Рекомендации
по защите от угроз фишинговых и вредоносных писем

Электронная почта является основным вектором компьютерных атак на корпоративные информационные сети и системы.

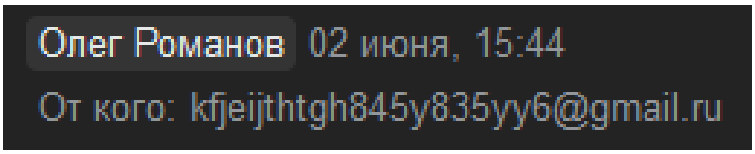
Злоумышленники составляют убедительные адресные письма и, используя техники социальной инженерии и актуальные информационные поводы, обманом заставляют пользователей загружать вредоносные программы себе на устройства чтобы раскрыть злоумышленнику конфиденциальную информацию или вводить на фишинговых страницах принадлежащие пользователю учётные и персональные данные, номер банковской карты и т.п.

В результате злоумышленники могут получить доступ в корпоративную сеть с целью кражи данных, конкурентной разведки, нарушения функционирования информационных систем, вывода из строя средств защиты информации и т.п

Признаки фишинговых писем:

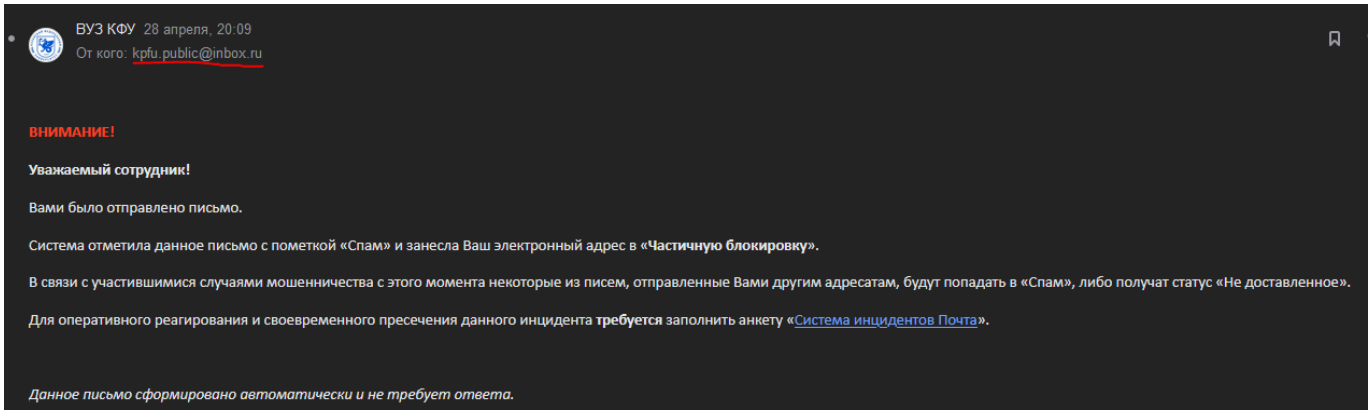
— Отсутствует имя отправителя и контактные данные.

— Адрес отправителя состоит из бессмысленного набора букв.



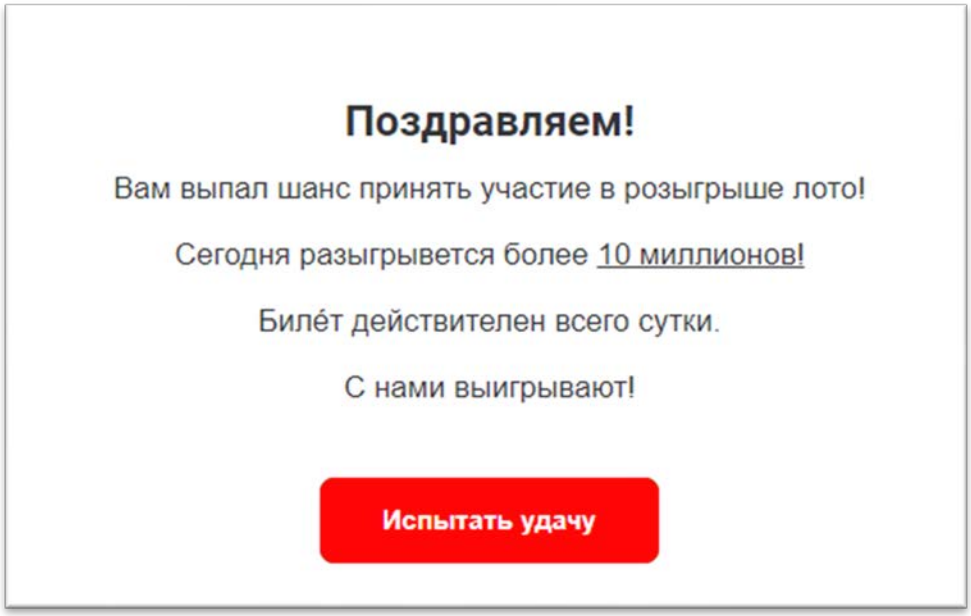
— Письмо приходит от имени крупной организации, но на официальном сайте адрес этого отправителя отсутствует.

— Отправитель представляется сотрудником компании, но пишет не с корпоративной почты, а с обычной: gmail.com, mail.ru, inbox.ru и т.п.



— В адресе ссылки есть необычные символы, например, @.

— В письме используются буквы, похожие на кириллицу.



— У файлов, вложенных в письмо, неизвестное расширение или непонятное название.

— Ссылки не вставлены в текст, а замаскированы изображениями, кнопками, яркими картинками и QR-кодами.

Некоторые темы, по которым можно отличить фишинговые письма:

— Кто-то взломал вашу почту и узнал пароль / Мы обнаружили подозрительные или мошеннические действия в вашей учётной записи / Кто-то изменил настройки безопасности вашей почты.

— Ваша учётная запись заблокирована или отключена / Вы добавлены в чёрный список: мы поняли, что вы мошенник или бот!

— Вам важный документ из налоговой, полиции, кредитной организации и т. п.

— Письмо от вашего коллеги/партнёра с документами или «важными рабочими» ссылками.

— Вы выиграли приз! Перейдите по ссылке, чтобы узнать условия получения и/или доставки.

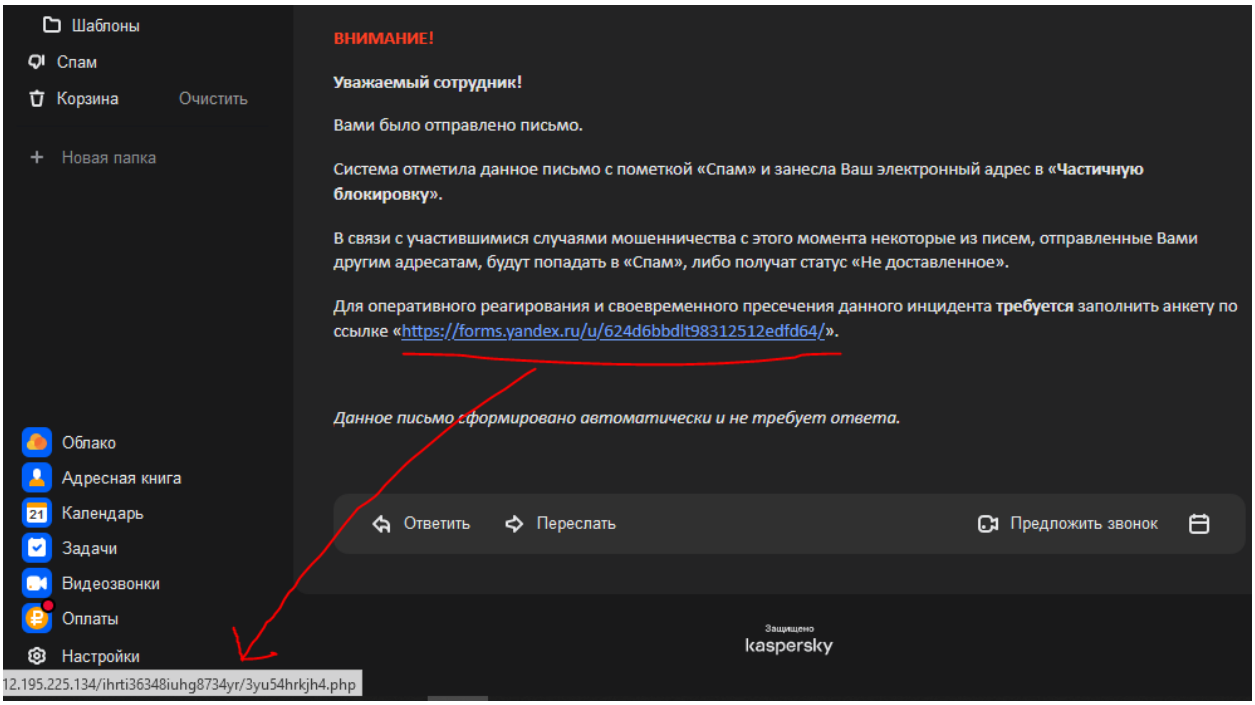
— Вы не погасили кредит — дело передаётся в суд.

Базовые меры защиты от фишинга и социальной инженерии

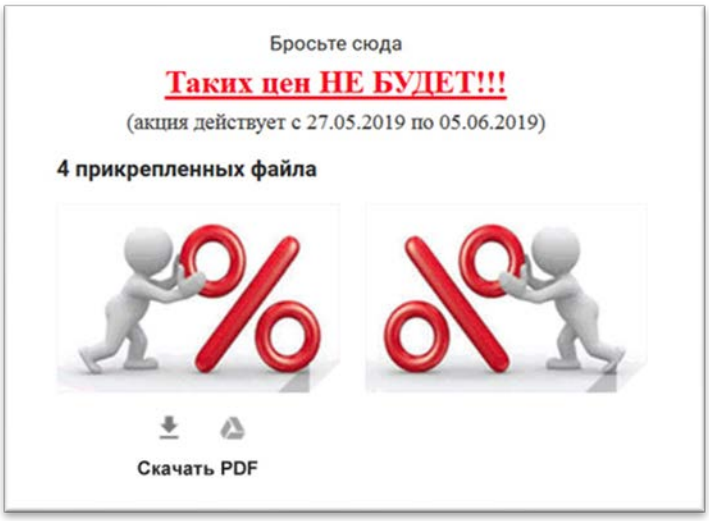
— Не переходить по ссылкам и не скачивать файлы, содержащиеся в письмах электронной почты от неизвестных адресантов.

— Уточнять у известных адресантов с помощью других доступных каналов связи (телефонного звонка, сообщения в мессенджере) действительно ли они отправляли электронное письмо.

— Проверять реальные адреса гиперссылок, содержащихся в письме, наводя на них курсор. Адрес, куда ведёт ссылка, будет отображён в строке состояния почтовой программы. Особое внимание обратить на длинные ссылки, ссылки, созданные с помощью сервисов сокращения (например, bit.ly, tinyurl.com), либо на гиперссылки, привязанные к тексту.



— Считать подозрительными письма, у которых в поле «Тема» содержится призыв к действиям (например «открой», «прочитай», «ознакомься»), а также упоминаются финансы, геополитическая обстановка или содержатся угрозы.



— Внимательно относится и проверять письма, содержащие вложения. Особенно если это документы с макросами, архивы с паролями, а также файлы с расширениями .rtf, .lnk, .chm, .vhd.

— Перепроверять письма, в тексте которых содержатся орфографические ошибки, письма на иностранном языке, письма с большим количеством получателей.

ВНИМАНИЕ! В случае сомнений в отнесении каких-либо писем к вредоносным, Вы можете создать заявку в системе заявок КФУ или отправить письмо на почту Службы информационной безопасности КФУ SIB@kpfu.ru.