ОСТОРОЖНО, ФИШИНГ!

Анализ сведений об угрозах безопасности информации указывает на нарастающую активность злоумышленников, направленную на попытки получения сведений ограниченного доступа посредством фишинговых рассылок писем, имитирующих официальные запросы федеральных государственных структур.

В связи с чем, обращаем внимание о мерах по противодействию фишиговым атакам для повышения осведомлённости и понимания основных принципов распознавания фишинговых писем во избежание передачи сведений ограниченного доступа злоумышленникам.

Основные меры по противодействию фишингу:

- Проверять адреса электронной почты, обращать внимание на домены отправителей, часто злоумышленники используют имена доменов, похожие на реально используемые федеральными органами, но содержащие орфографические ошибки или дополнительные символы.
- Избегать открытия вложений от неизвестных отправителей или из неожиданных источников.
- Проявлять бдительность при работе с гиперссылками, не переходить по ссылкам, содержащимся в письмах от незнакомых или подозрительных отправителей. Наведение курсора мыши на ссылку позволяет увидеть её реальный URL-адрес.

Также обращаем внимание на необходимость реализации технических мер, направленных на противодействие фишинговым атакам, на регулярной основе рассылаемых ФСТЭК России.

Дополнительно сообщаем, что информация о выявленных уязвимостях программного обеспечения и мерах по их устранению регулярно публикуется на сайте ФСТЭК России, ссылка на раздел «Уязвимости» сайта ФСТЭК России: https://bdu.fstec.ru/vul.

При выявлении любых попыток несанкционированного доступа к служебной информации и персональным данным сотрудников необходимо незамедлительно информировать министерство цифрового развития Красноярского края.