Банк России

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА.

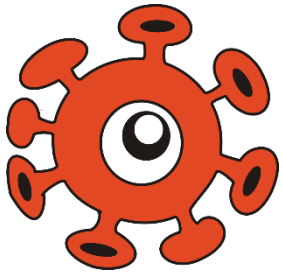
ПРАВИЛА БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ.

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.

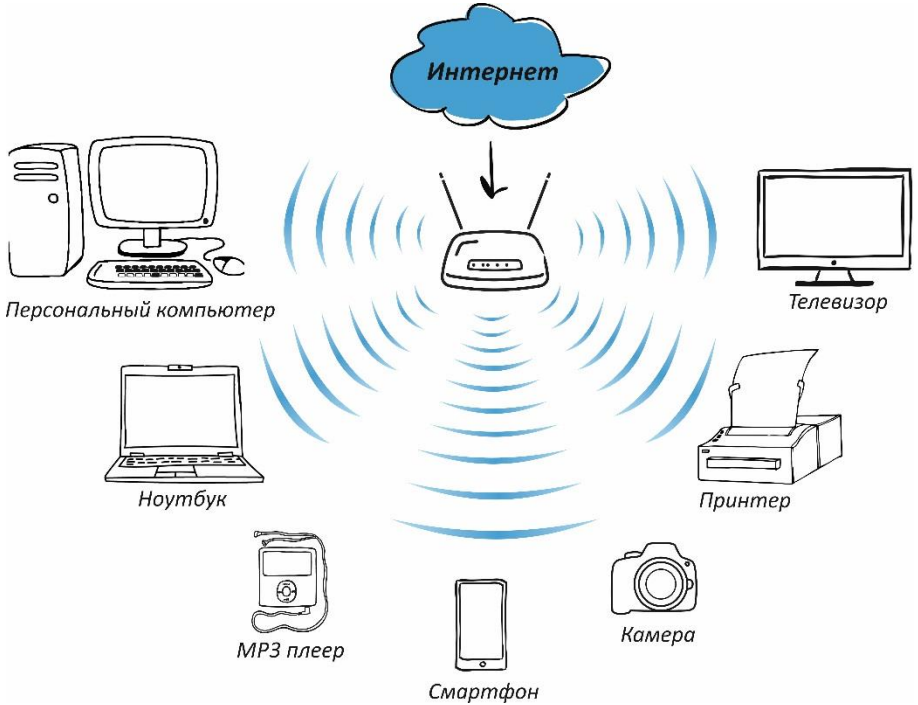


Интерактив

ЧТО ТАКОЕ КИБЕРПРОСТРАНСТВО?

Напишите ответ в чат

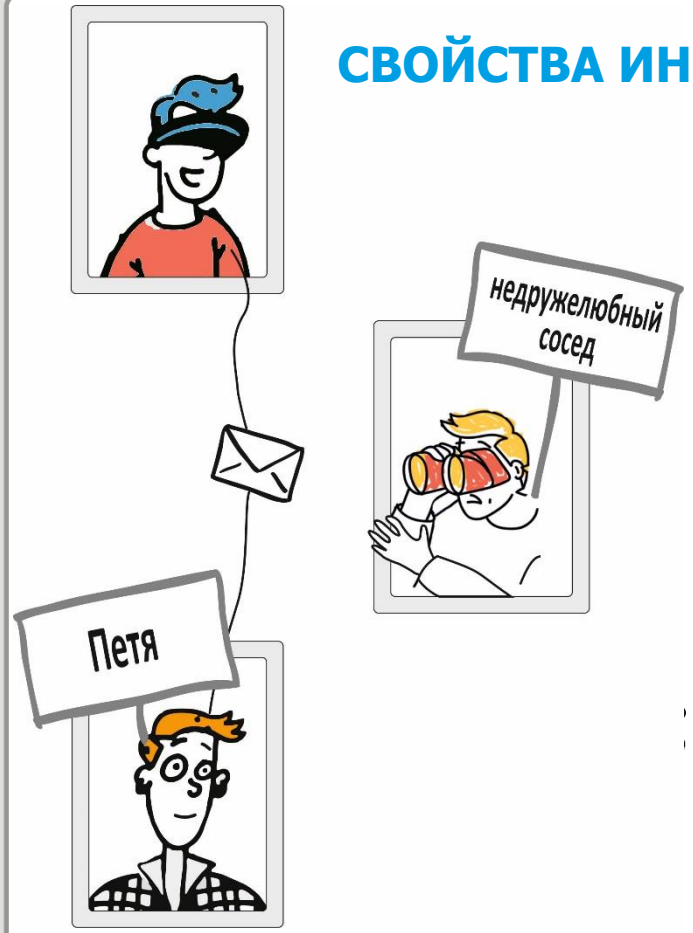
КИБЕРПРОСТРАНСТВО-ЭТО…



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.

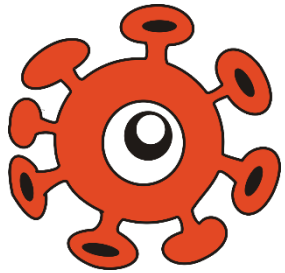
ЦЕЛОСТНОСТЬ- информация остается неизменной, корректной и аутентичной.

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

Интерактив

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)…

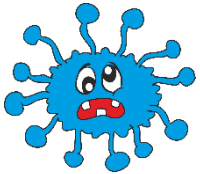
оказание банковских услуг с использованием возможностей глобальной сети Интернет и мобильной связи.

PC – 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.

ВИДЫ ВРЕДОНОСНОГО 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.

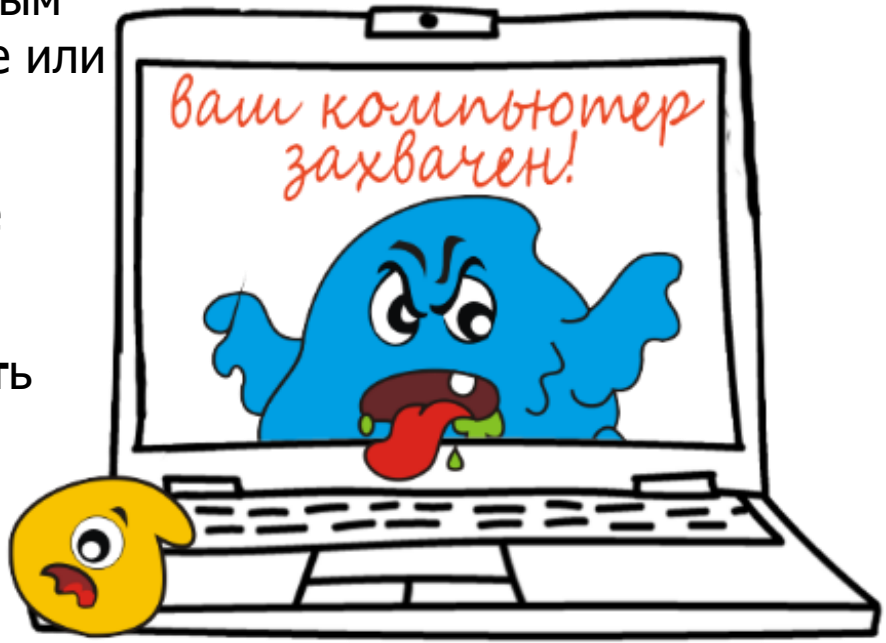
ВИДЫ ВРЕДОНОСНОГО ПО

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

Руткиты (от анг 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.

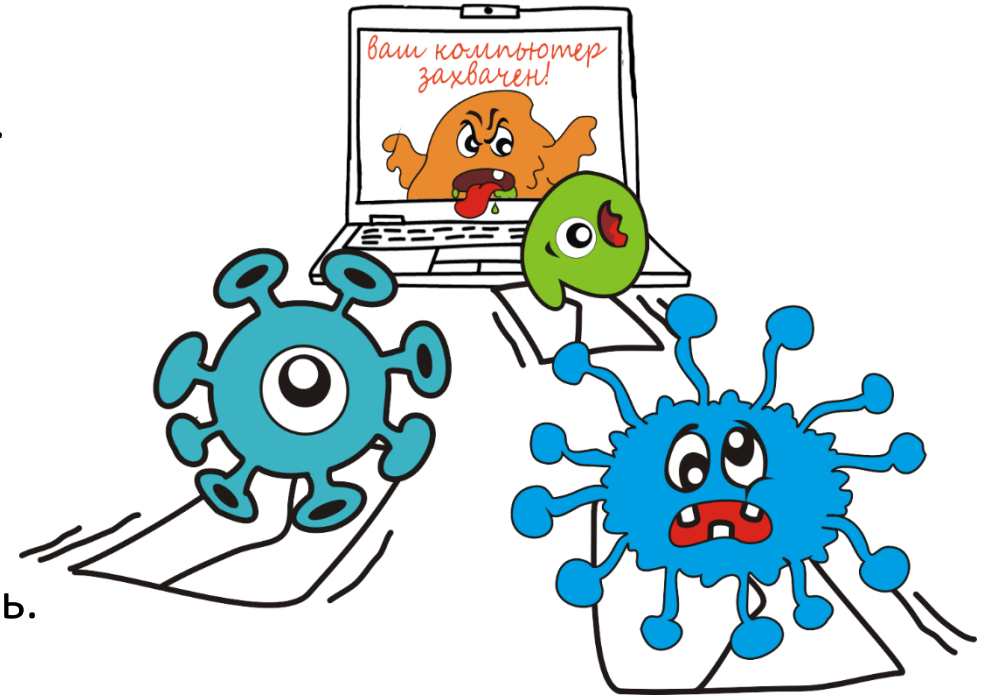


ЧТО ДЕЛАЕТ ЗАРАЖЕННЫЙ КОМПЬЮТЕР

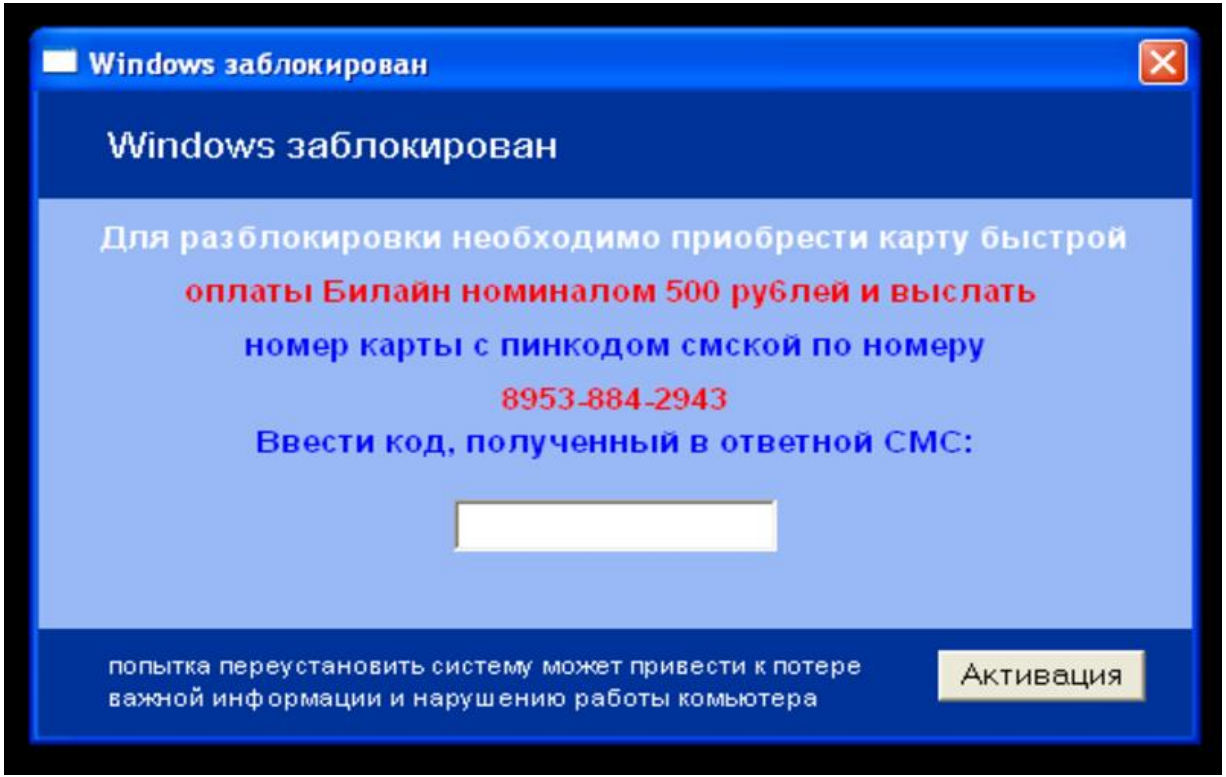
Похищает информацию.

Участвует в атаках.

Нарушает свойства информации – конфиденциальность, целостность, доступность.



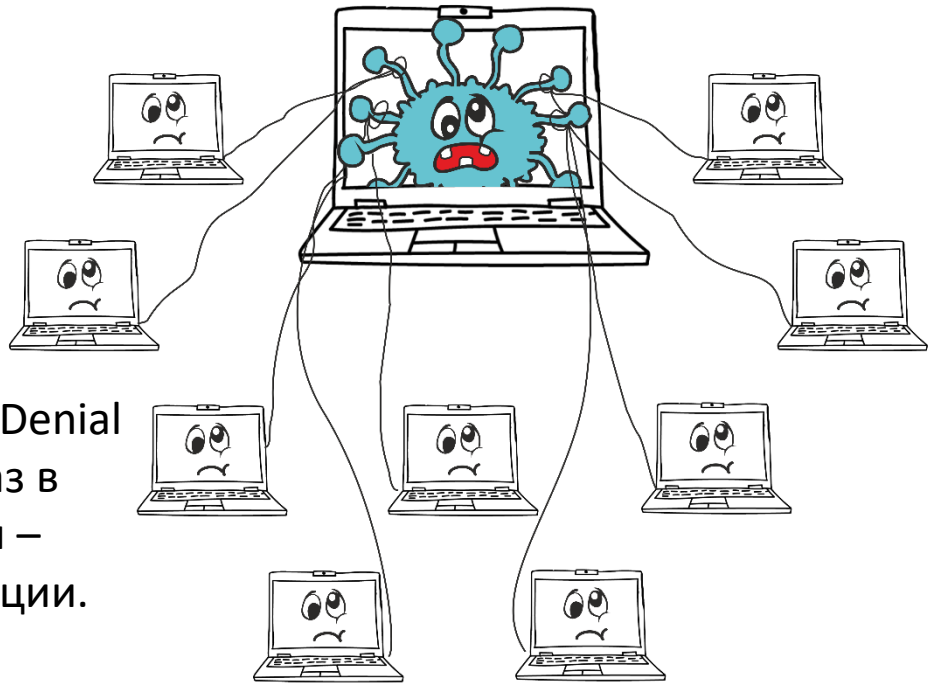
ПРИМЕР БЛОКИРОВКИ КОМПЬЮТЕРА



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?

Интерактив

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.

A. 1, 4

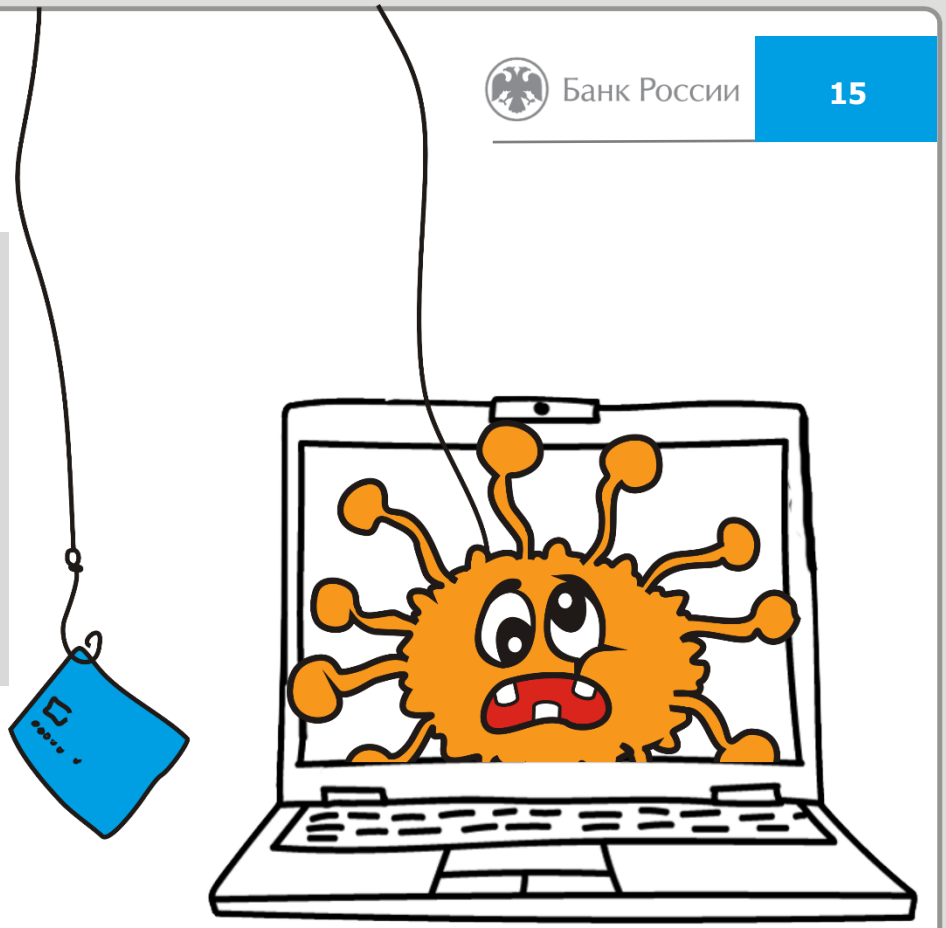
B. 1, 3

C. 2, 3

Напишите ответ в чат

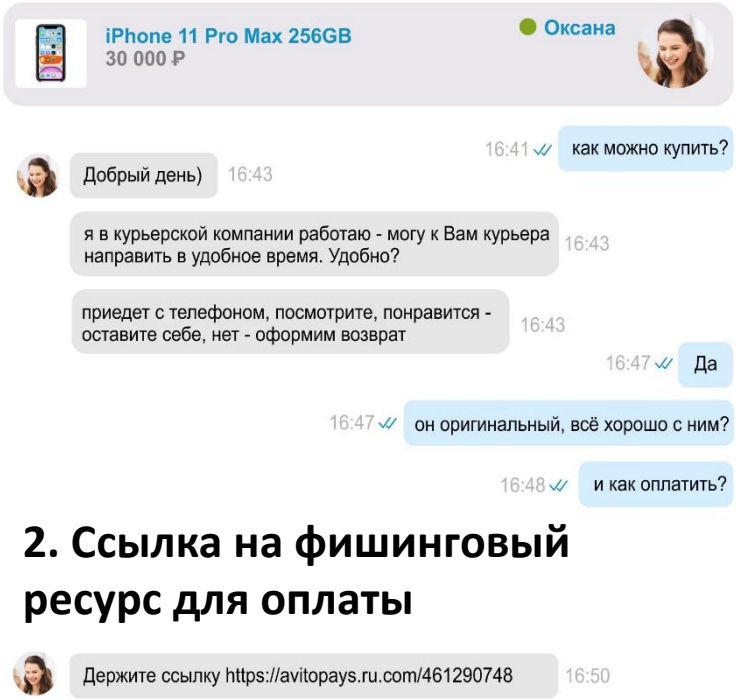
ФИШИНГ- ЭТО…

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



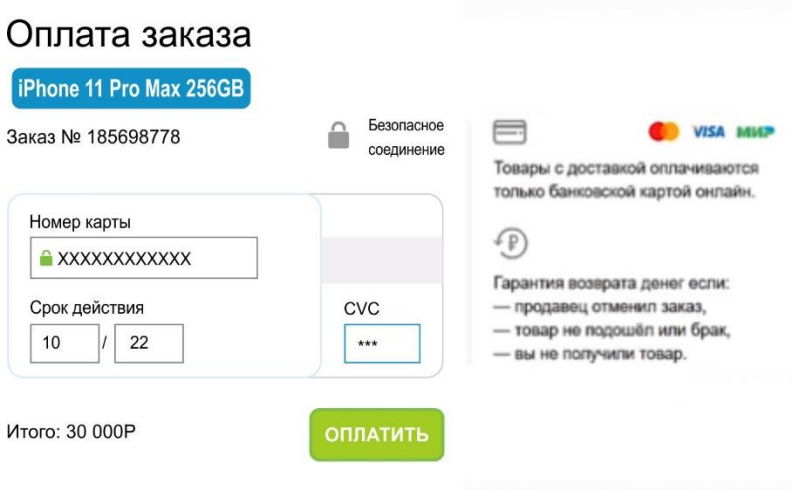
ПРИМЕРЫ ФИШИНГА

1. Общение с «продавцом»



2. Ссылка на фишинговый ресурс для оплаты

3. После «оплаты заказа» продавец пропадёт

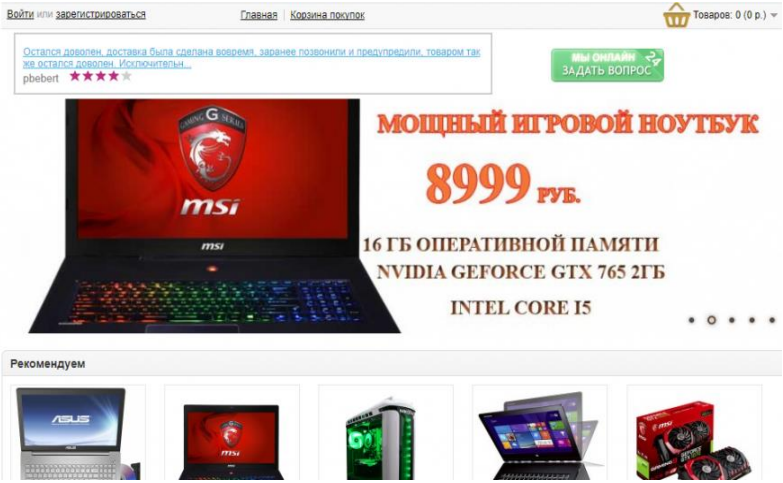


ПРИМЕРЫ ФИШИНГА

Фишинг с использованием «Социальных выплат»

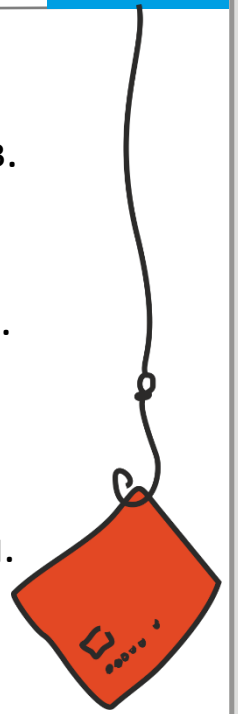
Главная страница портала базы данных Управления компенсационного обеспечения. / Россия 24

Фишинг с использованием поддельного интернет-магазина



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.

Интерактив

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: 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 .

Напишите ответ в чат

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам **нужны:**

БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ

ЗА

- высокая скорость выполнения платежной операции
- удобство для операций **до 1000** рублей - можно не вводить пинкод

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

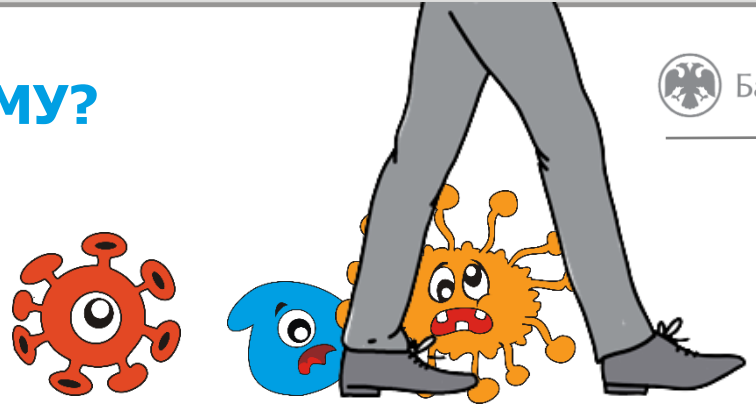
КАК И ГДЕ МОГУТ УКРАСТЬ ВАШИ ДАННЫЕ?

В банкомате — на нем мошенники могут установить скиммер и видеокамеру.

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

ТАК МОЖЕТ ВЫГЛЯДЕТЬ БАНКОМАТ СО СКИММЕРОМ

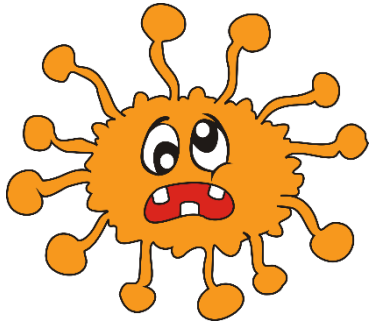
КАК ОБОЙТИ ПРОБЛЕМУ?



- 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?

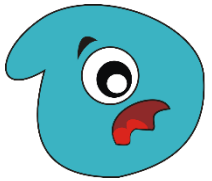
- Позвоните в банк и **заблокируйте карту.**
- Запросите выписку по счету и **напишите заявление о несогласии с операцией.**
- Обратитесь в полицию.



Интерактив

Как не стать жертвой киберпреступников?

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!!!

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