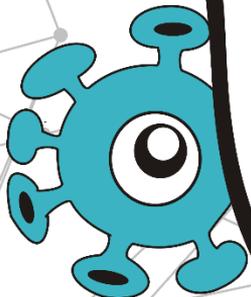
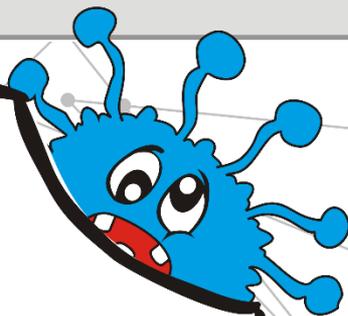
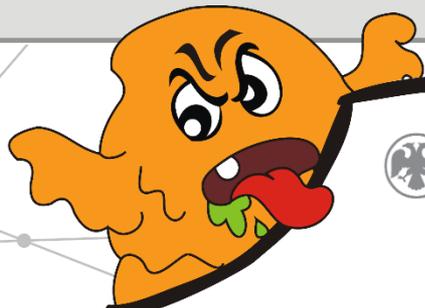




Банк России

**КАК ЗАЩИТИТЬСЯ
ОТ КИБЕРМОШЕННИЧЕСТВА.**

**ПРАВИЛА
БЕЗОПАСНОСТИ
В КИБЕРПРОСТРАНСТВЕ.**



СЕГОДНЯ НА УРОКЕ ВЫ УЗНАЕТЕ:



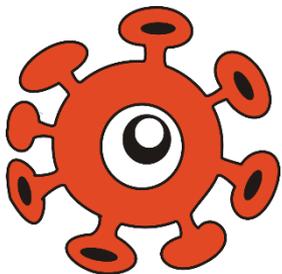
Какие виды мошенничества существует в сети Интернет.



Способы похищения злоумышленниками конфиденциальной информации о вас и ваших электронных средствах платежа.



Какие приемы социальной инженерии используют мошенники, чтобы завладеть вашими денежными средствами.

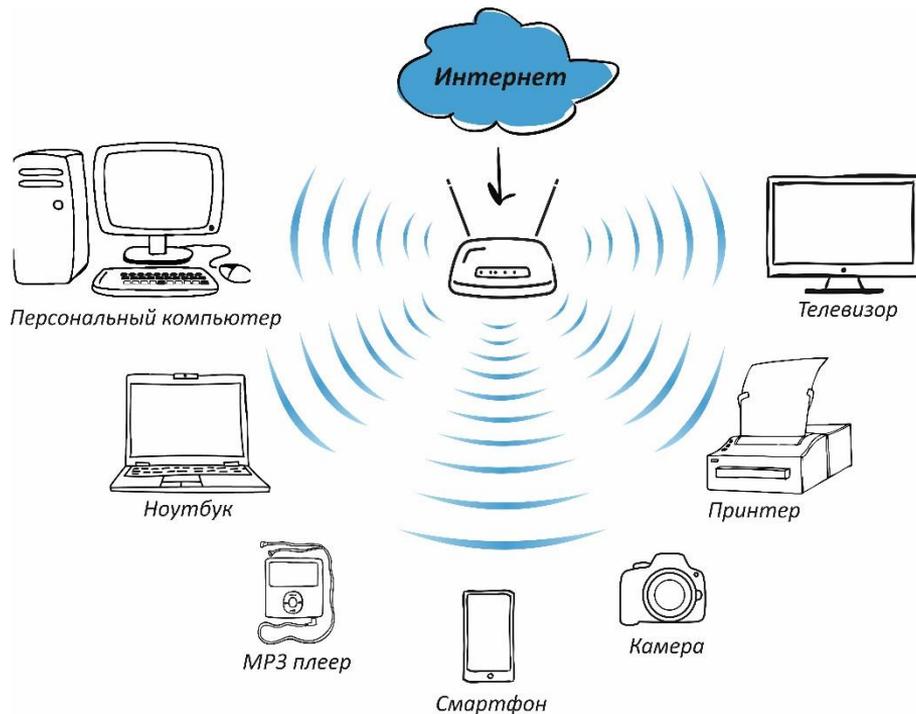


Интерактив

ЧТО ТАКОЕ КИБЕРПРОСТРАНСТВО?

Напишите ответ в чат

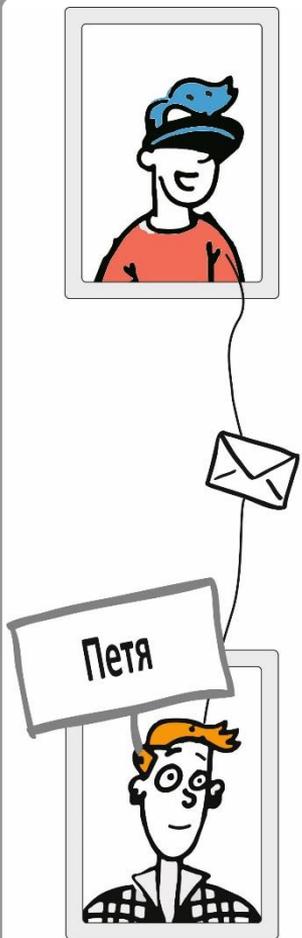




Среда информационного взаимодействия и обмена данными в компьютерных сетях и сетях связи.

Элементами киберпространства являются 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.

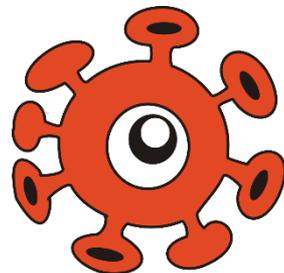
ДОСТУПНОСТЬ - авторизованные субъекты (допущенные к получению и обработке информации) имеют к ней беспрепятственный доступ.



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

1. Доступность
2. Конфиденциальность
3. Целостность

Напишите ответ в чат



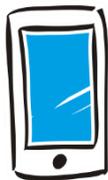
ЭЛЕКТРОННЫЙ БАНКИНГ (E-BANKING)...



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



РС – банкинг, удаленное управление своим банковским счетом с помощью компьютера



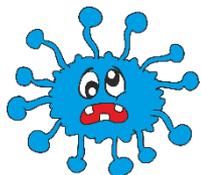
мобильный банкинг, с помощью мобильного телефона или смартфона.



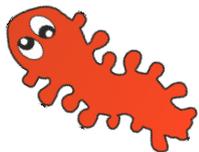
POS-терминалы и банкоматы, с помощью которых мы оплачиваем покупки в магазинах.

*« Нам нужен
банкинг, но не
банки »*

Билл Гейтс, один из создателей
и бывший крупнейший
акционер компании Microsoft



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.



Троян – проникает в систему под видом полезной утилиты, но вместе с этим скрытно ведет и разрушающую деятельность



Руткиты (от англ rootkit, набор программных средств) – 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.



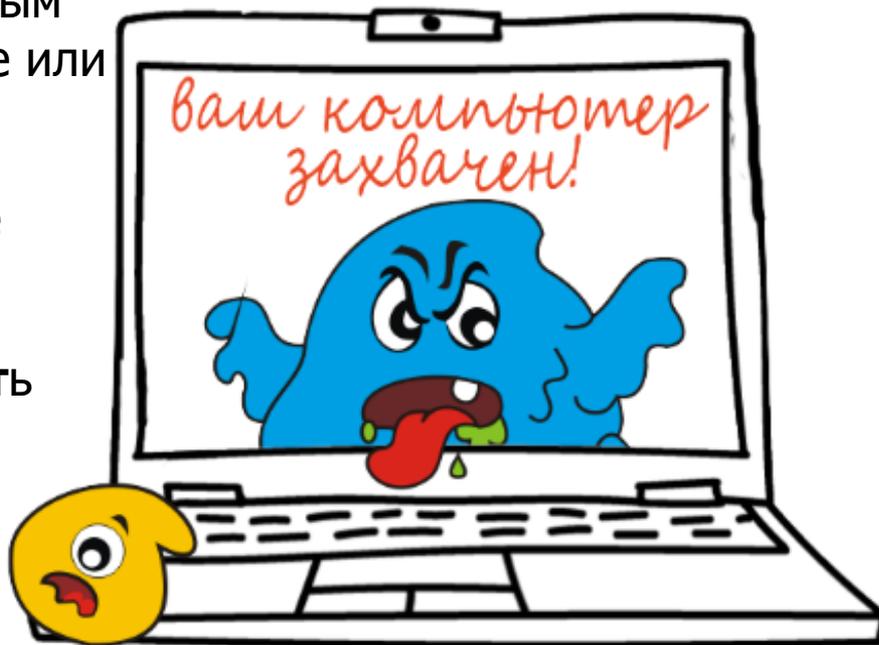
Открывать подозрительные вложения.



Скачивать и **устанавливать** «пиратское» ПО.



Вставлять непроверенные флешки, смартфоны и др.



ЧТО ДЕЛАЕТ ЗАРАЖЕННЫЙ КОМПЬЮТЕР



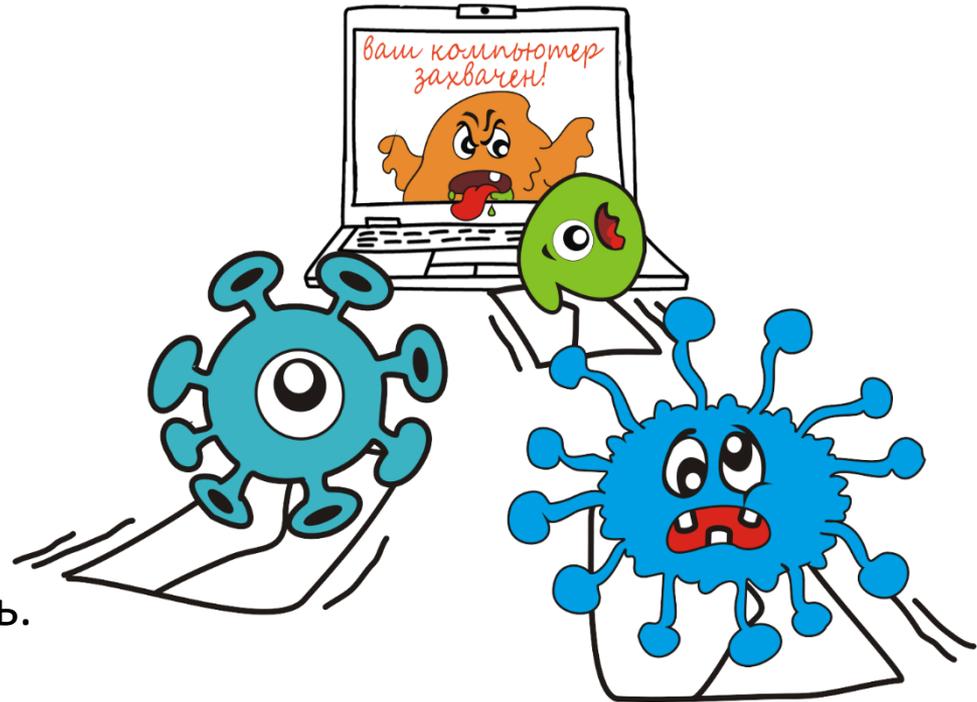
Похищает информацию.



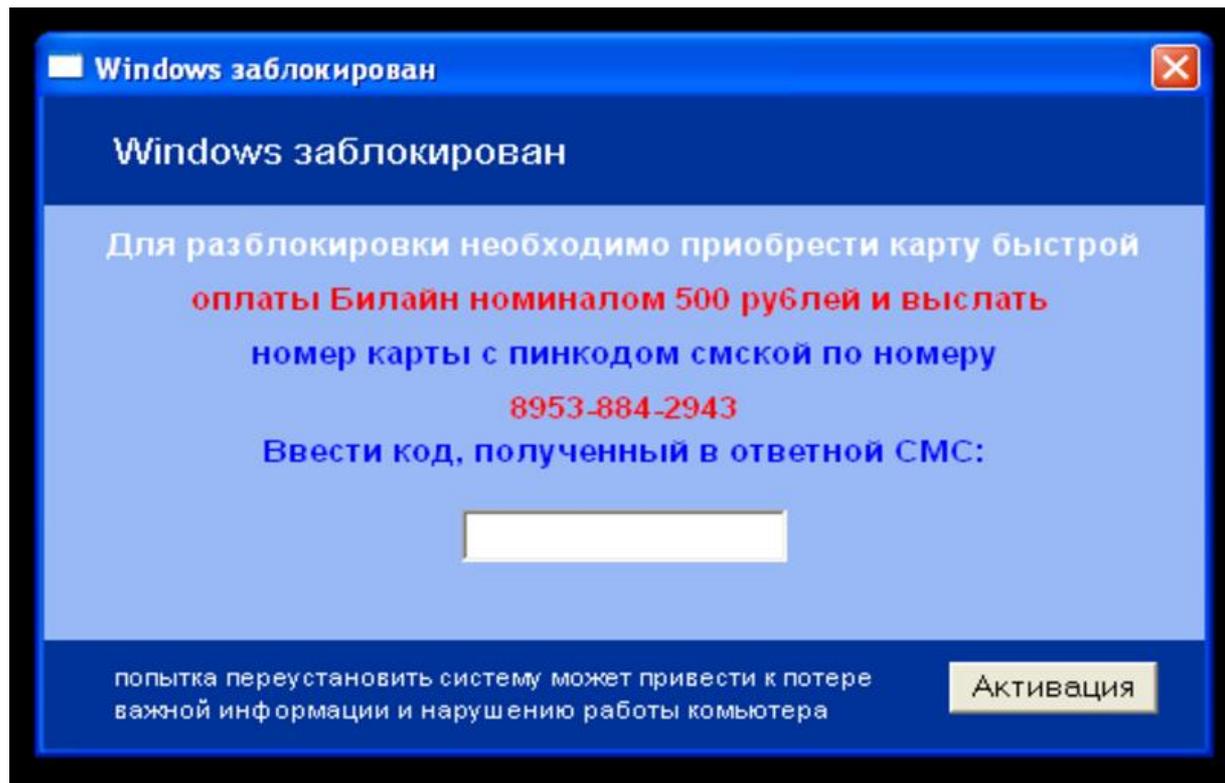
Участвует в атаках.



Нарушает свойства информации – конфиденциальность, целостность, доступность.



ПРИМЕР БЛОКИРОВКИ КОМПЬЮТЕРА



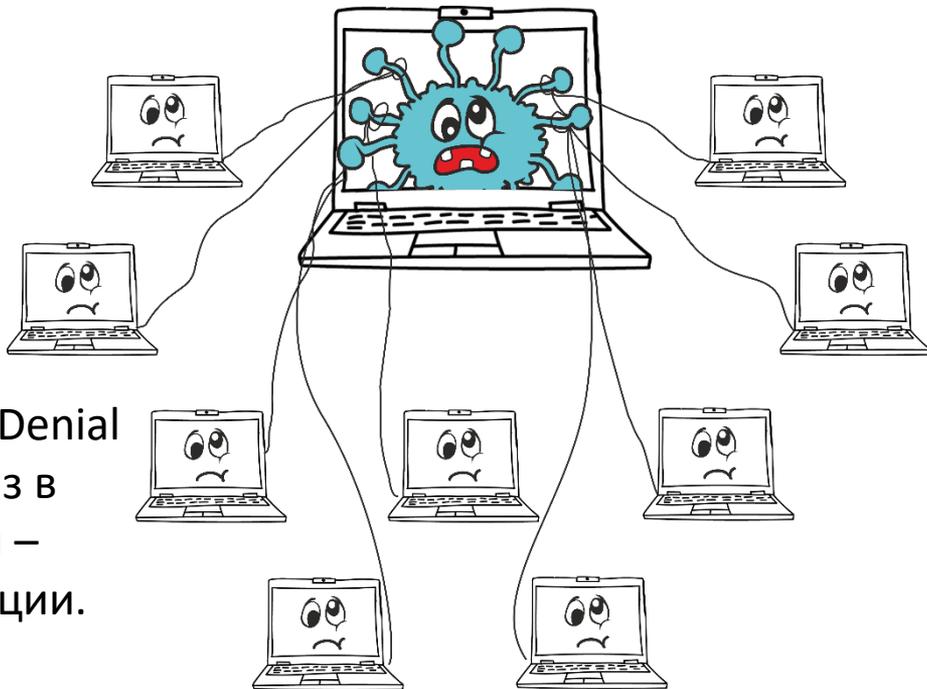
ЗАРАЖЕННЫЙ КОМПЬЮТЕР – ЭТО НЕ ВАШ КОМПЬЮТЕР!



БОТНЕТ – это сеть, состоящая из зараженных компьютеров, которые можно заставить действовать слаженно.



DDoS-атака (от англ. Distributed Denial of Service, распределённый отказ в обслуживании). Цель этой атаки – нарушить доступность 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.

А. 1, 4

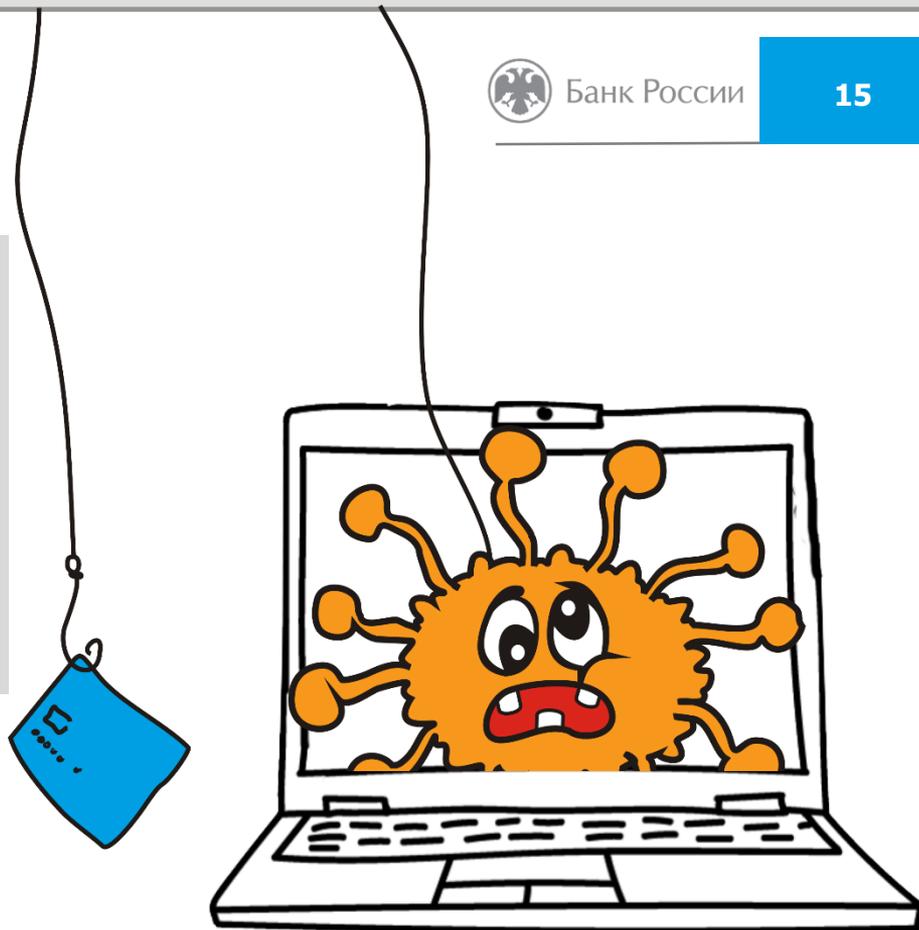
В. 1, 3

С. 2, 3

Напишите ответ в чат

ФИШИНГ- ЭТО...

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



ПРИМЕРЫ ФИШИНГА



Банк России

16

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

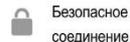
 Держите ссылку <https://avitopays.ru.com/461290748> 16:50

3. После «оплаты заказа» продавец пропадёт

Оплата заказа

iPhone 11 Pro Max 256GB

Заказ № 185698778



Безопасное
соединение

Номер карты	<input type="text" value="XXXXXXXXXXXX"/>	CVC <input type="text" value="***"/>
Срок действия	<input type="text" value="10"/> / <input type="text" value="22"/>	

Итого: 30 000P

ОПЛАТИТЬ



Товары с доставкой оплачиваются
только банковской картой онлайн.



Гарантия возврата денег если:

- продавец отменил заказ,
- товар не подошёл или брак,
- вы не получили товар.

ПРИМЕРЫ ФИШИНГА

Фишинг с использованием «Социальных выплат»

ВНИМАНИЕ!

Вы находитесь на официальном сайте **Департамента Социального Обеспечения**.
В интернете участились случаи мошенничества, пожалуйста будьте бдительны.
Сервис **ДСО** защищен по технологии шифрования **3D_Secure**,
Ваши конфиденциальные данные не будут переданы 3-им лицам.

3D Secure
CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

Сервис проверки и выплаты доступных компенсационных социальных начислений из организационных фондов

НАЖМИТЕ ЗДЕСЬ ДЛЯ ВХОДА И ПРОВЕРКИ СОЦИАЛЬНЫХ ВЫПЛАТ



Главная страница портала базы данных Управления компенсационного обеспечения. / [Россия 24](#)



Банк России

17

Фишинг с использованием поддельного интернет-магазина

Войти или зарегистрироваться | Главная | Корзина пустая

Товаров: 0 (0 р.)

Остаток доволен, доставка была сделана вовремя, заранее позвонили и предупредили, товаром тм, за остаток доволен. Обновить...
plbebt ★★★★★

Мы онлайн!
ЗАДАТЬ ВОПРОС

МОЩНЫЙ ИГРОВОЙ НОУТБУК

8999 руб.

16 ГБ ОПЕРАТИВНОЙ ПАМЯТИ
NVIDIA GEFORCE GTX 765 2ГБ
INTEL CORE I5

Рекомендуем



ПРИЗНАКИ ФИШИНГОВОГО САЙТА



- Доменное имя похоже на название известного интернет-магазина, банка, социальной сети, бренда, но отличается на несколько символов.
- Нет префикса **https: s** - secure - безопасное соединение.
- Опечатки, несоответствия, небрежности и ошибки, очень низкие цены.
- На странице оплаты отсутствуют логотипы программ MasterCard SecureCode и Verified by Visa, использующих технологию 3D-Secure.
- Ссылка пришла из неизвестного источника - СМС или социальные сети.
- Вы попали на сайт при использовании открытой сети Wi-Fi без пароля.



ТЕЛЕФОННЫЕ МОШЕННИКИ



Звонок якобы от имени банка: вас просят сообщить личные данные.



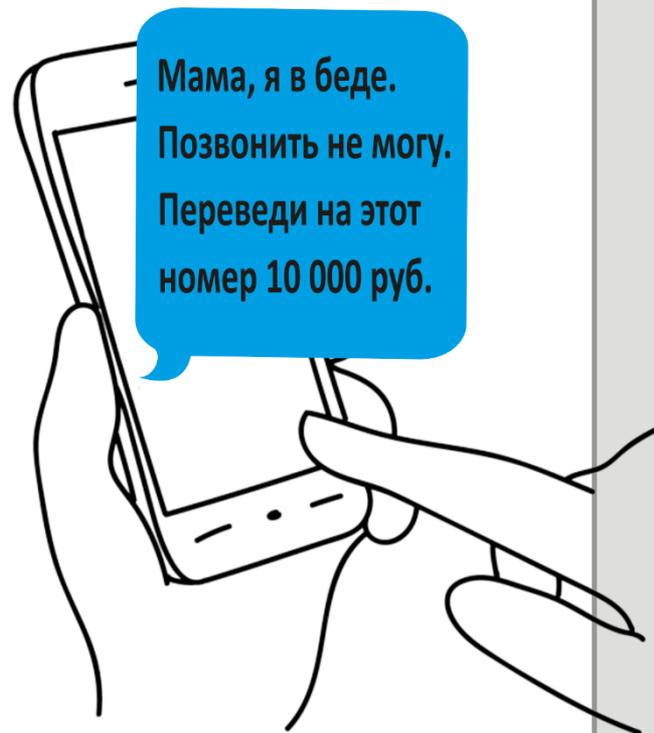
СМС или письмо якобы от банка с просьбой перезвонить.



СМС об ошибочном зачислении средств или с просьбой подтвердить покупку.



СМС от имени родственников, которые просят перевести деньги на неизвестный счет.



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.

КАК ПОСТУПИТЬ?

- 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 .

Напишите ответ в чат

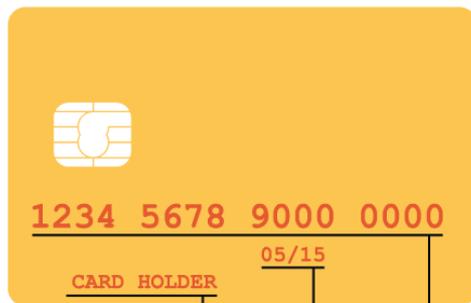


Интерактив

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ



Мошенникам **нужны:**



Имя владельца
Срок действия
Номер карты

Номер CVC или CVV

БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ



Банк России

22



ЗА



высокая скорость
выполнения платежной
операции



удобство для операций
до 1000 рублей - можно
не вводить пинкод

VS



ПРОТИВ



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 видеочкамеру.



В кафе или магазине — сотрудник-злоумышленник может сфотографировать вашу карту.



ТАК МОЖЕТ ВЫГЛЯДЕТЬ БАНКОМАТ СО СКИММЕРОМ

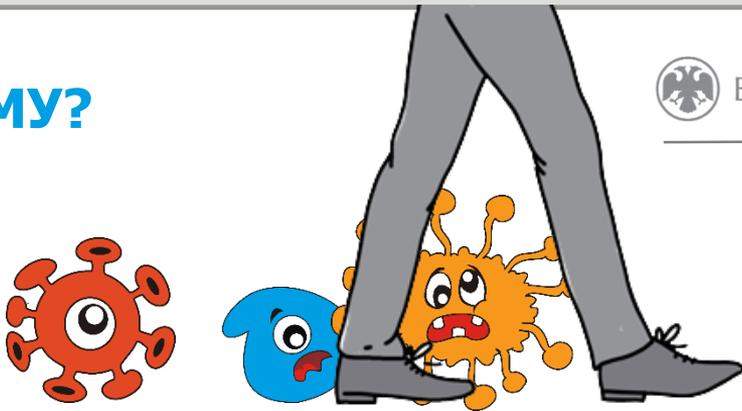


Банк России

24



КАК ОБОЙТИ ПРОБЛЕМУ?



- 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).

С МОЕЙ КАРТЫ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?



Позвоните в банк и **заблокируйте карту.**

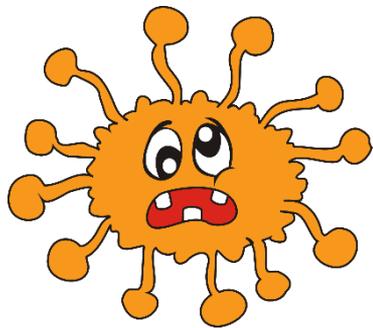


Запросите выписку по счету и **напишите заявление о несогласии с операцией.**



Обратитесь в полицию.





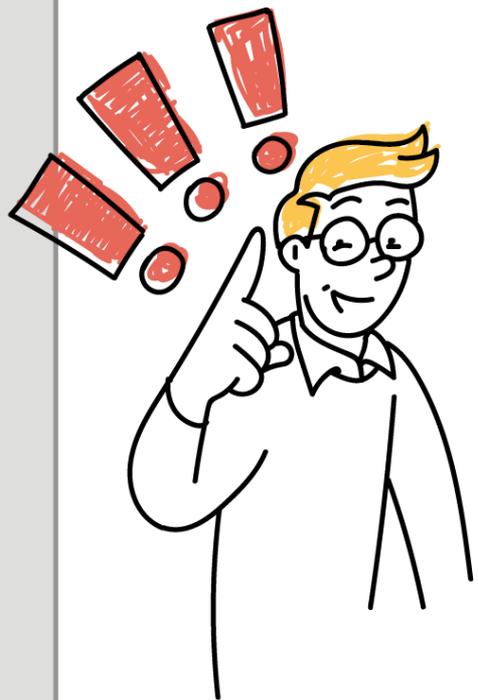
Как не стать жертвой киберпреступников?

Интерактив

Напишите ответ в чат



СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ



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

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

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

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, пожалуйста,
обращайтесь к нам **help@fincult.com**

Подписывайтесь в группы «Финансовое просвещение»!



Facebook: <https://www.facebook.com/groups/finprosvet/>



Одноклассники: <https://ok.ru/finprosvet>



ВКонтакте: <https://vk.com/finprosv>

