Банк России

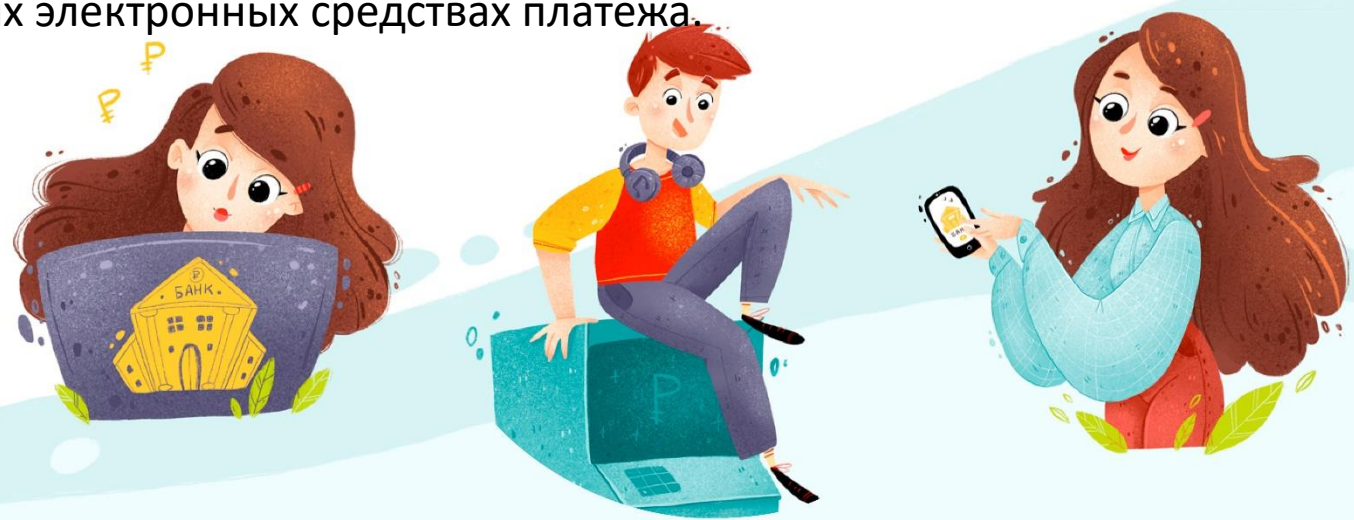
КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА.

ПРАВИЛА БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ.

Банк России

СЕГОДНЯ НА УРОКЕ ВЫ УЗНАЕТЕ:

- Какие виды мошенничества существуют в сети Интернет.
- Способы похищения злоумышленниками конфиденциальной информации о вас и ваших электронных средствах платежа.
- Какие приемы социальной инженерии используют мошенники, чтобы завладеть вашими денежными средствами.



Банк России

ЧТО ТАКОЕ КИБЕРПРОСТРАНСТВО?

Интерактив.

Напишите ответ в чат

КИБЕРПРОСТРАНСТВО-ЭТО…

Среда информационного взаимодействия и обмена данными в компьютерных сетях и сетях связи.

Элементы киберпространства:
серверы, компьютеры, мобильные гаджеты, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети.

СВОЙСТВА ИНФОРМАЦИИ

Банк России

- **КОНФИДЕНЦИАЛЬНОСТЬ -** информация может быть получена и обработана только теми лицами или процессами, у которых есть к ней доступ.
- **ЦЕЛОСТНОСТЬ-** информация остается неизменной, корректной и аутентичной.
- **ДОСТУПНОСТЬ -** авторизованные субъекты (допущенные к получению и обработке информации) имеют к ней беспрепятственный доступ.

Банк России

КАКОЕ СВОЙСТВО ИНФОРМАЦИИ ГАРАНТИРУЕТ, ЧТО ДОСТУП К ИНФОРМАЦИИ ИМЕЮТ ТОЛЬКО ОПРЕДЕЛЕННЫЕ ЛИЦА?

1. Доступность
2. Конфиденциальность
3. Целостность

Интерактив.
Напишите ответ в чат

ВИДЫ ВРЕДОНОСНОГО ПО

Банк России

- **Троян** – проникает в систему под видом полезной утилиты, но вместе с этим скрытно ведет и разрушающую деятельность.
- **Вирусы** – это самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя.
- **Червь** – программа, которая саморазмножается, она добавляется в систему отдельным файлом и ищет уязвимости для своего дальнейшего распространения.
- **Руткиты** – программа или набор программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного ПО.

ЧТО НЕЛЬЗЯ ДЕЛАТЬ ПОЛЬЗОВАТЕЛЮ …

- Переходить по подозрительным ссылкам в электронной почте или в браузере.
- Открывать подозрительные вложения.
- Скачивать и устанавливать «пиратское» ПО.
- Вставлять непроверенные флешки, смартфоны и др.

ЧТО ДЕЛАЕТ ЗАРАЖЕННЫЙ КОМПЬЮТЕР

- Похищает информацию.
- Участвует в атаках.
- Нарушает свойства информации – конфиденциальность, целостность, доступность.

БЛОКИРОВКА КОМПЬЮТЕРА

Банк России

Включаете компьютер и видите объявление, что все ваши файлы зашифрованы, чтобы их вернуть, нужно перевести деньги на указанный кошелек.

Нарушается целостность информации.

Банк России

КАКИЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРОВ И СМАРТФОНОВ НАРУШАЮТ ПРАВИЛА БЕЗОПАСНОСТИ И СТАВЯТ ПОД УГРОЗУ СВОЙСТВА ИНФОРМАЦИИ?

1. Использование чужих устройств для входа в мобильный банк, Интернет-банк, покупок в Интернете и сохранение на них личных данных.
2. Проверка флэшек на наличие опасных программ.
3. Переход по подозрительным ссылкам.
4. Немедленное отключение всех услуг при утрате телефона или планшета, к которым подключено смс-информирование или мобильный банк.

1, 4

1, 3

2, 3

Интерактив.
Напишите ответ в чат

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Банк России

Мошенникам **нужны:**

БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ

Банк России

- высокая скорость выполнения платежной операции
- удобство для операций **до 1000** рублей - можно не вводить пинкод
- карту украли, пользуются ею в магазинах **до 1000** руб. без ПИН-кода
- возможны мошенничества с платежными терминалами *(считывающие устройства на расстоянии)*

Рекомендации: установить суточный лимит и смс уведомления

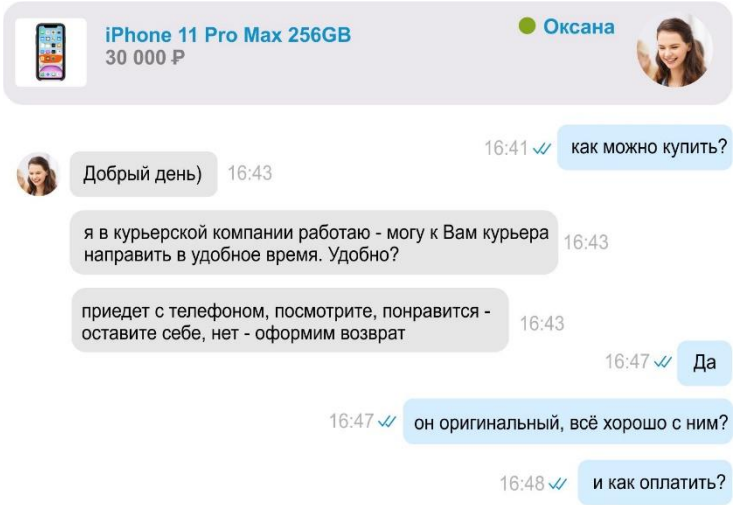
ФИШИНГ- ЭТО…

Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей и их деньгам.

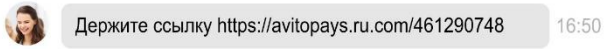
ПРИМЕРЫ ФИШИНГА

Банк России

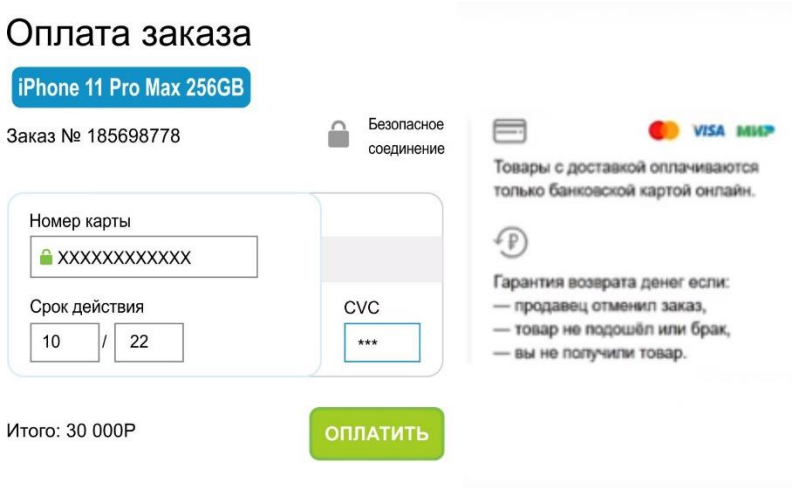
1. Общение с «продавцом»



2. Ссылка на фишинговый ресурс для оплаты



3. После «оплаты заказа» продавец пропадёт



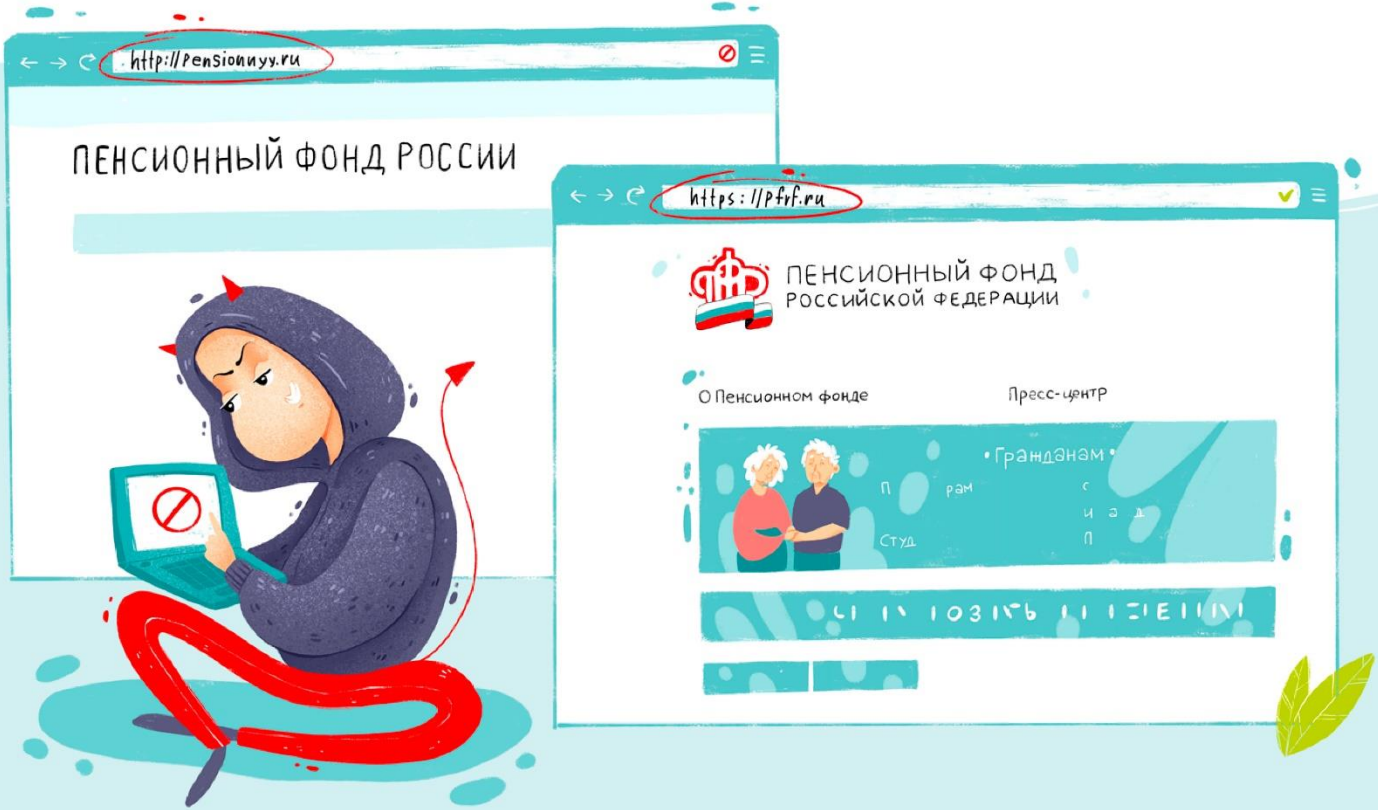
КАК ОБОЙТИ ПРОБЛЕМУ?

Банк России

- Не соглашаться на предоплату.
- Игнорировать объявления с ценой значительно ниже рыночной.
- Общаться с продавцом или покупателем исключительно на сайте с объявлением.
- Не открывать ссылки, которые вам может прислать продавец или покупатель.
- Использовать функцию «безопасная сделка» (по возможности).

ПРИМЕРЫ ФИШИНГА

Банк России



ВИДЫ МОШЕННИЧЕСТВА ПО ЭЛЕКТРОННОЙ ПОЧТЕ И В СОЦИАЛЬНЫХ СЕТЯХ

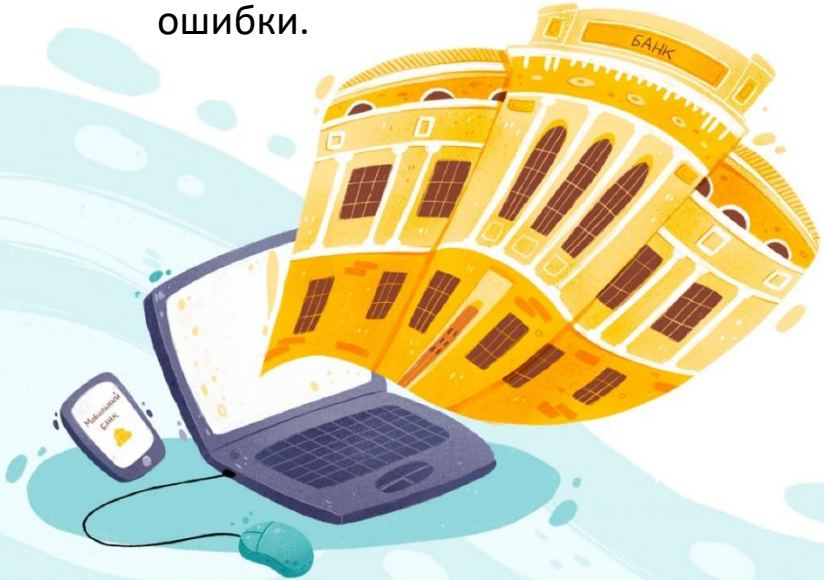
Банк России

- **Обещание социальных выплат.** «Вам положены деньги от государства! Перейдите по ссылке, чтобы узнать подробности»
- **Вознаграждение за участие в опросе!** Мошенники предлагают внести деньги за участие в опросе и только после этого обещают перечислить выигранные деньги.
- **Предложение купить товар с большой скидкой!**
- **Сообщение о выигрыше товара или лотереи!**

ПРИЗНАКИ ФИШИНГОВОГО САЙТА

Банк России

- Если организация представляется как финансовая, но информация о ней отсутствует в реестрах Банка России.
- Используется подозрительное доменное имя или адрес сайта содержит явные ошибки.



- **На сайте организации:**
  - информация об организации недостоверная или принадлежит другой организации;
  - грамматические, орфографические и дизайнерские ошибки;
  - размещены предложения товаров или услуг, чья цена значительно ниже рыночной;
  - предлагается пройти опрос, тест и т.п. за денежное вознаграждение или оформить какую-либо компенсационную выплату от государства или государственного органа.

КАК ПОСТУПИТЬ?

Банк России

Вы увидели в интернете рекламу знакомого онлайн-магазина, который предлагает модный смартфон по низкой цене. Перейдя по ссылке из рекламы, заметили, что дизайн сайта изменился, в его адресе и описании товаров есть ошибки.

1 Похоже на фишинг – сайт создан мошенниками, чтобы выманить секретные данные пользователей. Вводить свои данные не буду, закрою этот сайт и сообщу о нем в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (info_fincert@cbr.ru) или через Интернет-приемную Банка России (http://cbr.ru/reception/)

2 Вероятно, это новый интернет-магазин: почитаю отзывы покупателей, если они хорошие, то закажу смартфон.

3 Если скидка на смартфон большая и действует всего несколько часов, то не раздумывая, введу свои личные данные, а на этапе оплаты решу, использовать банковскую карту или нет .

Интерактив.

Напишите ответ в чат

Банк России

ТЕЛЕФОННЫЕ МОШЕННИКИ

- Звонок якобы от имени банка или правоохранительных органов: вас просят сообщить личные данные.
- СМС или письмо якобы от банка с просьбой перезвонить.
- СМС об ошибочном зачислении средств или с просьбой подтвердить покупку.
- СМС от имени родственников, которые просят перевести деньги на неизвестный счет.

НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА

- Предложение оформить карту за границей.
- Предложение покупки остатков товаров уходящих брендов.
- Предложения по использованию VPN – сервисов.
- Предложения об инвестициях в криптовалюту.

С МОЕЙ КАРТЫ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

- Позвоните в банк и заблокируйте карту.
- Запросите выписку по счету и напишите заявление о несогласии с операцией.
- Обратитесь в полицию.

Банк России

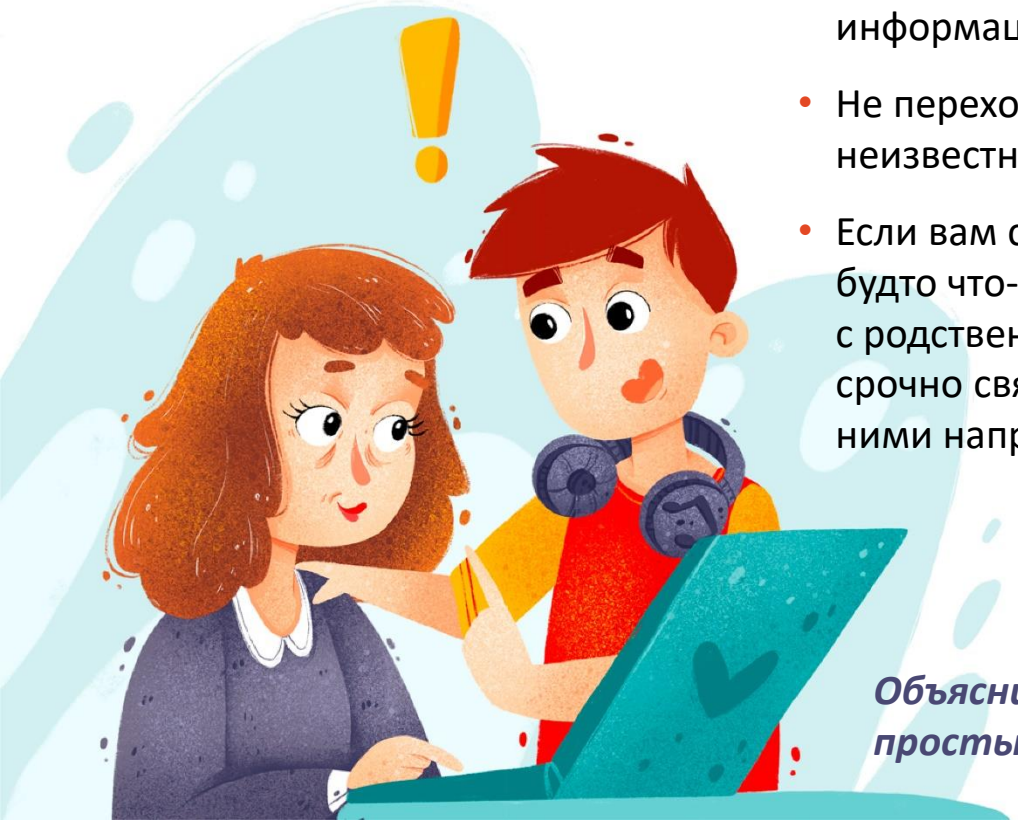
КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ?

Интерактив.

Напишите ответ в чат

СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

Банк России



- Всегда проверяйте информацию.
- Не переходите по неизвестным ссылкам.
- Если вам сообщают, будто что-то случилось с родственниками, срочно свяжитесь с ними напрямую.
- Не перезванивайте по сомнительным номерам.
- Не храните данные карт на компьютере или в смартфоне.
- Не сообщайте никому личные данные, пароли и коды.
- Установите антивирус на компьютер себе и родственникам

Объясните пожилым родственникам эти простые правила и будьте бдительны!!!

Банк России

БАНК РОССИИ – МЕГАРЕГУЛЯТОР ФИНАНСОВОГО РЫНКА

Функции Банка России:

- Защита и обеспечение устойчивости рубля
- Поддержание стабильности и развития финансового рынка
- Защита прав потребителей финансовых услуг и повышение уровня финансовой грамотности населения

Узнайте больше о финансах

Читайте статьи и новости:
fincult.info

Задавайте вопросы:
cbr.ru/reception/

Звоните бесплатно:
8-800-300-3000

Банк России

ДЛЯ ПОЛУЧЕНИЯ СЕРТИФИКАТА УЧАСТНИКА

направляйте отзывы на **basewebinar@fincult.com**

Форму отзыва все участники получат на электронную почту **в течение суток после урока.**

Подписывайтесь на группу «Финансовое просвещение»!

Игры по финансовой грамотности (doligra.ru)

Разнообразьте учебный процесс и досуг детей! Скачайте готовые игры по финансовой грамотности на сайте https://doligra.ru/

Играйте, заполняйте отзыв и получайте сертификат!

В случае возникновения вопросов обращайтесь в службу поддержки проекта: https://dni-fg.ru/help