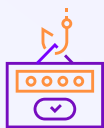


Памятка

Как распознать фишинг и не стать жертвой киберпреступников

Что хотят получить от вас злоумышленники



Учетные данные — логины и пароли от корпоративной или личной учетной записи.



Доступ к конфиденциальной информации или деньгам.



Доступ к системе безопасности для ее отключения или установки вредоносного ПО.

Как проанализировать подозрительное письмо

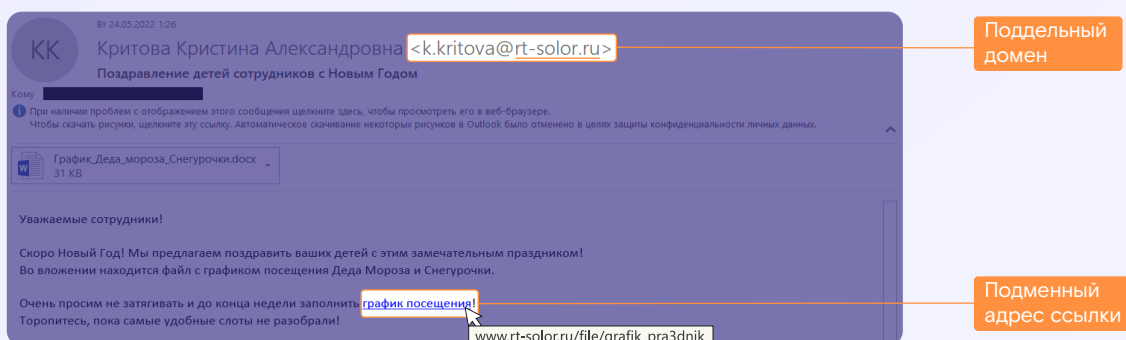
Для проверки письма на фишинг ответьте на вопросы. Если в ответах больше двух красных флажков — скорее всего, письмо прислали мошенники.

| О письме | Да | Нет |
|---|----|-----|
| Я ждал это письмо? | ✓ | 🚩 |
| Я знаю отправителя? | ✓ | 🚩 |
| Я ждал, что будет ссылка в письме? Я знаю URL ссылки? | ✓ | 🚩 |
| Текст ссылки = ее URL? | ✓ | 🚩 |
| Письмо с вложением: .zip / .js / .exe / .scr? | 🚩 | ✓ |
| Письмо с вложением .doc или .xls. Файл просит включить поддержку макросов? | 🚩 | ✓ |

Основные признаки фишинга

Фишинговое письмо чаще всего содержит:

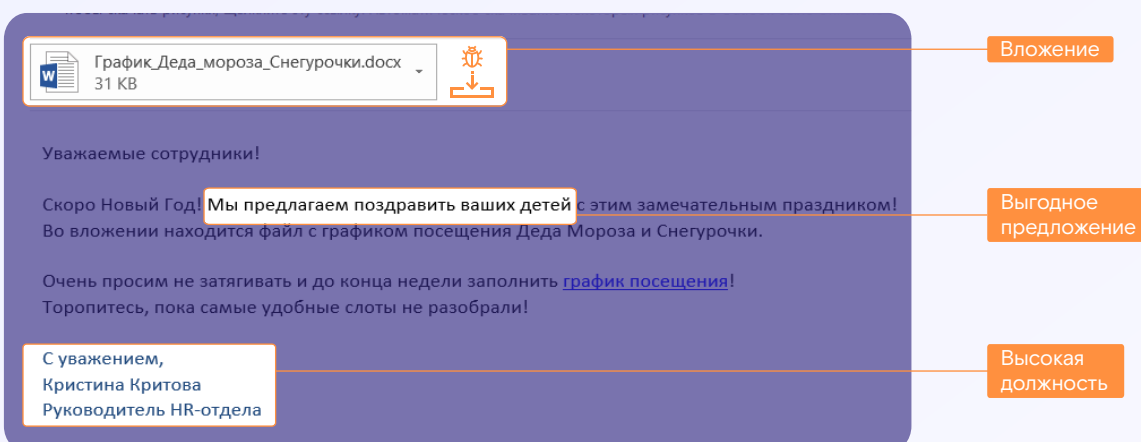
- Поддельный домен в адресе отправителя. Отображаемый адрес можно легко изменить и подделать.
- Подменный адрес ссылки. Для проверки ссылки наведите на нее курсор и посмотрите в нижнюю часть экрана или открывающуюся панель. Сайт www.google.com, www.yandex.ru или сайт вашей компании с парой лишних символов в доменном имени — признак мошенников.



При подозрении на фишинг перешлите письмо в службу информационной безопасности или ИТ-отдел.

Будьте внимательны, если в письме присутствует:

- Вложение. Даже если формат файла выглядит безопасным (html, pdf, docx), он может иметь вредоносное содержимое.
- Выгодное предложение, подарочный сертификат. В письме может быть призыв оплатить небольшую комиссию, чтобы получить приз.
- Высокая должность. Отправитель выдает себя за доверенное лицо, указывая солидную позицию.



Не отключайте параметр «Защищенный просмотр», не открывайте вложения и не переходите по ссылкам, если письмо кажется вам подозрительным.

Мошенники часто используют эмоциональные уловки:

- Чувство срочности и жесткие временные ограничения.
- Запугивание и устрашение. Угрозы наложить штраф или заблокировать учетную запись, если вы не перейдете по ссылке.
- Желание помочь. Ложная информация о потере вашим коллегой ценных вещей и просьба дать его прямые контакты.
- Раздражение. Чтобы отписаться от рассылки, вам необходимо перейти по ссылке в письме.



Закройте письмо, успокойтесь и проанализируйте информацию рационально.

Что еще может указывать на фишинг в письме

- Шаблонность письма и приветствие вида: «Дорогой клиент!»
- Использование личной информации о вас: фотографии, видео якобы с вашим участием.
- Подозрительная активность: запрос на смену пароля, если он инициирован не вами.

Сервис управления навыками кибербезопасности

Комплексный подход к обучению и тренингам снижает риски утечки конфиденциальной информации и проникновения киберпреступников в корпоративную сеть.

Сервис Security Awareness поможет вам и вашим коллегам научиться быстро распознавать фишинг и грамотно реагировать на него.



[Узнать больше о том, как снизить риски фишинга](#)