

Памятка  
по соблюдению мер безопасности при использовании  
служебной электронной почты  
для сотрудников ГАПОУ СО «УПК-МЦК»

1. Электронная почта является одним из самых распространенных путей заражения компьютерными вирусами и источником утечки конфиденциальной информации.
2. Для исполнения служебных обязанностей необходимо использовать только служебную электронную почту. Использование личной электронной почты в служебных целях не допустимо.
3. Не предоставляйте другим лицам (коллегам, родственникам) пароль доступа к почтовому ящику, не пересылайте пароль по электронной почте.
4. При работе с электронной почтой используйте антивирусные средства, которые своевременно обновляются.
5. При получении электронной почты обращайте внимание на адрес отправителя, оформление и стиль написания письма, не открывайте и не сохраняйте файлы (архивы, текстовые файлы, изображения и другие), которые вы не ожидаете, такие файлы могут содержать вредоносный программный код, даже если письмо было отправлено с официального адреса электронной почты.
6. Не открывайте подозрительные ссылки, содержащиеся в тексте писем, в случае перехода по ссылке внимательно проверяйте ее адрес, поскольку мошенники часто используют похожие адреса для фишинговых сайтов (сайты внешне похожие на официальные) с целью кражи конфиденциальной информации (логинов, паролей, реквизитов банковских карт).
7. С использованием электронной почты запрещается пересылать информацию ограниченного доступа (персональные данные, информацию для служебного пользования), а также пересылать нелегально распространяемые материалы (аудио-, видеоданные, программное обеспечение).
8. Старайтесь не указывать адрес электронной почты на сайтах и других ресурсах, если это не вызвано служебной необходимостью, поскольку это может привести к включению адреса в списки спам-рассылок.
9. Если поступило нежелательное или подозрительное электронное письмо переместите его в нежелательную почту (для этого щелкните правой кнопкой мыши на входящем письме и нажмите кнопку Нежелательные > Заблокировать отправителя).
10. Самостоятельно осуществляйте смену пароля, используемого для доступа к электронной почте, не реже одного раза в полгода. При компрометации пароля необходимо незамедлительно произвести его смену.
11. В случае компрометации пароля, используемого для доступа к электронной почте, получения подозрительного письма, подозрение на взлом или попытку взлома почтового ящика необходимо сообщить об этом в отдел информационно-технического обеспечения.