СБЕР

КИБЕРБЕЗОПАСНОСТЬ: КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Основные виды финансового мошенничества

Телефонное мошенничество

Интернет-мошенничество

СБЕР

Что нужно мошенникам

Ваши данные

Ваши деньги

Социальная инженерия

- это манипулирование людьми, в том числе психологическое, чтобы заставить их совершить определённые действия или сообщить конфиденциальную информацию

«Взломай» человека – взломаешь всё остальное

Злоумышленники используют...

СБЕР

Страх

Неосведомленность

Невнимательность

Доверие

Жадность

Сочувствие

Телефонное мошенничество

СБЕР

Эволюция уловок

- **2004 -2012** Звонки от «родственников» и «праздничные акции» для выманивания денег на сим-карту
- **с 2012...** Начало эры звонков от «службы безопасности»

•2021

Предлоги:

Перевод средств на «безопасный счёт»

Цели:

Сбережения

•2024

Предлоги:

Перевод средств на «безопасный счёт»

Продление договора

Помощь близкому

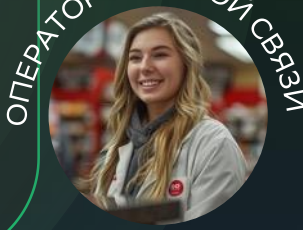
Дополнительный заработок

Цели:

Сбережения Кредиты Недвижимость

Хулиганство Акты терроризма

Взлом аккаунта



Что делать, если звонят мошенники

СБЕР

Внимательно проверяйте входящий номер

Не совершайте никаких операций по инструкциям звонящего

Сразу заканчивайте разговор и блокируйте номер при любых сомнениях

Положите трубку и сами перезвоните в организацию, откуда вам якобы звонили

Проверьте, не было ли сомнительных операций за время разговора

Поставьте приложение для фильтрации входящих вызовов

Если вы слышите любые призывы к быстрым действиям, даже под угрозой «страшных последствий» – **сразу прекратите разговор**

Фишинг

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

- перейти по мошеннической ссылке
- загрузить зараженный вирусами файл или другие вредоносные программы
- 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

СБЕР

1

Обращайте внимание на почтовый домен

Мошенники обычно используют домены, похожие на официальные имена компаний (напр. sberbankc[.]by)

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

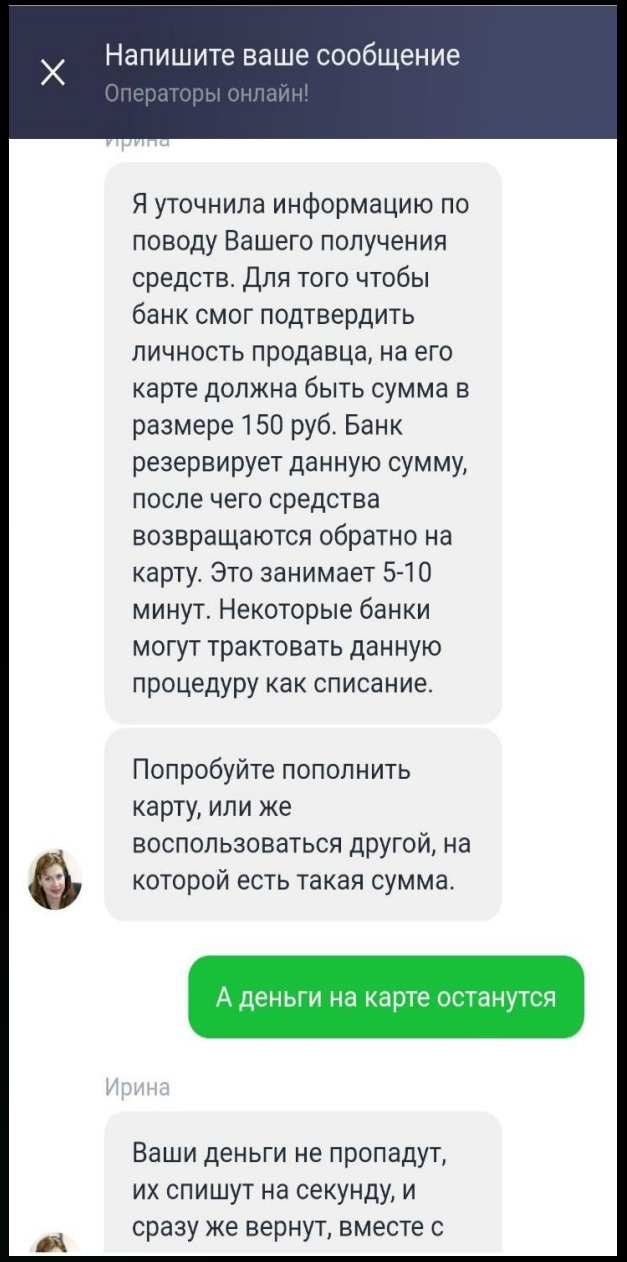
Не переходите по ссылкам, не кликайте на подозрительные объекты.

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

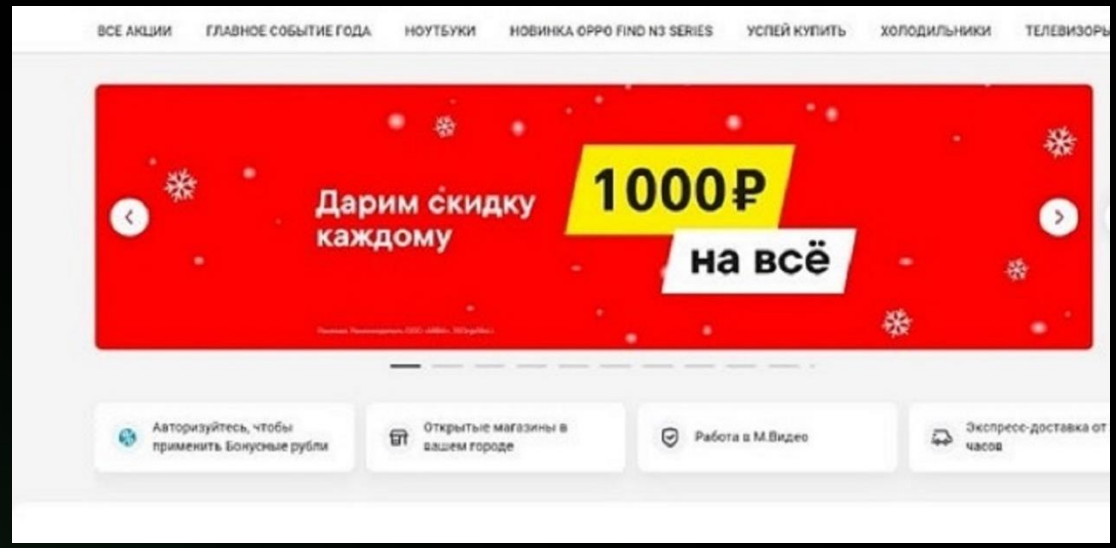
(логина, пароля) на подозрительных сайтах или в анкетных формах



Праздничный фишинг

В преддверии праздников, начала учебного года или отпускного периода мошенники «ловят» доверчивых покупателей на желании сэкономить и создают фейковые сайты онлайн-магазинов с низкими ценами, распродажами и скидками.

Часто имитируются сайты известных магазинов и брендов – и нужно хорошо приглядеться, чтобы заметить «подделку»



Что делать, если есть подозрение на фишинг

СБЕР

Обращайте внимание на домен / адрес, с которого пришло письмо

Внимание: побуждение к немедленному действию

Ошибки и опечатки в письме должны вас насторожить

Не переходите по ссылкам и не нажимайте на кнопки в письме

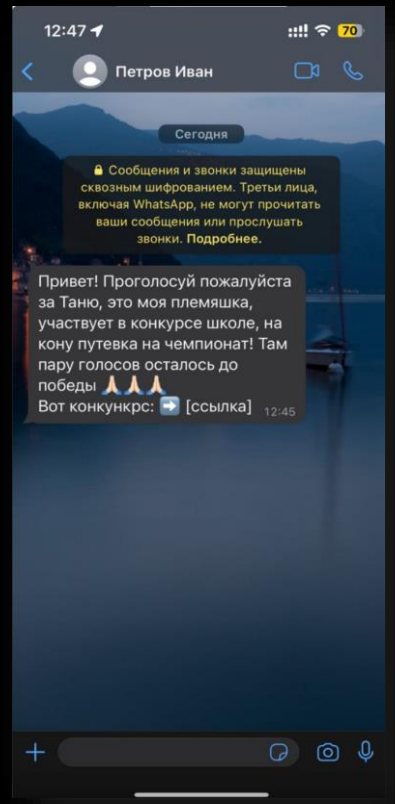
Будьте осторожны с вложениями

Не вводите свои данные и не отвечайте на подозрительные письма

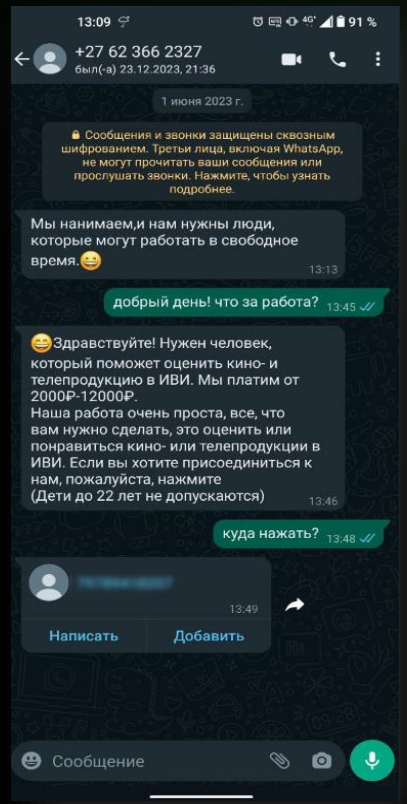
Мошенничество с использованием мессенджеров

Злоумышленники научились активно использовать мессенджеры для социальной инженерии

Просьба проголосовать за родственника

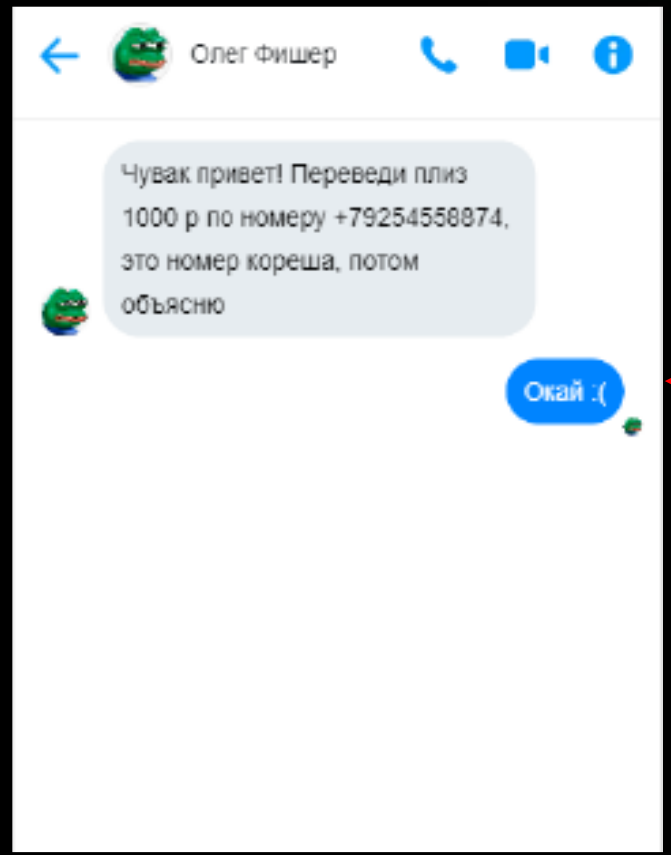


Предложение о работе

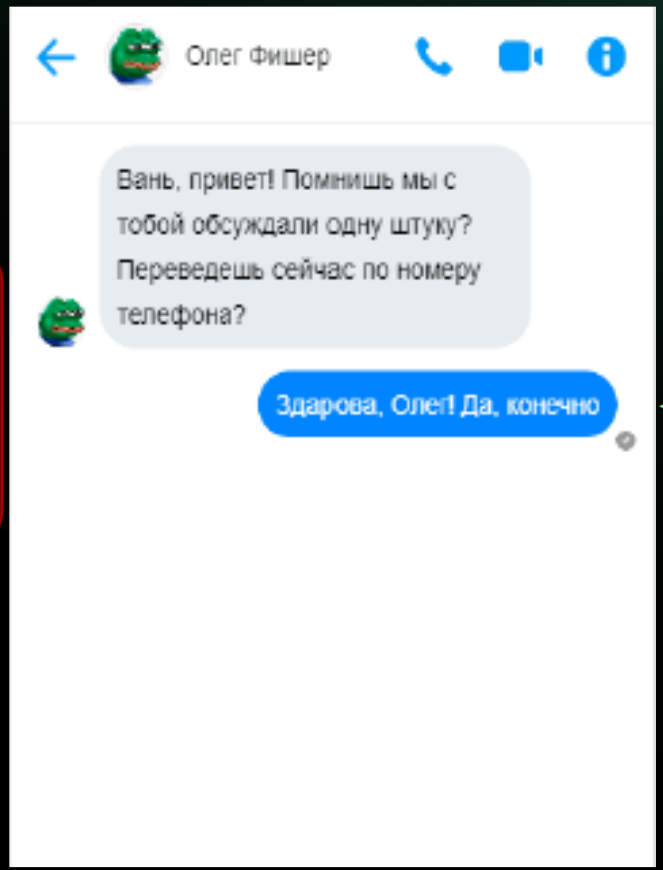


Просьба занять денег

Отличие мошеннических сообщений



- Нетипичный стиль общения для вашего друга
- Просьба совершить действие
- Отсутствие конкретики



- Привычная форма общения
- Есть предмет разговора
- Ожидание сообщения

Причины использования мессенджеров мошенниками

СБЕР

Сложность определения мошенников

Человеку сложно отличить действия мошенника
от действий легитимного пользователя

Дополнительные факторы доверия

Как правило мошенничество происходит
от имени лица, которого вы знаете

Неподготовленность жертв

Это новое явление, с которым
еще не все знакомы

Большой охват пользователей

Практически не осталось людей,
которые не используют
мессенджеры для общения

Наличие чувствительной информации

В переписке могут храниться
конфиденциальные данные
пользователей

Как защититься

Установите надёжный пароль
Пароль должен состоять из 12 и более знаков, а также содержать строчные и прописные буквы, цифры и символы

Проверьте настройки конфиденциальности и приватности
Каждая социальная сеть имеет свой набор настроек для усиления безопасности вашей страницы

Используйте только официальные приложения социальных сетей

Не указывайте в профиле больше личных данных, чем это нужно

Включите двухфакторную аутентификацию
Второй фактор защиты вашего аккаунта (одноразовы пароль, биометрические данные) позволяет защитить ваши данные надежнее, чем только пароль

Не переходите по подозрительным ссылкам
В сообщениях и комментариях, даже если они отправлены от ваших друзей

Ведя переписку с кем-либо,
убедитесь в том, что адресат – действительно тот, за кого себя выдает

Вредоносные программы

-Программы, намеренно разработанные и внедряемые для выполнения несанкционированных и зачастую вредоносных действий

Компьютерные вирусы, черви, программы-вымогатели, шпионское ПО и другое – это все вредоносные программы, способные нанести вред вашим компьютерам, смартфонам, личной и конфиденциальной информации, сбережениям

К примеру, для заражения Android-устройства злоумышленники распространяют файлы с расширенным .apk. Достаточно открыть его и запустить, чтобы началась распаковка и установка на мобильное устройство

Базовые правила

- ✓ В любой ситуации сохраняйте спокойствие и бдительность
- ✓ Если вас запугивают, обещают выгоду или торопят – это мошенники
- ✓ Положите трубку, удалите подозрительное сообщение
- ✓ Перезвоните в банк или другую организацию по официальному номеру телефона и проясните ситуацию
- ✓ Обращайтесь за помощью к близким – даже если вас просили сохранять конфиденциальность

«Никогда не разговаривайте с неизвестными»

М. А. Булгаков
«Мастер и Маргарита»

… и тем более не сообщайте им личные данные, номера карт и пароли

Будьте бдительны!