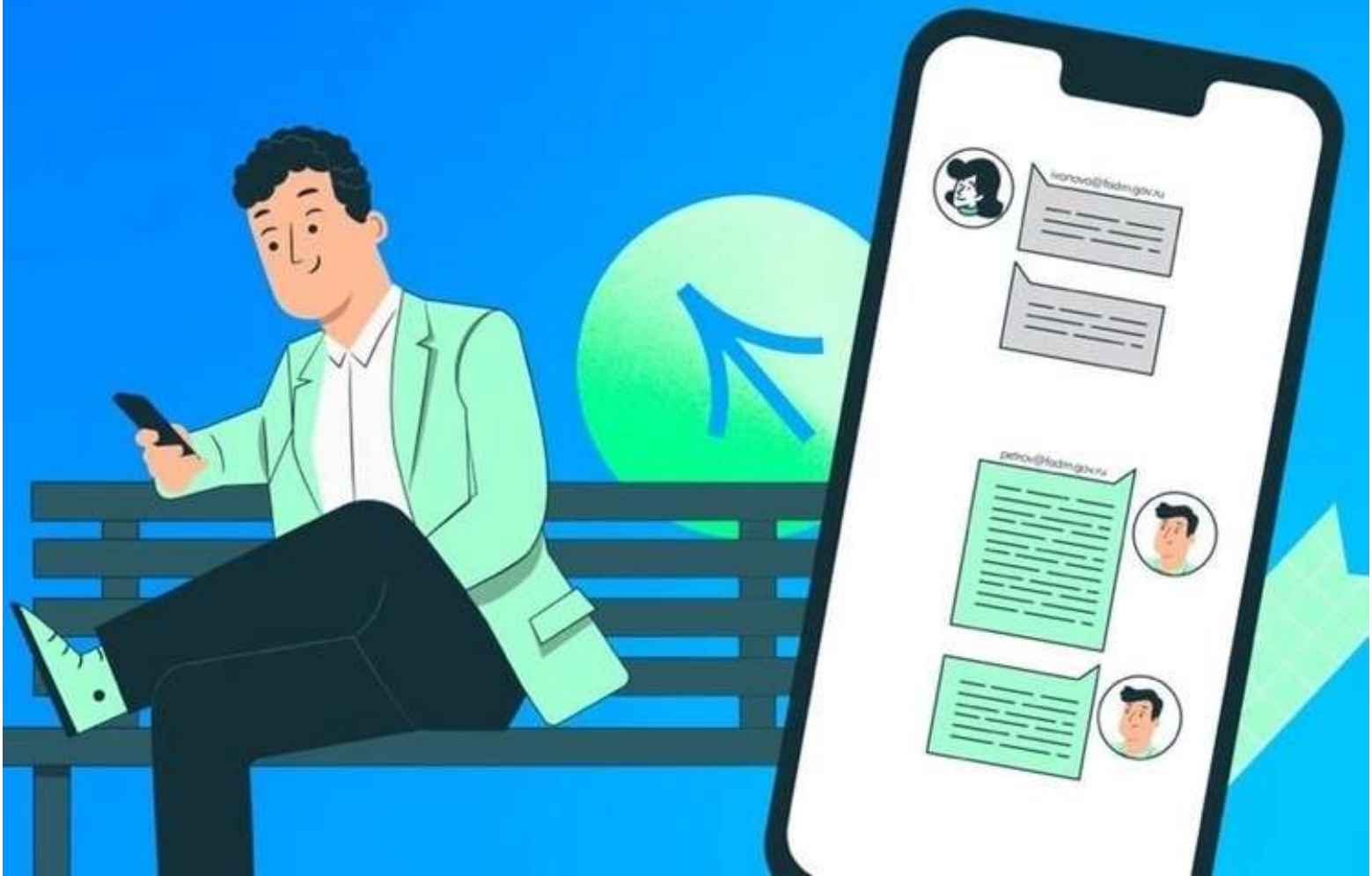
КАК АНАЛИЗИРОВАТЬ ПИСЬМО: АДРЕС ОТПРАВИТЕЛЯ

Имя должно быть корректным и совпадать с оригинальным

ПРИМЕР:

ivanova@fadm.gov.ru — ***корректный***

ivanova@fadm.gov.su — ***ложный***



КАК АНАЛИЗИРОВАТЬ ПИСЬМО: ССЫЛКИ

- посмотреть, знаком ли сайт
- проверить имя сайта: не подменены ли буквы, корректный ли домен (.ru, .com, .рф), нет ли «лишних» знаков вроде «точки» или «тире»

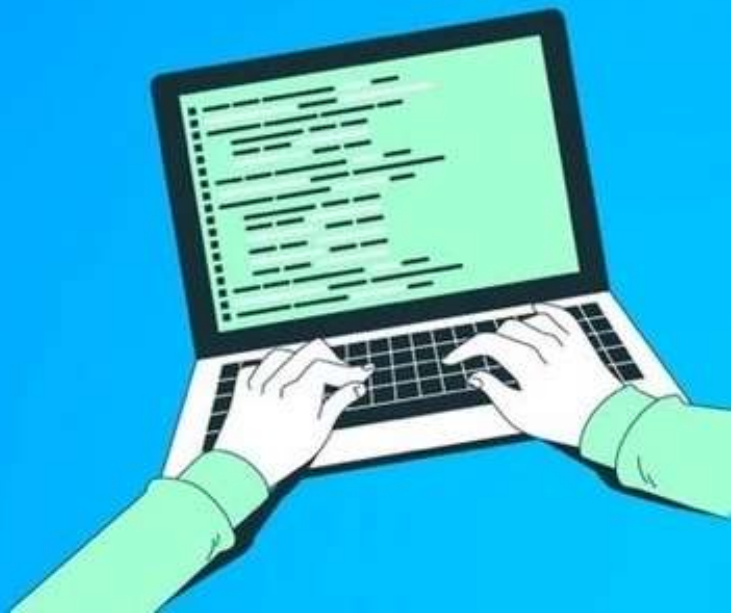
ПРИМЕР:

https://myrosmol.ru/ — ***корректный***
https://myrasmoll.ru/ — ***ложный***
(о заменено на а, есть вторая l)

обратить внимание на наличие коротких гиперссылок

ПРИМЕР:

https:/bit.ly/2sAHAOv
https:/cut.ly/wrwtLNH

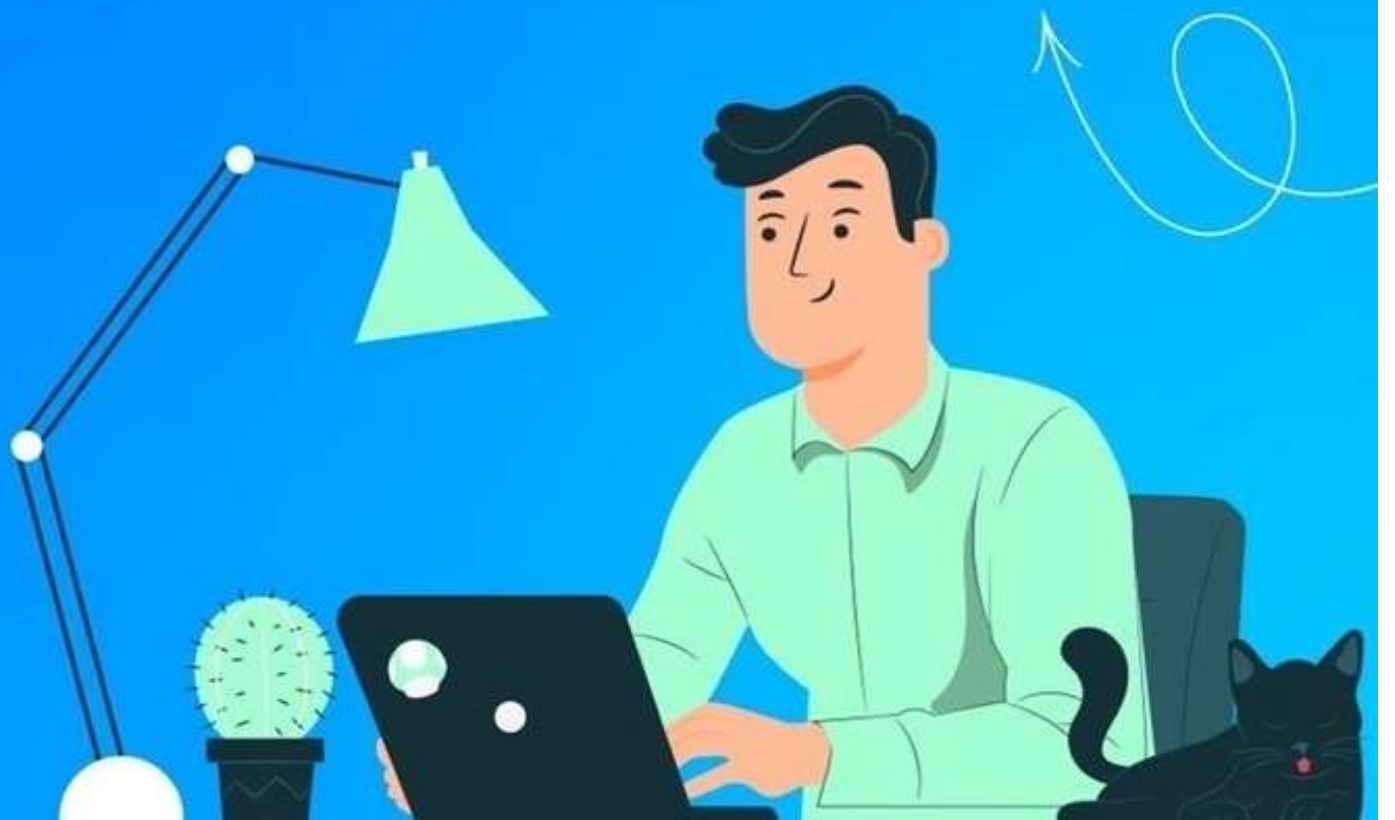


КАК АНАЛИЗИРОВАТЬ ПИСЬМО: ВЛОЖЕННЫЕ ФАЙЛЫ

Обратите внимание на расширение:

- какая программа может открыть данный документ?
- ждёте ли вы подобный файл в контексте беседы с данным человеком?
- посмотрите на сообщения от программ, которые могут сигнализировать об опасности

! ***Не запускайте файлы с незнакомыми вам расширениями!***

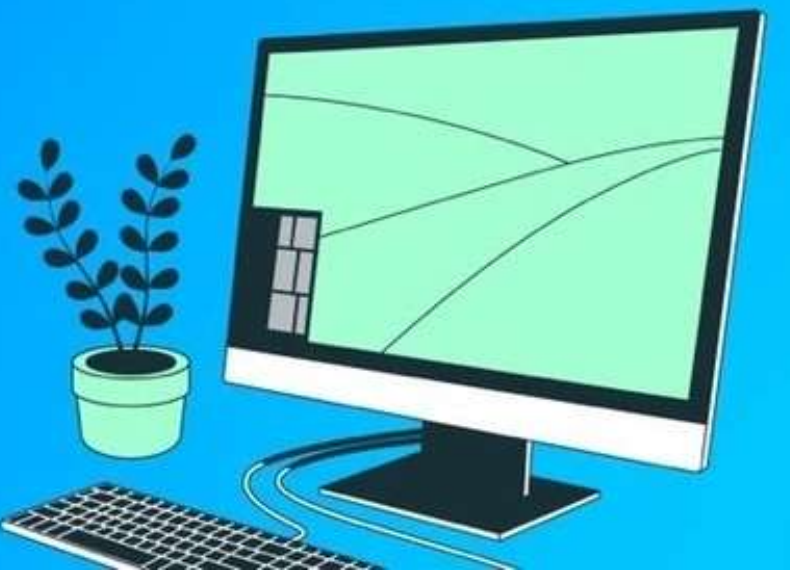


ЧТО ТАКОЕ ФИШИНГ И КАК С НИМ БОРОТЬСЯ?

Фишинг — вид интернет-мошенничества, его цель — получить ваши данные (логин-пароль), конфиденциальную информацию или запустить вредоносное ПО

Если вы получили письмо, которое требует от вас какого-либо взаимодействия и призывает действовать срочно, то задайте себе вопросы:

- Ожидаю ли я это письмо?
- Есть ли смысл в том, что от меня требуют?
- Знаю ли я автора этого письма?
- Если я отвечу, то какие могут быть последствия?



КАК РАСПОЗНАТЬ МОШЕННИКА

В ПОЧТОВЫХ СООБЩЕНИЯХ?

ДИАЛОГ ЦИФРОВЫЕ КОММУНИКАЦИИ × росмолодёжь