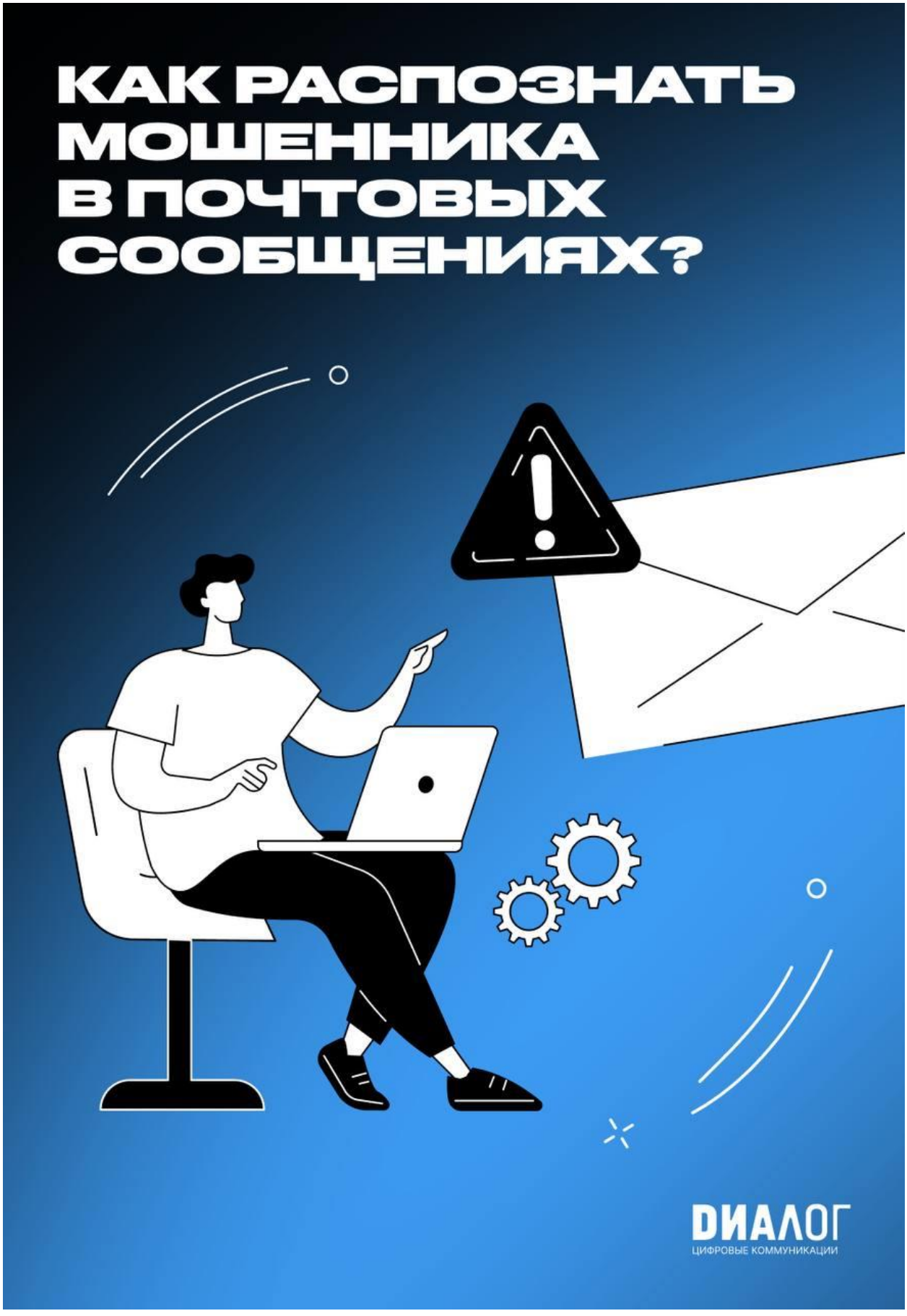
КАК РАСПОЗНАТЬ МОШЕННИКА В ПОЧТОВЫХ СООБЩЕНИЯХ?



ДИАЛОГ
ЦИФРОВЫЕ КОММУНИКАЦИИ

ЧТО ТАКОЕ ФИШИНГ И КАК С НИМ БОРОТЬСЯ?

Фишинг – вид интернет-мошенничества, его цель – получить ваши данные (логин-пароль), конфиденциальную информацию или запустить вредоносное программное обеспечение

Если вы получили письмо, которое требует от вас какого-либо взаимодействия, вызывает у вас чувство страха или любопытства, призывает вас действовать срочно, то задайте себе следующие вопросы:

- Ожидаю ли я это письмо?
- Есть ли смысл в том, что от меня требуют?
- Знаю ли я автора этого письма?
- Если я сделаю, что от меня требуют, какие могут быть последствия?
- Есть ли в письме подозрительные ссылки и вложенные файлы?

ДИАЛОГ
ЦИФРОВЫЕ КОММУНИКАЦИИ

ПРОАНАЛИЗИРУЙТЕ АДРЕС ОТПРАВИТЕЛЯ

1. Стоит внимательно изучить адрес, с которого пришло письмо. Если он написан неправильно или выглядит подозрительно, скорее всего, это спам.

   Пример:

   ivanova@gosuslugi.ru – корректный

   ivanova@gosuslugi.su – ложный

2. Проверьте тему письма. Спам-письма часто содержат темы, которые выглядят привлекательно или вызывающе беспокойство. Например, в таких письмах может содержаться информация о выигрыше в конкурсе, неожиданном наследстве или срочной необходимости оплаты счета.

ПРОАНАЛИЗИРУЙТЕ ВЛОЖЕНИЕ

- Не открывайте вложения в подозрительных письмах. Они могут содержать вирусы или другие вредоносные программы
- Не запускайте файлы с незнакомыми вам расширениями
- Обращайте внимание на сообщения от программ, которые могут сигнализировать об опасности (например, антивирус или средства безопасности операционной системы).
- Не разрешайте выполнение макросов в офисных документах (если вы сами с ними не работаете)

ДИАЛОГ
ЦИФРОВЫЕ КОММУНИКАЦИИ

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ ФИШИНГОВОЕ ПИСЬМО

- Не переходить по ссылке
- Не копировать адрес ссылки
- Не скачивать документы из письма
- Не открывать их
- Не пересылать письма коллегам
- Не использовать телефон для перехода по ссылке
- Не подгружать картинки от незнакомых людей
- Если вы сомневаетесь, правильно ли определили фишинг или нет, свяжитесь с собеседником по другому виду связи (позвоните на телефон, напишите в мессенджер и спросите, отправлял он вам сообщение или нет)
- Если вы ввели свои учетные данные и считаете, что они стали доступны злоумышленникам, срочно меняйте их, если есть возможность

ДИАЛОГ
ЦИФРОВЫЕ КОММУНИКАЦИИ

КАК ПРОВЕРИТЬ ПИСЬМО НА ФИШИНГ?

ПРОАНАЛИЗИРУЙТЕ ГИПЕРССЫЛКУ

1. Посмотрите, знаком ли вам сайт, на который предлагают перейти в письме

2. Имя сайта написано корректно?
Проверьте, не подменены ли буквы, корректно ли использован домен верхнего уровня (.ru, .com, .рф), нет ли «лишних» знаков

Пример:

https://dialog.info – корректный

https://clialog.info// – ложный (d заменено на cl)

3. Обратите внимание на наличие коротких гиперссылок

Злоумышленники часто прячут URL-адрес на свои фишинговые страницы за подобными короткими ссылками

Пример:

https:/bit.ly/2sAHAOv

https:/cut.ly/wrwtLNH

ДИАЛОГ
ЦИФРОВЫЕ КОММУНИКАЦИИ