



Банк России

КАК ЗАЩИТИТЬСЯ  
ОТ КИБЕРМОШЕННИЧЕСТВА.

ПРАВИЛА  
БЕЗОПАСНОСТИ  
В КИБЕРПРОСТРАНСТВЕ.



## СЕГОДНЯ НА УРОКЕ ВЫ УЗНАЕТЕ:

- Какие виды мошенничества существует 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.



# 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



- **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.

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

- 1 Доступность
- 2 Конфиденциальность
- 3 Целостность



*Интерактив.  
Напишите ответ в чат*

## ЭЛЕКТРОННЫЙ БАНКИНГ (E-BANKING)...

оказание банковских услуг с использованием возможностей глобальной сети Интернет и мобильной связи.



- **РС – банкинг**, удаленное управление своим банковским счетом с помощью компьютера
- **мобильный банкинг**, с помощью мобильного телефона или смартфона.
- **POS-терминалы и банкоматы**, с помощью которых мы оплачиваем покупки в магазинах.

# МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам **нужны:**





# БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ



- ✓ 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

## КАК И ГДЕ МОГУТ УКРАСТЬ ВАШИ ДАННЫЕ?



- **В банкомате** — на нем мошенники могут установить скиммер и видеокамеру.
- **В кафе или магазине** — сотрудник-злоумышленник может сфотографировать вашу карту.

## ТАК МОЖЕТ ВЫГЛЯДЕТЬ БАНКОМАТ СО СКИММЕРОМ



# КАК ОБОЙТИ ПРОБЛЕМУ ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ КАРТ?

- Используйте банковскую карту только в тех местах, которые заслуживают доверия.
- Осмотрите банкомат. На нем не должно быть посторонних предметов.
- Набирая ПИН-код, прикрывайте клавиатуру рукой.
- При наборе ПИН-кода вводимые цифры не должны отображаться (\*\*\*\*).
- Подключите мобильный банк и СМС-уведомления.
- Никому не сообщайте секретный код из СМС.
- Не теряйте карту из виду (в магазине, кафе).




## ФИШИНГ - ЭТО...



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




# ПРИМЕРЫ ФИШИНГА

## 1. Общение с «продавцом»

 iPhone 11 Pro Max 256GB  
30 000 P

 Оксана 

 Добрый день) 16:43

16:41 ✓ как можно купить?

я в курьерской компании работаю - могу к Вам курьера направить в удобное время. Удобно? 16:43


приедет с телефоном, посмотрите, понравится - оставите себе, нет - оформим возврат 16:43

16:47 ✓ Да

16:47 ✓ он оригинальный, всё хорошо с ним?

16:48 ✓ и как оплатить?

## 2. Ссылка на фишинговый ресурс для оплаты

 Держите ссылку <https://avitopays.ru.com/461290748> 16:50

## 3. После «оплаты заказа» продавец пропадёт

### Оплата заказа

**iPhone 11 Pro Max 256GB**

Заказ № 185698778

Безопасное соединение

Товары с доставкой оплачиваются только банковской картой онлайн.

Гарантия возврата денег если:  
— продавец отменил заказ,  
— товар не подошёл или брак,  
— вы не получили товар.

Итого: 30 000P

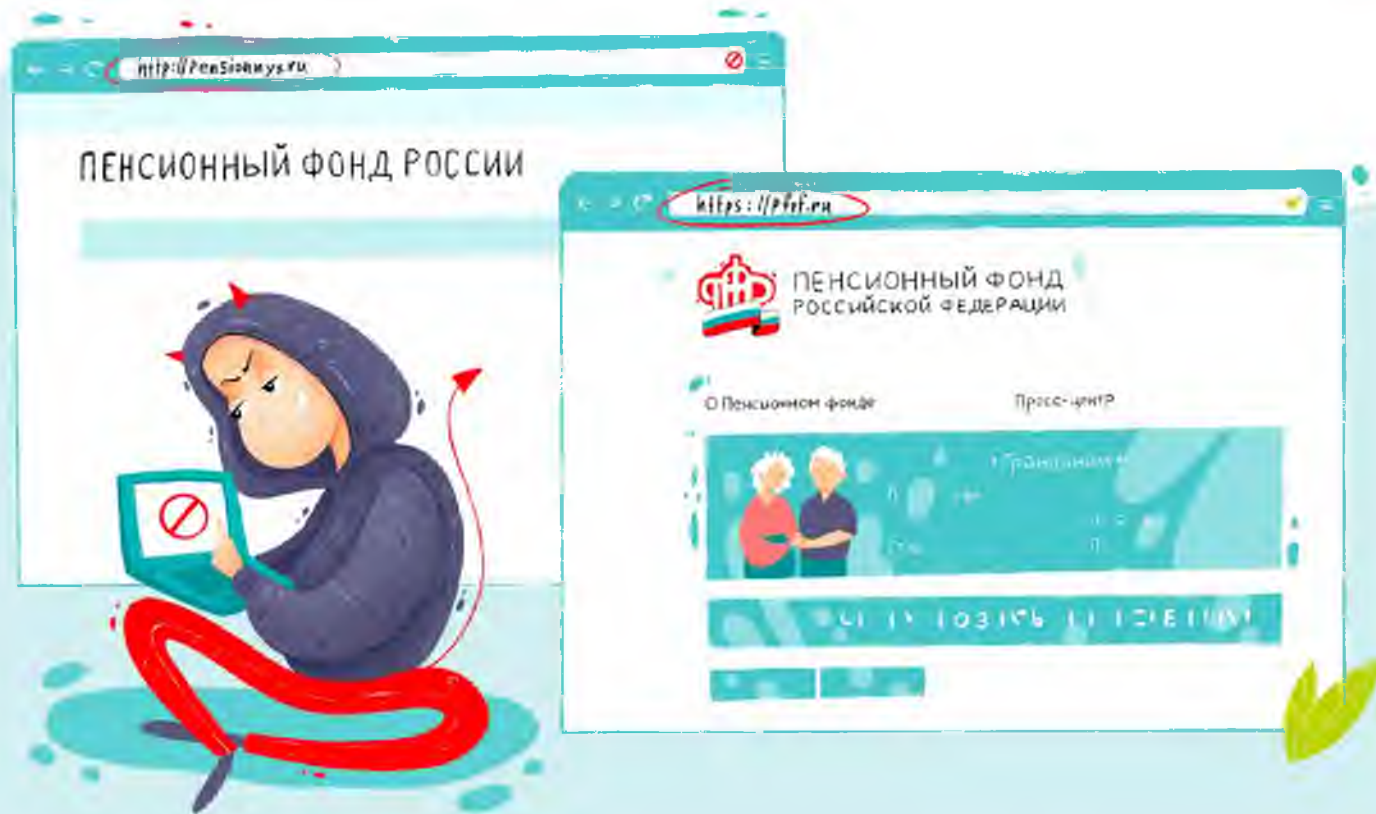
**ОПЛАТИТЬ**

# КАК ОБОЙТИ ПРОБЛЕМУ?

- 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).



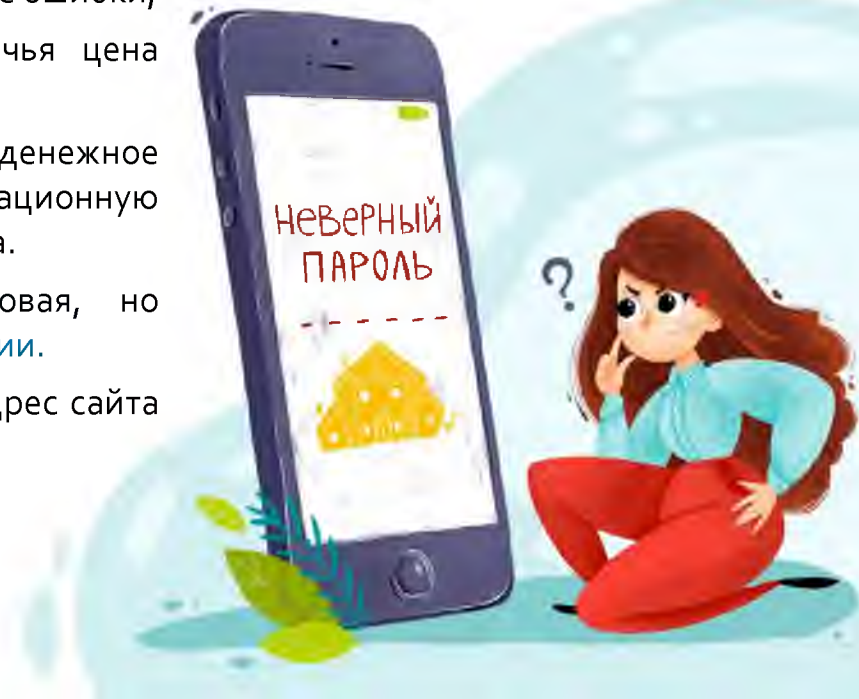
# ПРИМЕРЫ ФИШИНГА





# ПРИЗНАКИ ФИШИНГОВОГО САЙТА

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





## 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.





## 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.

## КАК ПОСТУПИТЬ?

*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: прочитаю 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*



## ВИДЫ ВРЕДОНОСНОГО ПО

- **Троян** – проникает в систему под видом полезной утилиты, но вместе с этим скрытно ведет и разрушающую деятельность
- **Руткиты** – программа или набор программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного ПО.
- **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.



## 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



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

Нарушается целостность информации.



## 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*



# Как не стать жертвой киберпреступников?

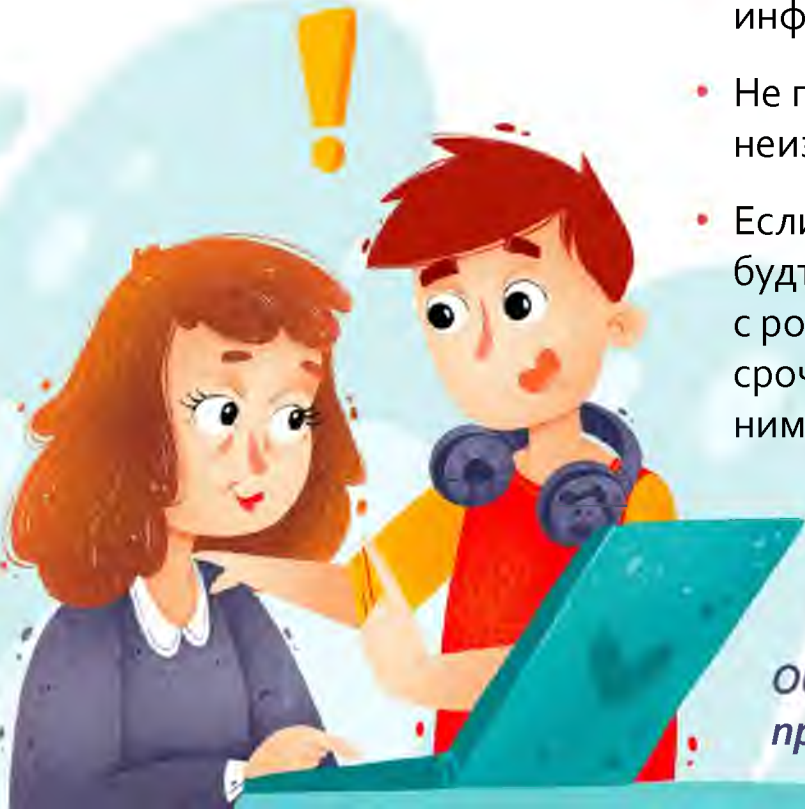


*Интерактив.  
Напишите ответ в чат*

## СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

- 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 – 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](http://fincult.info)



Задавайте вопросы:  
[cbr.ru/reception/](http://cbr.ru/reception/)



Звоните бесплатно:  
**8-800-300-3000**

## Для получения Сертификата участника

направляйте отзывы на

**basewebinar@fincult.com**

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



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

**Подписывайтесь в группы «Финансовое просвещение»!**



finprosvet

**Игры по финансовой грамотности (doligra.ru)**

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



finprosvet



finprosv

Играйте, заполняйте отзыв и получайте  
сертификат!

