

Фишинговое письмо: «красные флаги»

ПОДДЕЛЬНЫЙ ОТПРАВИТЕЛЬ (ДОМЕН)

Опечатки в домене. Домен после «@» не корпоративный: @gmail.com, @yandex.ru

СРОЧНОСТЬ И ДАВЛЕНИЕ

Слова: «Срочно», «Немедленно», «Последний шанс», «Блокировка», «Увольнение», «Штраф», «Зарплата задержана». Ультиматумы: «Сделай до (сегодня – вечер)», «Иначе последствия»

КОНФИДЕНЦИ- АЛЬНОСТЬ

Просьбы: «Никому не говори», «Не пересылай», «Сохрани в тайне», «Это только для тебя». Обоснования: «Секретная сделка», «Внутреннее расследование», «Личный приказ директора»

ЗАПРОСЫ ДАННЫХ ИЛИ ДЕНЕГ

Просьба передать: пароли, логины, банковские реквизиты, отчеты по счетам, ИНН/ паспортные данные, контрольные вопросы. Требование перевести деньги на новый счет, оплатить «срочный штраф»

ВЛОЖЕНИЯ

Неожиданные файлы от коллеги или руководства. Подозрительные расширения: .exe, .scr, .js, .vbs, .bat, .cmd, .zip с паролем, .docm, .xlsm

КРИЧАЩЕЕ ФОРМАТИРОВАНИЕ

Красные заглавные буквы, много восклицательных знаков. Орфографические или грамматические ошибки. Логотипы компании низкого качества, нестандартные шрифты

«ЛИЧНЫЙ» КОНТАКТ

Просьба ответить на другой e-mail или в Telegram и WhatsApp. «Пиши мне в личку здесь: +79XXX...». Обход корпоративных каналов через указание «личного» номера телефона для «срочной связи»

ЧУВСТВО ДИСКОМФОРТА

«Что-то не так», «Директор так не пишет», несоответствие стандартным процедурам организации

Что делать, если обнаружили «красные флаги»

- 1 **НЕ** отвечать на письмо
- 2 **НЕ** открывать вложения
- 3 **НЕ** переходить по ссылкам
- 4 **НЕ** пересылать письмо коллегам
- 5 Написать в IT-отдел:
 - переслать письмо как вложение (полностью, включая текст!);
 - кратко описать подозрительное письмо
- 6 Удалить письмо из почтового ящика после передачи в службу безопасности

Что делать, если нажали на ссылку

- 1 Немедленно закройте вкладку
- 2 Не вводите логины, пароли, номера карт. Если уже ввели – срочно меняйте пароли
- 3 Сообщите в службу IT
- 4 Проверьте безопасность своего компьютера:
 - запустите антивирус;
 - посмотрите, не началась ли странная активность – автозапуски, реклама, сломанная почта
- 5 Смените пароли, если хоть что-то вводили