## Обобщенный анализ схемы

Через копоративную почту или мессенджер сотрудник организации получает сообщение от службы техподдержки или службы безопасности своей организации. В письме сообщается об истечении срока действия пароля, почтового аккаунта, изменения технических условий работы почтовой службы и т.п. Для продления работы ресурсов мошенник просит передать набор персональных/служебных данных: ФИО, пароль, номер телефона и т.п.

**Важно:** в данном сценарии мошенник действует от лица анонимного пользователя или реального сотрудника организации, чей аккаунт был взломан ранее.

# Типовой сценарий

**На корпоративную почту или в мессенджер сотрудника организации направляется письмо следующего содержания:**

Уважаемый пользователь учетной записи электронной почты:
логин@домен организации.ру.
Из-за большого количества спам-сообщений в настоящее время мы обновляем корпоративную базу данных.
Чтобы продолжить использовать свою учетную запись, Вам необходимо ответить на это письмо и предоставить следующую информацию (*перечисляется набор персональных/служебных данных: логин, пароль и т.п.*).

Если Вы не ответите на данное сообщение, Ваша учетная запись будет деактивирована.

# Кейсы из реальной жизни

Это уведомление по электронной почте предназначено для [redacted]@ranepa.ru

18 июля, 2024 г. | 18:16:52 вечера

[redacted]@ranepa.ru - Уведомление об истечении срока действия пароля!!!

Срок действия пароля для [redacted]@ranepa.ru истекает сегодня , 18 июля 2024 г.

Пожалуйста, найдите время сейчас, чтобы сохранить свой пароль, чтобы избежать прерывания или автоматической блокировки вашей электронной почты:

ВОЙДИТЕ, ЧТОБЫ НАЧАТЬ НАЧАТЬ

# Кейсы из реальной жизни

[Запрос №202211031064748] Обновление вашего технического запроса

R ranepa.ru Служба поддержки 22 февраля в 2:48
Я >

Возможно, этот отправитель олицетворяет домен, связанный с вашей организацией. Узнайте о риске, связанном с этой ситуацией

Уважаемый пользователь учетной записи электронной почты: @ranepa.ru

Из-за большого количества спам-сообщений в настоящее время
Мы обновляем нашу базу данных, чтобы предоставить вам лучшее
услуга.

Чтобы продолжить использовать свою учетную запись, вам необходимо ответить на это письмо,
прежде чем предоставлять следующую информацию для продолжения:

Полные имена:
Электронная почта:
Имя пользователя:
Пароль:
Подтвердите пароль:
Тел:

Примечание. Если вы не ответите на это сообщение, ваша учетная запись будет деактивирована в нашей базе данных и больше не будет получать и отправлять электронные письма.
Приносим извинения за возможные неудобства.

Привет,

Административные системы.