ПАМЯТКА ПО БЕЗОПАСНОЙ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ.

В связи продолжающейся фиксацией фактов рассылок фишинговых писем проводимых злоумышленниками с целью получения конфиденциальных данных пользователей, внедрения вредоносного програмного обеспечения, а также рассылки заведомо ложных сообщений об актах терроризма. Пользователям при работе с электронной почтой сети Интернет необходимо соблюдать следующие правила:

1. Внимательно проверяйте электронные письма

Получив любое письмо, не спешите отвечать или выполнять инструкции из него: сначала обратите внимание на важные детали. Что должно насторожить?

- Броская тема. Крупные переводы, денежные компенсации, взлом или блокировка учетной записи, мошеннические операции, банковская деятельность, геополитическая обстановка… Злоумышленники стараются завладеть вниманием, играя на чувствах жертвы, особенно часто — на жадности или страхе.
- Нагнетание обстановки. Фразы вроде «срочно!» и «у вас осталось всего 3 часа», обилие восклицательных знаков — все это уловки злоумышленников, цель которых заставить вас торопиться, паниковать и от этого потерять бдительность.
- С особой осторожностью относиться к письмам, в которых содержаться угрозы или требования к совершению определенных действий («Открой», «Прочитай», «Подтвердить регистрацию» и т.д.).
- Ошибки, опечатки и странные символы в тексте, а также замена части букв на похожие латинские. Это способ обойти спам-фильтры.
- Странный адрес отправителя. Нагромождение случайных букв и цифр. Или неверно указанный домен в адресе отправителя письма с именами известных почтовых сервисов с небольшим изменением, например: mayl.ru или qoogle.com — признаки фишинговых писем.
- Ссылка в письме, если она там есть. Точнее, адрес сайта, на который она ведет. Чтобы увидеть его, нужно навести мышку на ссылку и внимательно проверить адрес.
- Вложения. Фишинговые письма могут содержать вложения в виде файлов с вредоносным программным обеспечением.
- Просьбы о предоставлении личной информации. Фишинговые письма могут содержать требования о предоставлении логинов, паролей, номеров банковских карт другой конфиденциальной информации.

2. Что делать, если Вы обнаружили фишинговое письмо?

- Внимательно проверить адрес отправителя письма.
- Не нажимайте на ссылки, если они заменены на слова.
- Не скачивайте вложения из писем, если вы не уверены в их подлинности.

- 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.
- Не загружайте картинки содержащиеся в письмах полученных из незнакомых вам источников.
- Внимательно относиться к письмам на иностранном языке.
- Не пересылайте письма коллегам, родственникам и иным лицам;
- Удалите фишинговое письмо.

3. При поступлении на адрес электронной почты заведомо ложного сообщения об акте терроризма необходимо принять следующие меры:

- Поступившее сообщение об акте терроризма не удалять.
- Осуществить копирование текста сообщения об акте терроризма в виде снимков экрана устройства (скриншотов либо фотоизображений, полученных посредством цифровой фотофиксации).
- На скриншотах (фотоизображениях) должна отображаться следующая информация об объекте:
  - название темы письма;
  - адрес электронной почты отправителя письма;
  - дата и время отправления письма;
  - полный текст письма;
  - вложения в виде файлов;
- При невозможности фиксации сообщений об акте терроризма в виде скриншотов/фотоизображений осуществить их фиксацию посредством функций копирования и вставки в документ Word (с сохранением указанной информации об объекте).
- О поступившем сообщении об акте терроризма незамедлительно сообщить старшему дежурному оперативному БГУ по телефону (3952) 500008, доб. 151, ожидать дальнейших инструкций.