ФИШИНГ

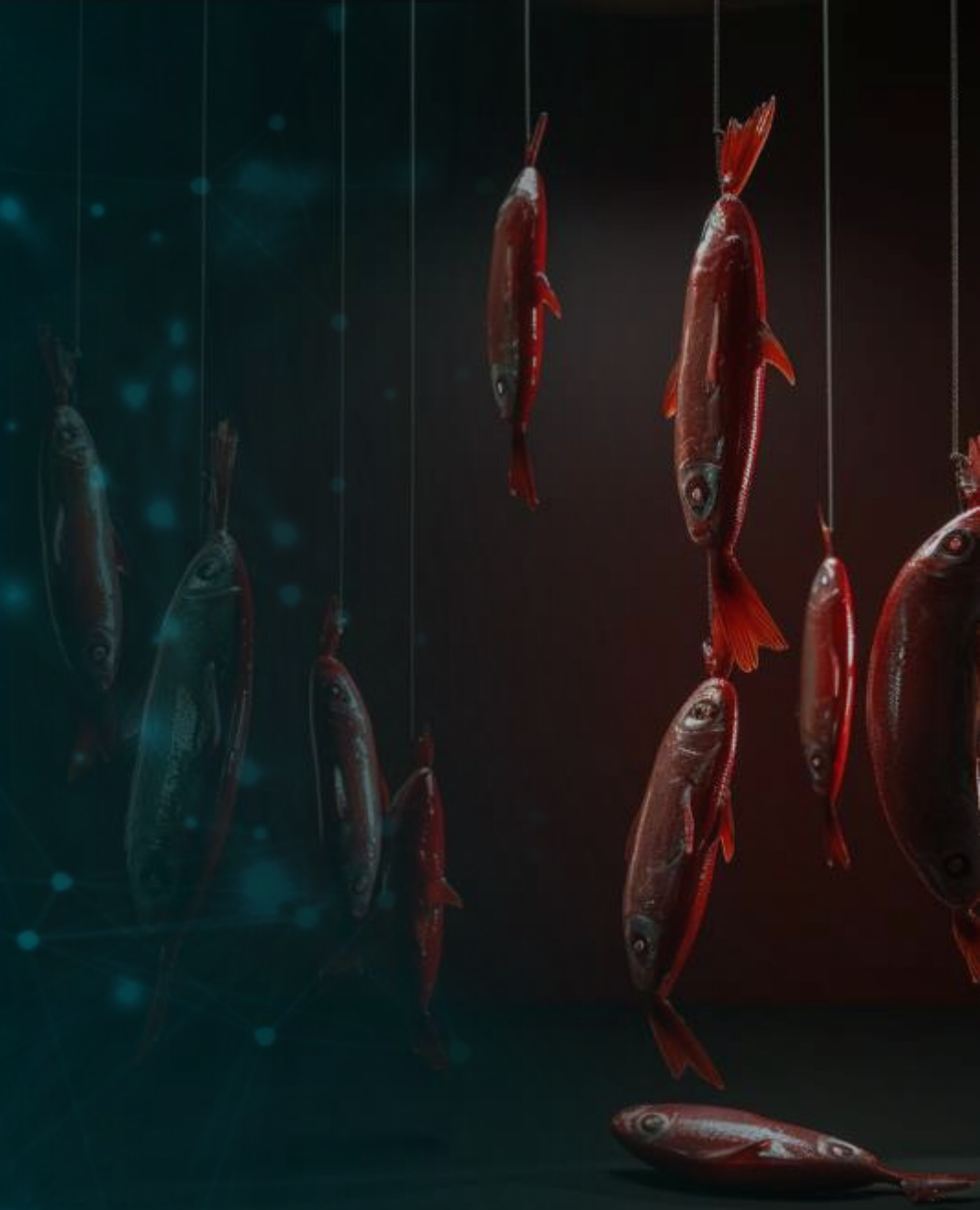
Фишинг – это...

…**вид мошенничества**, при котором злоумышленники рассылают письма и пытаются обманом заставить получателей совершить какое-то действие:

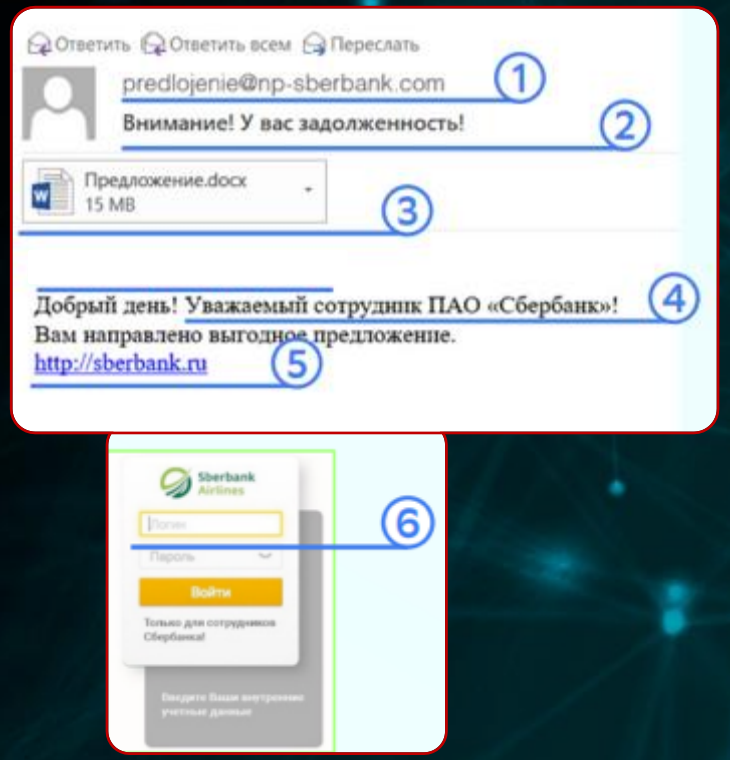
- перейти по вредоносной ссылке
- загрузить зараженное вложение
- сообщить персональные данные и иную конфиденциальную информацию

С английского «phishing» – созвучно с «fishing» (рыбалка)

Фишинговое письмо — письмо, которое содержит вредоносное вложение или ссылку
на мошеннический сайт



Основные признаки фишингового письма



1

Обращайте внимание на почтовый домен

Мошенники обычно используют общедоступные домены gmail.com, mail.ru
и т.п., или домены, похожие на официальные имена компаний (напр. sberbankc[.]ru, 1c-sberbank[.]com и т.д.)

2

Изучите тему. Контент письма и название файлов

Побуждают вас к немедленному действию.
Обращайте внимание на грамотность письма

3

Будьте осторожны с вложениями

Открывайте только те, которые ждали.
Проверьте расширение вложения.

4

Обращайте внимание на обращение и подпись

Если они являются безличными, или есть признак автоподстановки в обращении,
то высока вероятность фишинга

5

Не переходите по ссылкам, не кликайте на подозрительные объекты.

Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании

6

Письмо требует ввода данных

(логина, пароля) на подозрительных сайтах или в анкетных формах

security team
#SBERTEAM

Какие уловки используют злоумышленники в письмах

Службы доставки

Маркетплейсы

Туроператоры и отдых

Криптовалюта

Горячие новости

Билеты на мероприятия

Лотерии

Дополнительный заработок и инвестиции

Подписки и онлайн-сервисы

Как защититься от фишинга

Обращайте внимание
на домен

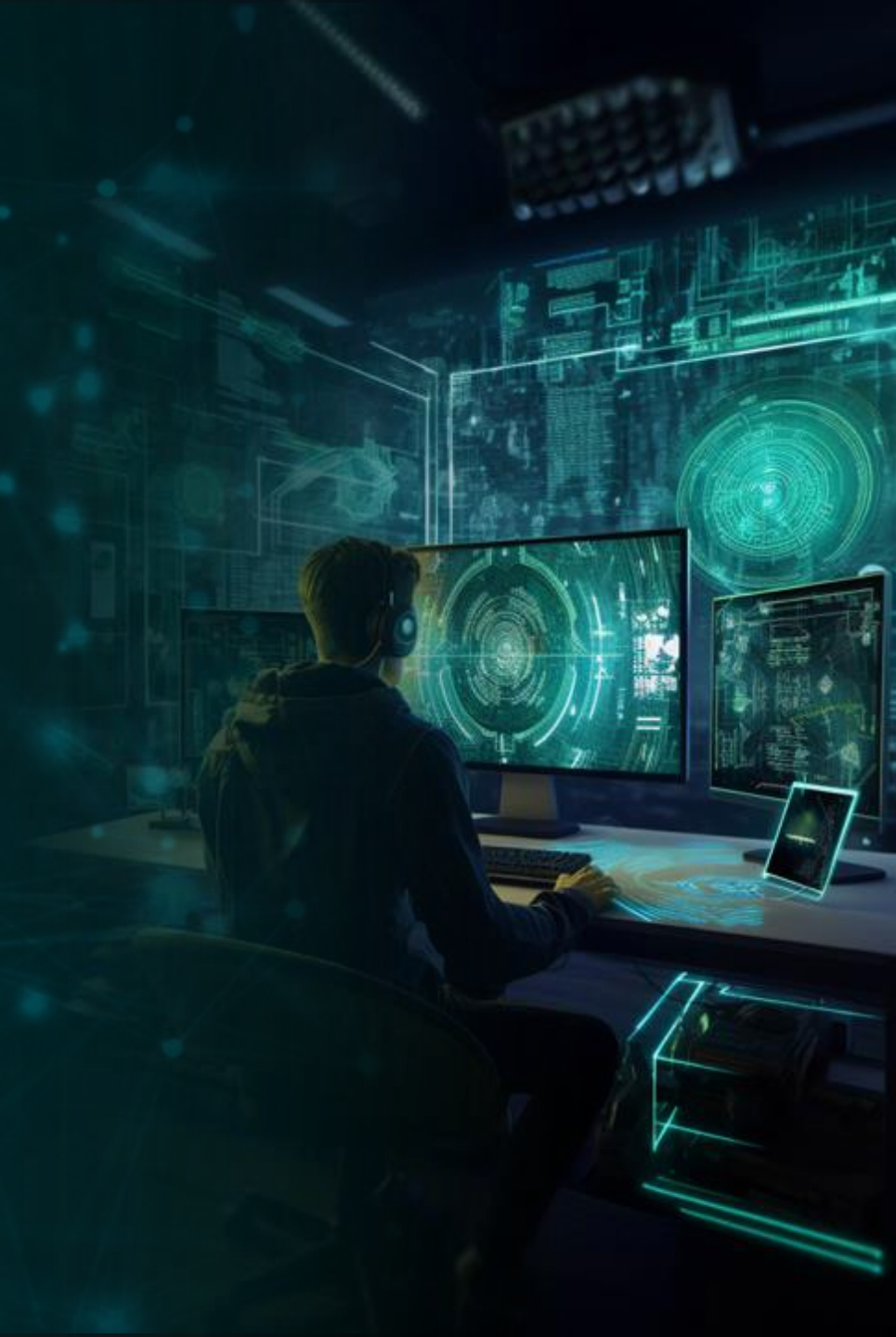
Обращайте внимание
на обращение и подпись

Внимание: побуждение
к немедленному действию

Не переходите по ссылкам,
не кликайте на подозрительные объекты.

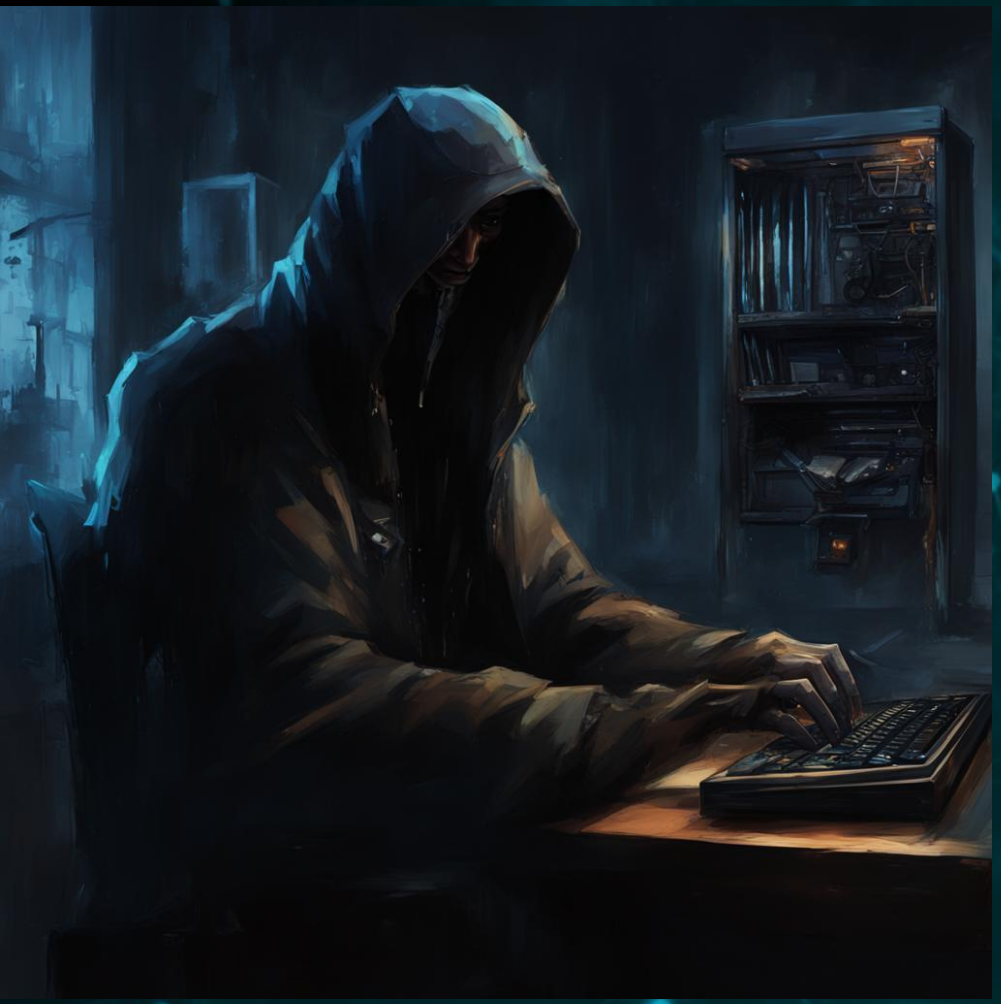
Будьте осторожны
с вложениями

Не вводите свои данные
и не отвечайте
на подозрительные письма



security team
#SBERTEAM

Как вычислить поддельные сайты



Как распознать поддельный сайт?

- ✓ **Проверьте адрес сайта, который указан на верхней строке браузера, убедитесь, что он начинается с английских букв и знаков «https://» и имеет пиктограмму замка, которая гарантирует безопасную передачу информации.**
- ✓ **Проверьте доменное имя сайта, возможно обнаружите замену одной буквы на другую или дополнительный символ.**
- ✓ **Обратите внимание на дизайн сайта и его содержание. Поддельный сайт, как правило, имеет некачественный дизайн и грамматические ошибки в текстах.**
- ✓ **Попробуйте найти информацию о сайте в поисковых системах, например, «Яндекс», «Гугл» или на официальных форумах. Обычно люди делятся своим опытом попадания на мошенников и предупреждают о поддельных сайтах.**

Как распознать поддельный сайт?

- ✓ **Сравните цены на товар и условия продажи на нескольких сайтах. Слишком низкая цена -признак, отличающий мошенников.**
- ✓ **Если веб-сайт представляет собой онлайн-магазин или компанию, убедитесь, что на нем представлены наименование юридического лица или индивидуального предпринимателя, адрес регистрации и фактический адрес организации, реквизиты расчетного счета.**
- ✓ **Настоящие сайты обычно имеют дополнительные функции безопасности, такие как возможность создания пользователем учетной записи с логином и паролем, опции настройки приватности, позволяющие задать правила и ограничения для доступа к персональным данным. С их помощью пользователь может выбирать, кому открывать информацию или ограничивать доступ к ней различными способами.**

СПАСИБО!

security
team
#SBERTEAM