ПАМЯТКА
по безопасному использованию электронного почтового сервиса ДВГУПС

ОБЩИЕ РЕКОМЕНДАЦИИ

Электронная почта по своему существу небезопасна. Написать письмо Вам может абсолютно любой пользователь/организация и этим не могли не воспользоваться злоумышленники.

Чтобы не попасться на уловки мошенников соблюдайте следующие рекомендации:

- Проверяйте адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- не открывайте письма от неизвестных адресатов;
- проверяйте письма, в которых содержаться призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- не переходите по ссылкам, которые содержаться в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.);
- не нажимайте на ссылки из письма, если они заменены на слова, не наводите на них мышкой и внимательно проверяйте полный адрес сайтов;
- проверяйте ссылки, даже если письмо получено от другого пользователя информационной системы;
- не открывайте вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD.

Иногда сложно понять, какое письмо от действительного адресата, а какое поддельное. Мошеннические письма обычно рассылаются по огромному списку адресов, попасть в которые может каждый. К счастью, есть общие признаки, которые типичны для них и которые должны насторожить Вас:

- Приложенные документы и ссылки в тексте письма;
- Ошибки, опечатки, проблемы с грамматикой (их допускают намеренно для обмана спам-фильтров);
- Письмо на иностранном языке, адресованное многим получателям;
- Непрофессиональная графика;
- Просьбы срочно подтвердить ваш адрес или другие личные данные;

- Просьба в той или иной форме раскрыть ваши учетные данные, пароль;
- Универсальные, неличные обращение, такие как «Дорогой клиент»;
- Обезличенные поля «От» и «Кому» могут быть признаком фишинга;
- Большинство писем от легитимных компаний не приходит с почты @gmail.com, @live.com и т. д. Обычно официальные письма приходят с официальных доменов;

Но, помимо массовых рассылок подобных писем, возможен другой сценарий, и злоумышленник будет использовать индивидуальный подход именно к Вам. Так как данные о сотрудниках университета размещены на сайте в открытом доступе, то вы можете получить похожее на официальное письмо, без опечаток и с довольно убедительным текстом. Тут Вас должно насторожить то, что официальные обращения должны быть в печатном виде, либо в виде скана, со всеми обязательными подписями/печатями. И, обычно, официальные документы вы ожидаете получить и заранее это обговариваете, либо с Вами связываются сразу по факту их получения. Либо рассылка официальных документов, распоряжений, приказов происходит через корпоративную систему электронного документооборота **Directum**.

Если Вы сомневаетесь в надёжности полученного письма, перешлите его по адресу: **proverka@festu.khv.ru**

РАЗБОР РЕАЛЬНОГО СЛУЧАЯ ФИШИНГА
(в программе Microsoft Outlook 2013)

Ниже приведён пример фишингового письма. В нём мы видим корректный адрес отправителя, обращение по имени и отчеству, отсутствие опечаток, указание что-либо сделать, однако не подкреплённое документально и никак не обговоренное отдельно. Это тоже может быть фишинговым письмом, но как это проверить?

Самое очевидное - связаться с отправителем и уточнить по поводу отправки им этого письма. Но это не всегда возможно и не всегда удобно. Второй способ - посмотреть в свойствах письма через какие сервера оно было переслано.

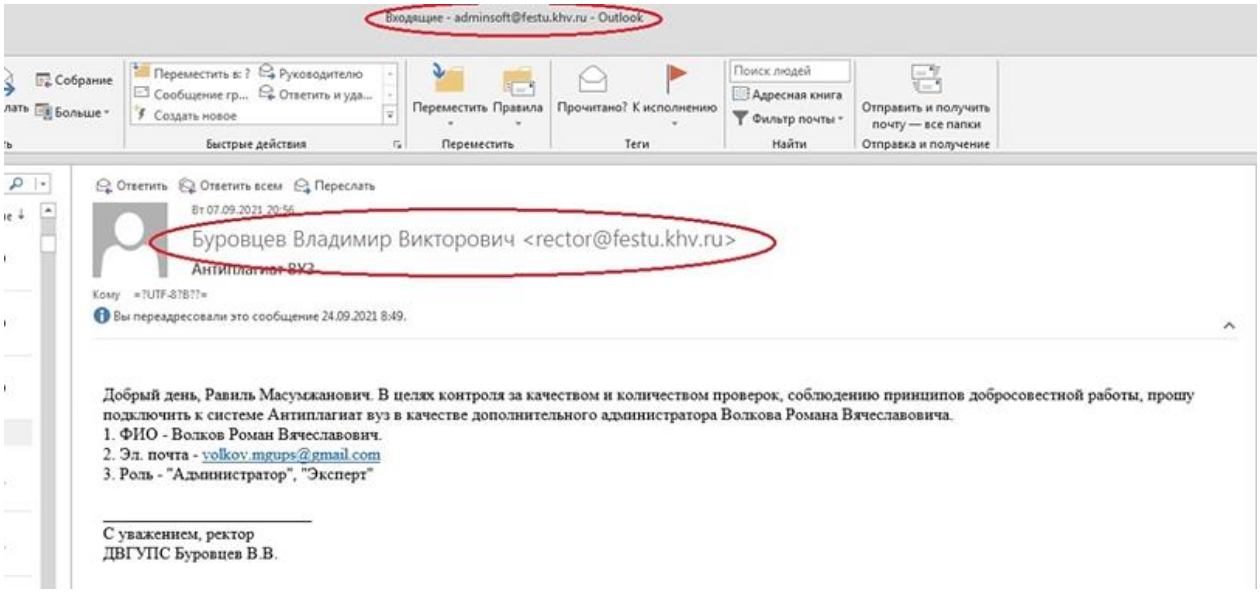

рис. 1 – фишинговое письмо

На первый взгляд письмо, присланное от имени ректора ДВГУПС выглядит максимально убедительным, но при детальном рассмотрении увидим, что письмо пришло из внешней почты, не принадлежащей домену ДВГУПС.

Для того чтобы узнать откуда пришло письмо, необходимо открыть входящее письмо нажав двойным щелчком левой кнопкой мыши.

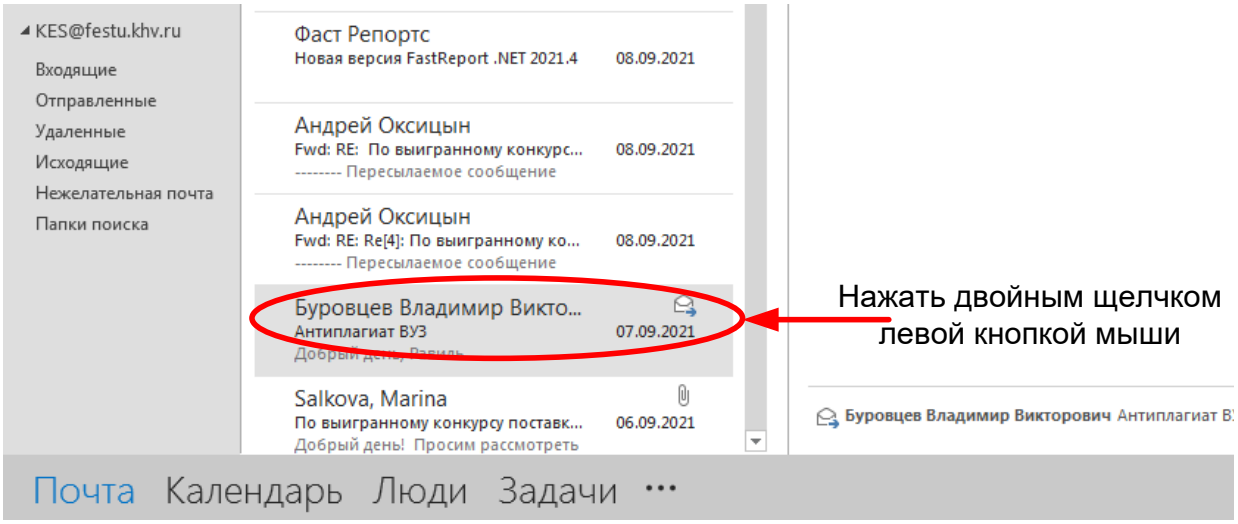

рис. 2 – открытие проверяемого письма

В открывшемся окне нажать на меню «ФАЙЛ».

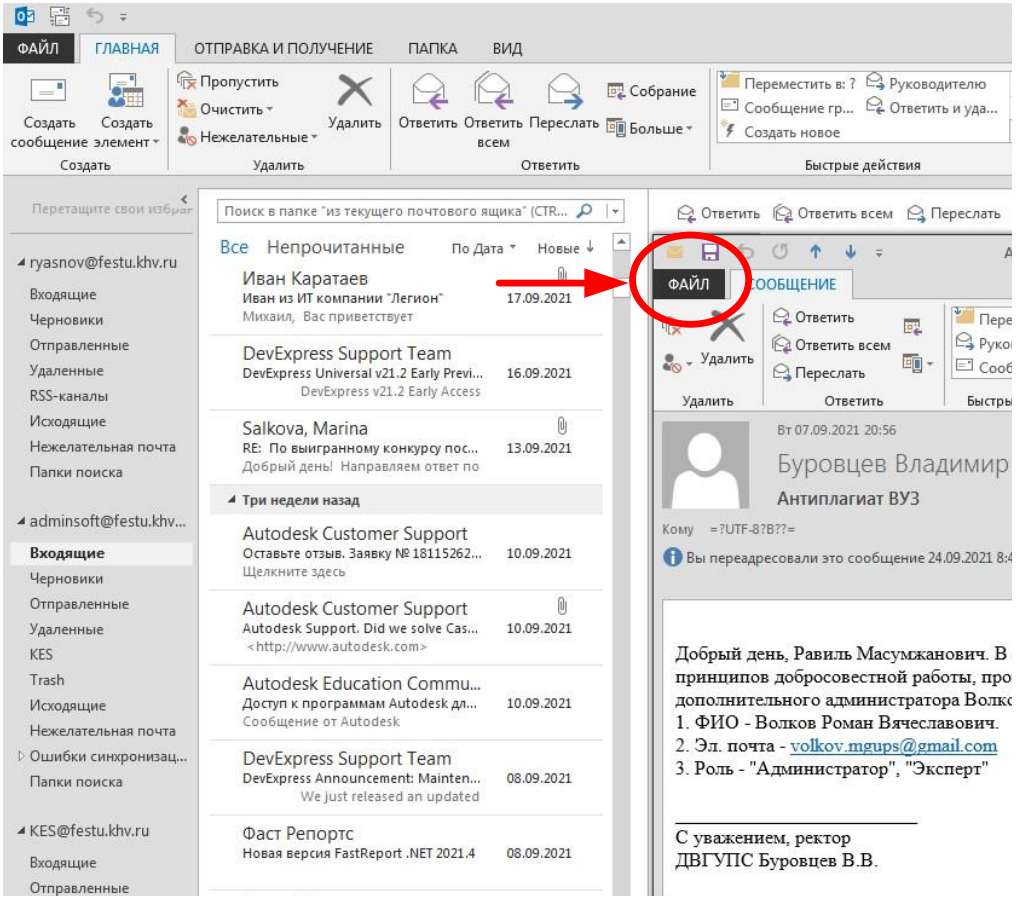

рис. 3 – кнопка вызова меню «ФАЙЛ» письма

Далее в открывшемся окне нажать на вкладку свойства.

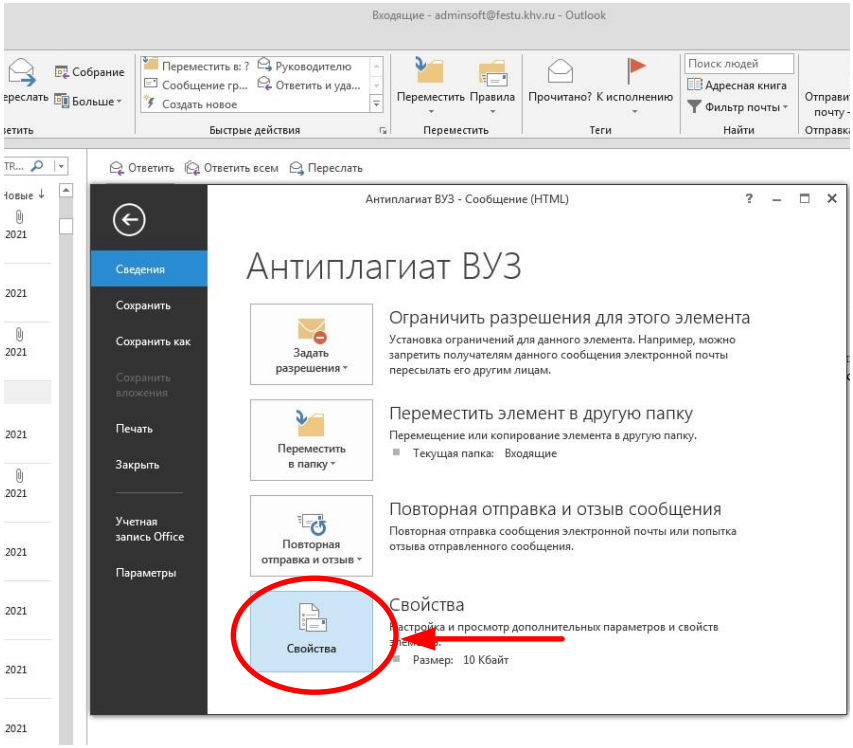

рис. 4 – кнопка открытия свойства письма

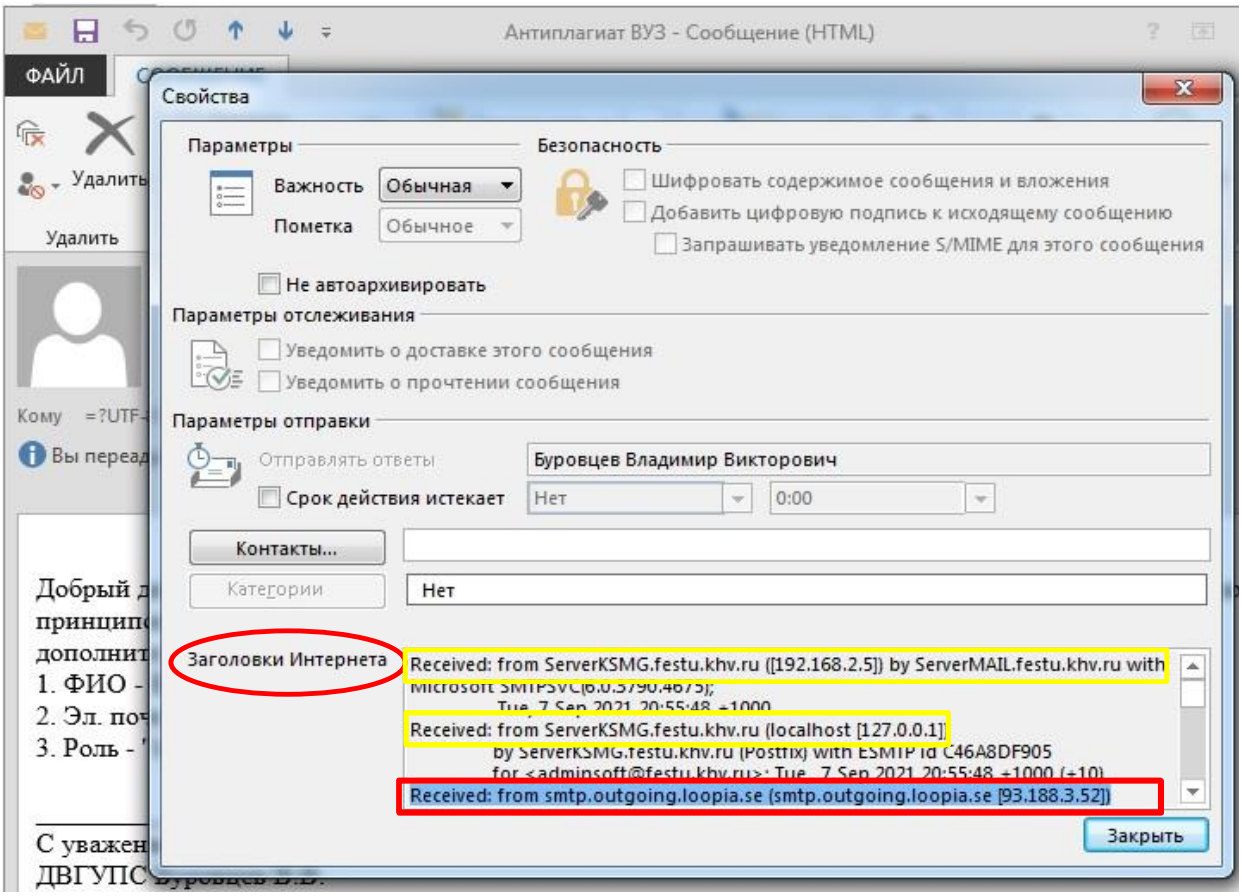

рис. 5 – свойства письма

В открывшемся окне обратите внимание на нижний раздел «Заголовки Интернета», где расписано *от кого получено* (**Received: from**) и *для кого направлено* (**for**) письмо.

Просмотрите в этом окне все строчки, начинающиеся с «**Received: from** …». Как видно на рисунке 5, жёлтым цветом отмечено, что сообщение прошло через сервера ДВГУПС (имена серверов ДВГУПС всегда заканчиваются на «**.festu.khv.ru**»). Последовательность пересылки сообщений отображается снизу-вверх и если пролистать ниже, то можем увидеть строчку, выделенную красным прямоугольником, где фигурирует сторонний сервер (**smtp.outgoing.loopia.se**), который и переслал нам это сообщение.

Однако, письма ДВГУПС обрабатываются на серверах университета и при пересылки корпоративной почты между сотрудниками сторонние адреса участвовать никак не должны! А значит это письмо - очередная уловка мошенников.

Будьте бдительны и не спешите доверять приходящим Вам письмам!

С уважением, сотрудники УИТ