Правительство
Ростовской области

Министерство
цифрового развития,
информационных технологий
и связи Ростовской области
(мининформсвязь области)

Социалистическая ул., д. 110-112/12«а»/15
г. Ростов-на-Дону, 344050
телефон/факс (863)280-68-06
e-mail: minsvyaz@donland.ru
http://minsvyaz.donland.ru

Руководителям
исполнительных органов
Ростовской области

Главам администраций
муниципальных образований
Ростовской области

Анализ сведений об угрозах безопасности информации показывает, что зарубежными хакерскими группировками в адрес органов государственной власти субъектов Российской Федерации, федеральных органов исполнительной власти и организаций Российской Федерации направляются фишинговые письма, содержащие вредоносные вложения в виде ссылок на информационные ресурсы, архивов и файлов, а также призывы к действиям экстремистского характера.

С целью предотвращения реализации угроз безопасности информации, связанных с фишингом, необходимо принять следующие дополнительные меры защиты информации:

1. Довести до сотрудников единый почтовый ящик для направления подозрительных электронных писем: anti-spam@donland.ru.

2. Проинформировать работников ведомства (организации) о необходимости:

направления всех подозрительных электронных писем на почтовый ящик электронной поты, указанный в пункте 1 настоящих рекомендаций;

внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;

не открывать письма от неизвестных адресатов;

проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься», «срочно»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т. д.);

не нажимать на ссылки из письма, если они заменены на слова, не наводить на них курсором и просматривать полный адрес сайтов;

проверять ссылки, даже если письмо получено от другого пользователя информационной системы;

не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

внимательно относиться к письмам на иностранном языке, с большим количеством получателей.

3. Настроить в средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на почту вложений.

4. Активировать (при возможности) механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM, DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий.

5. Заблокировать (при возможности) получение пользователя информационной системы в электронных письмах вложений с расширениями: ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

6. Заблокировать доставку писем от доменов-отправителей стран, поддержавших санкции Украины, США и страны Европейского союза.

Прошу поручить довести до ответственных должностных лиц для использования в повседневной деятельности.

Министр
цифрового развития,
информационных
технологий и связи
Ростовской области Е.В. Полуянов

Коваленко Евгений Николаевич
+7 (863) 240-50-73