**Рекомендации по защите информации от фишинговых электронных писем с вредоносным вложением**

I. С целью предотвращения реализации угроз безопасности информации, связанных с утечкой защищаемой информации, при помощи фишинговых электронных писем с вредоносным вложением в виде ссылок на информационные ресурсы, архивов и файлов, необходимо принять следующие дополнительные меры защиты информации:

1. обеспечить пересылку всех подозрительных электронных писем на адрес электронной почты spam@e-dag.ru;

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

3. не открывать письма от неизвестных адресатов;

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

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

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

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

8. не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширением RTF, LNK, CHM, VHD;

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

Также злоумышленники используют методы социальной инженерии, получают доступ к электронной почте и отправляют от их имени фишинговые

электронные письма с вредоносным вложением. Одно из таких писем имеет следующие индикаторы компрометации:

«Приказ №21 от 29-03-2022.docx,
md5: 23c16062cd05f15d6ddd8e843c2267c9,
url:https://roskazna.net/acpx/t.php?t=afe6b1892cdc57c660d6ac5dd69b1fb4356001bee7910d983619d69ddc294c3359a20345fd3a8ee67c8228a7058dc7ce&action=show_document&z=1&x=2500».

При этом, направляя фишинговые рассылки со следующих зарегистрированных почтовых серверов:

mx.roztec.ru, mx.nacimibio.ru, mail.kazkad.ru, mlrmailer.com, mail.mlrmailer.com, sender-gosuslugi.ru, mail.sender-gosuslugi.ru, mail.gazpromlpg.ruoe.ru, mail.npoem.ruoe.ru, email.tpprf.ruoe.ru, dionis.r31.rosreestr.ruoe.ru, mx.vertical.ruoe.ru, mail.muctr.ruoe.ru, mail.tcm-u.ruoe.ru, mail.it-vbc.ruoe.ru, mail.ktrv.ruoe.ru, mail.hi-tech.ruoe.org, mail.acti.ruoe.ru, mail.am-tec.ruoe.ru, mail.sevastopolteplo.ruoe.ru, olymp.deloports.ruoe.ru, outlook.ekassir.uercus.com, post.sberbank-tele.uercus.com, mail-kras.bbr.ruoe.ru, email.okb-nouator.ru, mail.kronshadt.ru, mail.tscrimea.ruoe.ru, mail.gazpromviet.uercus.com, mail.volnamobile.ruoe.ru, mail.5-tv.ruoe.ru, exchange-log.rzdlog.ruoe.ru, mail.rossiya-airlines.uercus.com, mail.dynasystem.ruoe.ru, mail.ventocloud.ruoe.ru, mail.omg.transneft.ruoe.ru, mail.digital.gov.ruoe.ru, mail.tass.ruoe.ru, post2.interfax.ruoe.ru, mail.iz.ruoe.ru, app.aif.ruoe.ru, mail.tvrain.ruoe.ru, mail.life.ruoe.ru, mail.vniiem.ruoe.ru, mail.aviaremont.ruoe.ru, smtp.mikron.ruoe.ru, mail.kmz.ruoe.ru, mail.vympel-rybinsk.ruoe.ru, mail.goz.ruoe.ru, mail.ach.gov.ruoe.ru, mail.fadm.gov.ruoe.ru, mail.rst.gov.ruoe.ru, mail.minstroyrf.ruoe.ru, mail.minobrnauki.gov.ruoe.ru, postman.rosleshoz.ruoe.ru, mail.21.mchs.gov.ruoe.ru, email.mkrf.ruoe.ru, mail.knaaz.ruoe.org, mail.nicevt.ruoe.ru, mail.gardatech.ruoe.ru, mail.dtln.ruoe.ru, webmail.planar-elements.ruoe.ru, mx13.m13.ruoe.ru, mail.informseti.ruoe.ru, mail.cloud.mts.ruoe.ru, exchange.avito.ruoe.ru.

II. С целью предотвращения реализации угроз безопасности информации, связанных внедрением вредоносного программного обеспечения через почтовые вложения. Нарушители используют методы социальной инженерии, отправляя пользователям фишинговые электронные письма с вредоносным вложением.

Указанные электронные письма содержат вложения в виде электронных документов, содержащих списки участников совещания, протоколов (например, электронные документы с наименованиями «Список участников.doc» и

«17.06.2022_Протокол_МРГ_Подгруппа_ИБ.doc»). Фишинговые письма направляются с адресов электронных почт, содержащий домен gmx.ru.

В целях предотвращения реализации угроз безопасности информации считаем необходимым принять дополнительные меры:

- заблокировать доставку писем от домена-отправителя gmx.ru;

- обновить базы антивирусных средств защиты информации до актуальных версий;

- обеспечить мониторинг информационных ресурсов Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) на предмет выявления фишинговых рассылок в органы (организации) с целью оперативного принятия мер защиты информации на основании индикаторов компрометации, содержащихся в бюллетенях НКЦКИ.

Проинформировать пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно:

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

- не открывать письма от неизвестных адресатов;

- не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, исполняемые файлы.