Правила
безопасной работы с почтовыми сервисами в сети Интернет

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

1. Организовать единый почтовый ящик электронной почты внутри ведомства (организации), на который работники направляют подозрительные электронные письма.

2. Проинформировать необходимости: работников ведомства (организации) о направления всех подозрительных электронных писем на почтовый ящик электронной почты, 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»), 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 мышкой и просматривать полный адрес сайтов;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
- не открывать вложения, особенно если в них содержаться 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 стран Европейского союза.