ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

Правила, которые необходимо соблюдать при работе с электронными письмами:

1. Используйте только официальные почтовые ящики (вида i.o.familiya@oiv.rkomi.ru)

Не просматривайте на работе свою личную почту на @mail.ru, @yandex.ru, @gmail.com и других бесплатных почтовых сервисах.

2. Всегда проверяйте отправителя электронного письма

Дозвонитесь до него и уточните, действительно ли он направил Вам это письмо, не открывая при этом никакие вложенные файлы и не переходя ни по каким ссылкам. Злоумышленники обязательно вышлют Вам вирус в тот момент, когда Вы ждете похожее сообщение (изменение в законодательстве, госпрограмме). И обязательно подделают его под сообщение «с сайта», на рассылку с которого Вы ранее подписались.

3. Не вводите «защитных кодов» и паролей

Установка пароля на архив с документами – всегда говорит о попытке обмана. Если в письме Вас просят ввести пароль, «защитный код», всегда уточняйте у отправителя, что за данные он выслал и зачем. Уточнять необходимо только по телефону. Если телефон не известен, уточните его, задав вопрос отправителю по электронной почте (на «той стороне» может отвечать злоумышленник). После выяснения номера, найдите его в Интернет на сайте организации-отправителя, для того чтобы убедиться, что номер не поддельный (злоумышленник может выдать Вам свой личный номер телефона).

4. Не открывайте файлы, не предназначенные Вам

Никогда не открывайте файлы, которые попали к Вам по ошибке — например, не открывайте присланное Вам резюме, если Вы не работаете в отделе кадров — перешлите письмо им или не отвечайте вовсе.

5. Макросы, "активное содержимое", скрипты и ActiveX в Microsoft Office — это вирусы.

Запомните слова "макрос", "активное содержимое", "скрипт" и "ActiveX". Если Вы встретите их на желтой линии при открытии офисных

документов — это вирус, **не включайте** их использование. При открытии нормальных документов, предупреждения о макросах быть не должно. Именно о макросах, либо "активном содержимом", либо скриптах, либо ActiveX. Пока вы не нажмете на кнопку "Включить содержимое", вирус не запустится. Такая кнопка – часть системы защиты. Обычно в поддельных документах злоумышленники ссылаются на то, что у вас стоит старый офис, не активирована некая важная функция для просмотра именно этого документа и просят включить "макросы".

6. Не помогайте открывать «неоткрывающиеся» файлы

Если коллега просит Вас помочь открыть «не открывающийся файл, присланный ему по почте» — не помогайте. Очень часто при открытии файла-вируса показывается «ошибка открытия» или показываются непонятные символы в WORD, и идет шифрование (даже после закрытия файла). Файл рассылается коллегам с просьбой помочь открыть его. В итоге шифруются файлы всего отдела или организации. Не просите помочь коллег — обращайтесь с заявкой в Службу технической поддержки ГАУ РК «ЦИТ».

7. Не посещайте сайты, не связанные с работой

Не посещайте на служебном компьютере не связанные с выполнением служебных обязанностей сайты (ВКонтакте, Одноклассники, Яндекс-Почта, Google Mail, Mail.ru, Youtube и т.п.). Личную почту просим читать дома.

8. Не используйте программы, не связанные с работой, не устанавливайте программы самостоятельно

Не используйте на рабочем месте не связанные с выполнением служебных обязанностей программы (Skype, ICQ, радио, видео и т.п.). Не пытайтесь устанавливать программы самостоятельно, даже при наличии компетенции в данном вопросе. При необходимости установить на компьютер какую-либо программу обращайтесь с заявкой в Службу технической поддержки ГАУ РК «ЦИТ».

9. Будьте бдительными перед отдыхом и после него!

Будьте особо бдительны перед уходом с работы, перед выходными, перед праздниками и после болезни — злоумышленники всегда пошлют письмо Вам, именно тогда, когда вы устали и менее внимательны.