# Памятка по безопасной работе
# с корпоративной email-корреспонденцией

## *Письма стоит считать подозрительными, если они содержат:*

- ✓ ссылки в виде цифр. Пример: 178.248.232.27
- ✓ ссылки, содержащие символ «@»; Пример: http://bank.ru@phish.ru
- ✓ ссылки с двумя и более адресами. Пример: https://bank.ru/bitrix/rd.php?go=https://bitly.com/bank
- ✓ в начале адреса сайта есть www, но нет точки или стоит тире. Пример: wwwbank.ru или www-bank.ru
- ✓ в начале адреса сайта есть http или https, но нет «://». Пример: httpsbank.ru
- ✓ в ссылке после www вместо точки встречается тире. Пример: www-bank.ru
- ✓ когда в адресе сайта несколько точек, смотрите то, что написано в правой части, до первого символа «/», там вы обнаружите исходный сайт и если он вам не знаком ссылка подозрительна. Пример: www.bank.ru.zlodey.ru/login?id=12/aa/bank.ru
- ✓ если при наведении указателя «мыши» ссылка выглядит по-другому. Пример: в тексте письма написано tele2.ru, а при наведении мыши, в нижнем углу браузера отображается teie2.ru
- ✓ ссылка может быть не кликабельна, но содержать подмененные символы. Злоумышленник надеется, что вы скопируете ссылку и вставите в браузер. Пример: в письме указана ссылка tele2.ru, копируете и вставляете в браузер, но оказывается, что это teie2.ru
- ✓ злоумышленник может заменить букву “o” на цифру “0” или маленькую латинскую букву L “l”, на большую букву i “I” или b на d и т.д. Пример: 0nline.dank.ru вместо online.bank.ru
- ✓ если ссылка начинается с https:// — это не значит, что она безопасна;
- ✓ несколько ошибок и описок;
- ✓ буквы в тексте частично подменены; Примеры: д0брый денb, kaк делα;
- ✓ письма с отсутствующими дополнительными контактами (ФИО, должность, телефон, почтовый адрес);
- ✓ используется нестандартное оформление корпоративного стиля, который обычно использовался. Пример: без логотипа, другим размером или стилем шрифта.
- ✓ любые письма с вложениями по умолчанию стоит считать подозрительными. Это не значит, что их сразу нужно отправлять в службу безопасности. Просто через вложения чаще всего заражают компьютеры и ни один антивирус не гарантирует полной защиты.
  Если вы не ожидали письма с этим вложением и/или в письме есть другие признаки, следуйте инструкции ниже.

**Помните:** email в поле «Отправитель» может быть подделан или знакомого отправителя могли взломать.

## *Что делать при получении подозрительного письма:*

Итак, вы определили, что письмо подозрительное, что делать дальше?

- ✓ лично, по телефону, через мессенджер или каналы коммуникации в вашей организации уточнить факт отправки такого письма;
- ✓ контакт для связи взять не из письма, а из других источников: собственная записная книжка, визитка, спросить у коллег, узнать на официальных сайтах, корпоративный телефонный справочник;
- ✓ либо, сразу перешлите письмо в службу безопасности.