АНТИТЕРРОР
УРАЛ

Основные приемы фишинга

- Рассылка поддельных электронных писем от имени популярных брендов, банков или государственных органов с вирусными ссылками и файлами

- Распространение поддельных QR-кодов оплаты квитанций или форм регистрации

- Создание копий сайтов, досок объявлений, сервисов поиска услуг, маркетплейсов, интернет-провайдеров, управляющих компаний и банков

АНТИТЕРРОР
УРАЛ

Фишинг*

распространенный вид интернет-мошенничества, целью которого является получение доступа к личным данным для последующей кражи средств

Мошенники посредством манипуляций убеждают пользователей перейти по поддельным ссылкам и сайтам, чтобы завладеть их паролями, данными банковских карт и получить доступ к цифровым сервисам

*термин произошел от англ.fishing – «рыбалка»

АНТИТЕРРОР
УРАЛ

Как распознать обман?

- **Email-адрес содержит лишние символы,** ошибки или ранее вам не встречался

- **Поступают просьбы ввести логин, пароль,** а также предложения перейти по сомнительным ссылкам

- **Присутствует обезличенное обращение** или подпись в конце письма. Остерегайтесь слов «Уважаемый сотрудник», «Дорогой друг» и т.д.

- Прикрепленная в письме ссылка имеет сокращенный вид или **начинается с http вместо https**

- **Имеются ошибки в словах и названиях брендов.** Мошенники намеренно совершают орфографические ошибки, чтобы обойти спам-фильтры

АНТИТЕРРОР
УРАЛ

Как мошенники обманывают своих жертв?

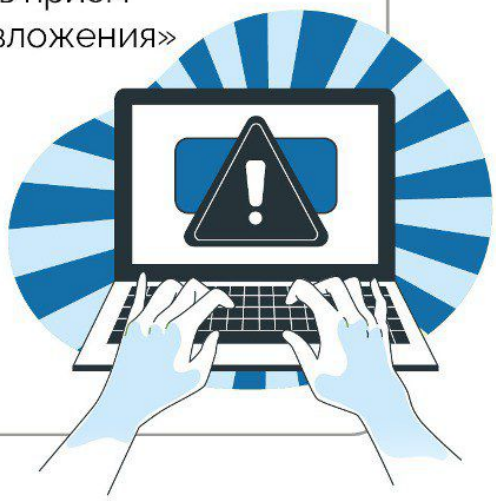
Чтобы заставить вас пройти по ссылке или скачать файл, мошенники входят в доверие с помощью приемов социальной инженерии:

- копируют манеру общения руководителя, коллег, представителей власти, правоохранительных органов
- дублируют аккаунты в мессенджерах
- используют для рассылки адреса электронных почт, схожие с оригинальными
- апеллируют к поручениям авторитетных лиц
- торопят жертву, чтобы не дать возможности и опомнится. Остерегайтесь слов «срочно», «немедленно», «прямо сейчас»
- угрожают блокировкой или списанием средств
- просят передать конфиденциальные сведения: пароли, личные данные, финансовые реквизиты, просят открыть доступ к корпоративным системам

АНТИТЕРРОР
УРАЛ

Как защитить себя от утечки данных?

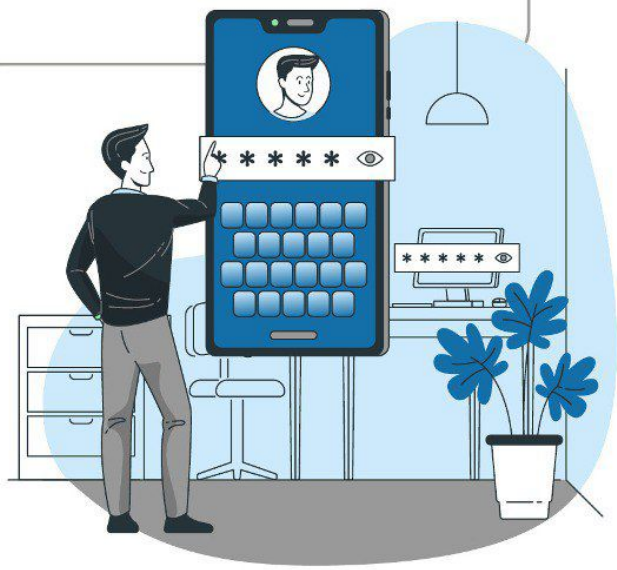
- Не переходите по подозрительным ссылкам, не скачивайте и не открывайте незнакомые файлы
- Установите и регулярно обновляйте антивирусную программу
- Внимательно относитесь к переписке с незнакомыми
- Заведите отдельную почту для регистрации на сервисах и оформления подписок
- Регулярно меняйте пароли на новые и более сложные. Не используйте единый пароль для всех аккаунтов.
- В настройках почты включите «запретить прием сообщений, содержащих исполняемые вложения»
- Не храните в почте пароли и копии личных документов
- Никому не сообщайте реквизиты банковской карты, включая трехзначный код с обратной стороны, а также ПИН-коды и СМС от банка



АНТИТЕРРОР
УРАЛ

При фишинговой рассылке по электронной почте мошенники часто маскируют вредоносные файлы и ссылки под:

- уведомления об оплате онлайн-сервисов
- сообщения от портала Госуслуги
- письма от сервисов доставки
- письма от туроператоров
- уведомления о проблемах с учетной записью от техподдержки
- предложения пройти опрос или получить выигрыш



АНТИТЕРРОР
УРАЛ

Куда обратиться, если вы стали жертвой мошенников?

- Обратитесь в **отдел полиции по месту жительства** или через форму на официальном сайте **Министерства внутренних дел Российской Федерации** **https://мвд.рф/request_main**

- Подать жалобу о вредоносном ресурсе можно в информационной системе мониторинга фишинговых сайтов **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации** **https://paf.occsirt.ru/**

- Обратиться за бесплатной юридической помощью вы можете в **Центр правовой помощи гражданам в цифровой среде Роскомнадзора** **https://4people.grfc.ru**