Инструкция по алгоритму действий

при поступлении анонимных электронных почтовых сообщений

Уважаемые коллеги!

В связи с участившимися случаями мошенничества с использованием средств электронной почты (фишинговые рассылки), просим Вас придерживаться следующих рекомендаций специалистов по защите информации при обработке корреспонденции на корпоративном рабочем месте:

∙ Получив неожиданное или подозрительное письмо (например, содержащее неправильно написанные слова, неправильные URL-домены, с низким качеством графики, неизвестными отправителями, расхождениями в форматировании), сразу перешлите его на адрес электронной почты **ibinfo@yarregion.ru** для анализа.

∙ С вниманием относитесь к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса. Постарайтесь без необходимости не открывать вложения и не переходить по ссылкам.

∙ Вложениями к письмам могут оказаться любые файлы Microsoft Excel, Microsoft Word, PDF-документы, изображения. В случае получения письма с вложением в виде документов Excel или Word помните: выполнение макросов в этих документах может стать причиной заражения вашего компьютера вредоносным ПО.

∙ В случае, если вложение необходимо сохранить, проверьте его антивирусом.

∙ Не распространяйте это подозрительное письмо!

∙ Не игнорируйте сообщения браузера о возможных угрозах.

∙ Проверяйте URL-адреса. Особенно ссылки, полученные от незнакомых отправителей. Зачастую злоумышленники используют похожие по написанию домены. Например, g00gle.com, faecbook.com, secure-paypal.com.

∙ Если все же необходимо посетить ресурс, лучше введите его адрес вручную или воспользуйтесь ранее сохраненными закладками.

∙ Проверяйте наличие префикса HTTPS:// на сайтах, где требуется ввести конфиденциальную информацию, например, пароли.

∙ Никогда не сообщайте никому пароли, коды или иные данные, используемые для подтверждения чего-либо, а также чувствительную для вашей деятельности информацию, предназначенную для служебного пользования (отчеты, графики, приказы). Просящий может представиться любым человеком. Современные системы безопасности создаются таким образом, чтобы пароли и коды не передавались от человека к человеку.

В случае возникновения проблем обращайтесь в службу технической поддержки государственного бюджетного учреждения Ярославской области «Электронный регион».

Министерство цифрового развития Ярославской области